INTERNET USE FOR BUSINESS DEVELOPMENT

AN INTRODUCTORY SET OF TRAINING MODULES FOR POLICYMAKERS

UNITED NATIONS
Bangkok 2007
INTERNET USE FOR BUSINESS DEVELOPMENT

AN INTRODUCTORY SET OF TRAINING MODULES FOR POLICYMAKERS

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

The views expressed do not necessarily represent the decisions or the stated policy of the United Nations. Mention of firm names and commercial products does not imply the endorsement of the United Nations.

This publication has been issued without formal editing.
The role of small and medium-sized enterprises (SMEs) in national competitiveness and development, as well as in generating jobs and revenues for countless citizens, is well documented. Their meaningful and useful access to Information and Communications Technologies (ICT), particularly the Internet, will significantly enhance this critical role and will drive demand for and innovation in the ICT sector even more.

This set of training modules was therefore developed to serve as a policymaking reference on Internet Use for Business Development, principally for middle- to senior-level Internet policy makers and implementers of public policy issues of Internet governance. More particularly, it is intended as an introductory guide to the various issues and legislative/policy options that developing countries should consider as they put into place the policies and rules that will encourage SMEs to take advantage of the Internet to create business opportunities.

Pilot-tested before senior science and ICT ministers from the Asia-Pacific region at the offices of the Economic and Social Commission for Asia and the Pacific in Bangkok in November 2006, this set of training modules underwent further refinement and was finalized based on lessons learned from further pilot national workshops in four developing countries: Cambodia, Lao People’s Democratic Republic, Mongolia and Nepal.

To be sure, this document does not provide all the answers. It does, however, provide many of the critical questions that need to be considered. In this sense this document can provide a useful starting point for policy and decision makers as they grapple with sometimes difficult choices to ensure the continued growth of and access to ICT in their respective countries.

Each country, therefore, can choose to use and adapt the various sections of this training material as they best see fit, given their respective socio-economic and political contexts. It is hoped that they can then share their successes, criticisms, findings and suggestions so that this document can continuously be improved and remain relevant in the fast-changing future.
# TABLE OF CONTENTS

**PREFACE**

**LIST OF BOXES, TABLES AND FIGURES**

**LIST OF ABBREVIATIONS**

**MODULE 1: INTRODUCTION TO INTERNET USE FOR BUSINESS DEVELOPMENT**  1  
I. Introduction  1  
II. A Brief History of Why We Are Where We Are  3  
   A. ICT 4 What?  
III. Overview: ITC for SMEs  8  
   A. Benefits of ICT to SMEs  8  
   B. Barriers to SME Access and Use of ICTs  10  
   C. General Status of Internet Use for Business Development  13  
   D. The Role of Governments in Encouraging ITC Use by SMEs  14  
IV. A Final Point: The Need for Systematic and Continuously Updated Data  17  
Summary: Module 1 in a Nutshell  19  
Additional Information on Internet Use for Business Development  21  

**MODULE 2: LEGISLATIVE AND POLICY OPTIONS**  23  
I. Why Should SMEs Engage in e-Commerce  24  
II. What Can Governments Do to Encourage SMEs to Engage in e-Commerce?  25  
III. e-Commerce Legislation  26  
   A. From a Legal Perspective, What Should SMEs Be Concerned about If They Plan to Engage in e-Commerce?  26  
   B. What Sort of Legal/Regulatory Regime Should Be in Place to Provide This Assurance?  26  
   C. What Are Electronic and Digital Signatures?  27  
   D. Are Electronic Signatures the Same as Digital Signatures?  27  
   E. How Do Digital Signatures Work?  28  
   F. A Note on the Concept of “Technological Neutrality”  35  
   G. Should the Government Formally Endorse the Validity of Digital (or PKI) Signatures?  38  
Summary: Module 2 in a Nutshell  38  
Additional Information on Legislative and Policy Options to Promote e-Commerce and Expand Internet Use  39  

**MODULE 3: CYBER CRIME AND SECURITY**  42  
I. Incidents/Attacks – Trends and Internet Growth  43  
II. Incidents/Attacks – Their Sources and Types  48  
III. Legislative and Policy Considerations to Address Cyber Crime and Security Issues  51  
Annex: Tips on How to Avoid Becoming a Victim of a Cyber Crime  55  
Summary: Module 3 in a Nutshell  60  
Additional Information on Cyber Crime and Security  61  

**MODULE 4: OTHER ISSUES TO BE ADDRESSED IN CREATING AN**
LIST OF BOXES, FIGURES AND TABLES

BOXES
Box 1. Millennium Development Goals
Box 2. How ICT Benefits SME Relations and Interactions  8
Box 3. Examples of Country Initiatives to Address Barriers to SME Access to and Use of ICT  12
Box 4. Making Transactions Secure
Box 5. Specific Government Initiatives and Policies to Encourage the Growth of SMEs
Box 6. What is Electronic Commerce, or e-Commerce?
Box 7. Case Study: The Document Hub
Box 8. Dynamic and Vulnerable
Box 10. How Are Online Consumer Protections Different from Those Offline?
Box 11. A Balancing Act
Box 13. Free and Open Source Software Development  74

FIGURES
Figure 1. Message hops from origin to destination on the Internet  29
Figure 2. Sending a digitally signed message  30
Figure 3. Verifying a digitally signed message  31
Figure 4. Certificate authorities, digital certificates and digitally signed messages  34
Figure 5. Sources of threats  48

TABLES
Table 1. How SMEs benefit from e-commerce processes and techniques  24
Table 2. Vulnerabilities reported by CERT/CC
Table 3. Countries that have enacted cyber crime statutes  51
**LIST OF ABBREVIATIONS**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACID</td>
<td>ASEAN CERTs Incident Drill</td>
</tr>
<tr>
<td>APEC</td>
<td>Asia Pacific Economic Cooperation</td>
</tr>
<tr>
<td>ASEAN</td>
<td>Association of Southeast Asian Nations</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>CERT/CC</td>
<td>CERT Coordination Centre</td>
</tr>
<tr>
<td>ccTLD</td>
<td>country code top-level domain</td>
</tr>
<tr>
<td>DMCA</td>
<td>Digital Millennium Copyright Act</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DSL</td>
<td>digital subscriber line</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>ICT</td>
<td>information and communication technology</td>
</tr>
<tr>
<td>IM</td>
<td>instant messaging</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPP</td>
<td>Internet Printing Protocol</td>
</tr>
<tr>
<td>IRC</td>
<td>Internet Relay Chat</td>
</tr>
<tr>
<td>MDG</td>
<td>Millennium Development Goals</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Cooperation and Development</td>
</tr>
<tr>
<td>PIN</td>
<td>personal identification number</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PSTN</td>
<td>public switched telephone network</td>
</tr>
<tr>
<td>SME</td>
<td>small and medium-sized enterprises</td>
</tr>
<tr>
<td>SSL</td>
<td>secure socket layer</td>
</tr>
<tr>
<td>TLD</td>
<td>top-level domain</td>
</tr>
<tr>
<td>UNCTAD</td>
<td>United Nations Council on Trade and Development</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over Internet Protocol</td>
</tr>
<tr>
<td>WebDAV</td>
<td>Web-based Distributed Authoring and Versioning</td>
</tr>
</tbody>
</table>
I. INTRODUCTION

The Internet has revolutionized, and continues to profoundly affect, the way one does business. It is now a critical (if not the main) tool and venue for conducting commerce. As a tool, it allows buyers and sellers nearly unlimited access to information, goods and services. As a venue, it does away with the limits of geography, the time zones and, in some cases, the need for a physical office. With its tremendous potential, it has become commonplace for businesses and consumers to utilize the Internet for a variety of transactions ranging from emails to actual online purchases.

From a policy point of view, it may seem best to let the Internet and the conduct of its users be left to develop and evolve on its own. In many respects, it is best to rely and trust in the market to lead in the development of the information and communications technology (ICT) sector in general and e-commerce in particular.

Leaving everything to the market, however, is likely to lead to failure. Markets can overlook the needs of remote and unprofitable areas that would otherwise benefit greatly from access to the Internet. Moreover, sound government policies can create the necessary environment and incentives to encourage small and medium-sized enterprises (SMEs) to take advantage of the Internet to create business opportunities.

Further, the huge potential for e-business has attracted unscrupulous individuals who wish to exploit the Internet for their own selfish interests. This type of conduct makes users vulnerable to a host of possible attacks that compromise the confidentiality, integrity and availability of information that they exchange through the Internet. As a result of such illicit activities, people tend to lose trust on the security of doing business in the Internet and thus, forego its huge potential for business, among other socially desirable uses. It is therefore necessary that security measures be set in place to thwart would be attackers who make Internet use unsafe and insecure. Along this line, it becomes of paramount importance to establish mechanisms about the standards, policies, rules, and enforcement and dispute resolution procedures to apply to global inter-networking activities in order to make the Internet free, fair, reliable, transparent, and accessible to all.

Simply put, e-commerce can never prosper unless a secured environment for doing business exists. But this can only happen if the correct policies for securing the Internet are put in place.

This set of training modules is designed to serve as a policymaking reference on Internet Use for Business Development, principally for middle- to senior-level Internet policymakers and implementers of public policy issues of Internet governance. More particularly, it is intended as an introductory guide to various issues and legislative/policy options that developing countries should consider as they put into place the policies and rules that will encourage SMEs to take advantage of the Internet to create business opportunities.

---

1 The definition of what constitutes an SME varies widely across the world and within the Asia-Pacific region from country to country, according to the number of employees and the amount of invested capital or turnover. For example, “SMEs are defined to have less than 200 employees with invested capital of less than K1 million for Myanmar, less than 20 million Baht for Thailand, less than 5 billion VND for Vietnam and less than P15 million for Philippines”, (from the DatumXchange SME definition by Andy Hor [updated June 2002], <http://www.datumxchange.com/articles/smearticle.htm>). According to the Small and Medium Industries Development Corporation (SMIDEC), in Malaysia an SMI is defined as industrial-based companies or companies providing manufacturing-related services with annual sales turnover not exceeding US$8 million and with full-time employees not exceeding 150 individuals. However, there is a less substantial definition for SMEs, which naturally covers a much broader range besides manufacturers and so leaves a certain amount of ambiguity.
The first module provides a comprehensive introduction to the development of the Internet as it relates particularly to SMEs. It outlines the relevance of ICTs to SMEs in terms of opportunities and barriers thereto, and identifies specific policy steps and issues that ought to be considered by countries – particularly developing nations – as they strive to develop legal and regulatory frameworks that will facilitate and encourage access to and use of ICT by SMEs.

The second module deals with key legal and policy topics relating to e-commerce, and the issues that need to be considered to encourage SMEs to engage in e-commerce.

The final two modules focus on other issues that need to be considered in order to truly establish an enabling environment for Internet Use for Business Development. Particular focus is given to cyber crime and security in the third module. Overviews of other critical issues, including consumer protection, intellectual property rights, data protection and privacy, as well as the need for international cooperation and harmonization, are provided in the final chapter.

The materials included here, as well as the issues contained herein, are not exhaustive. This is merely an introduction, and it is hoped, nonetheless, that they convey a sense of need – and realistic possibility – for a holistic approach to policymaking in this area.

This document does not purport to provide ready answers. Rather, it is intended to pose questions and issues for the reader in the hope that these will provoke thoughtful reflections. It should be noted that there is no one set of policies or rules that will apply to each and every jurisdiction. Therefore, it is hoped that this document will be a useful reference on ICTs for all stakeholders, not in the sense of a map or encyclopedia that provides easy answers, but rather as a useful tool for readers to think through the issues, learn about best practices and models, and then, ultimately, reach conclusions on their own.

II. A BRIEF HISTORY OF WHY WE ARE WHERE WE ARE

Before going into the main subject of this Module, i.e., the use of the Internet for Business Development, particularly by SMEs, it would be useful to consider and revisit the trends and factors that converged to make the ICT sector the critical driver of the global economy that it, undeniably, is today.

The global ICT sector has been, and continues to be, shaped by a number of powerful interrelated forces. Chief among these forces are:

- Technological developments;
- Convergence of telecommunications, broadcasting and multimedia;
- Globalization and internationalization of markets; and
- Emergence of broadband services.

(a) Technology: The key technological development which has occurred is the emergence of the digital packet switched network architecture, which effectively replaced traditional circuit switched networks. This dramatically reduced cost, improved quality and enabled the development of a wide range of innovative applications.

The establishment of the Internet Protocol (IP) as the global open network service standard, in particular, facilitated the blending of different services (e.g., telephony, data, interactive video) via one infrastructure.

The delivery of services over IP is now a leading driver of change and innovation, the result of which is that new participants in the ICT sector now exclusively build IP networks.

(b) Convergence: The deployment of digital packet switched technology also fuelled the convergence of telecommunications, broadcasting and multimedia. Previously, each sector was treated as distinct, and therefore regulated separately.
As digital technology emerged with increasingly open interfaces between different applications, the distinctions between each sector have rapidly eroded. Cable companies can now provide internet telephony while telecommunications companies can provide internet services. Newspapers can now also be read online.

In the digital world, the “network” is not confined to specific applications. The digital network is a ubiquitous platform, capable of transporting all digital data with equal ease. The network is “blind” to distinctions between voice, computer data, video, or transactional data. All are simply digital data.

The Internet is virtually substitutable for all forms of existing media and is a competitive threat to every provider of telecommunications, broadcasting, operating software and data communications. As a result of convergence, different content services (voice, radio, television, etc.) can now be delivered by practically anyone to anyone anywhere in the world.

(c) Globalization: Globalization is the process in which the world is treated as one market without regard to national boundaries. Over the last decade, globalization and ICT have gone hand in hand – the rapid spread of the use of ICT is both a result and a driver of globalization.

ICT is a key enabler of globalization. The specialization of production through advances in manufacturing techniques has lowered costs and shortened economic distances. In addition, the systematic rationalization of procedures and documentation and the wider and easier dissemination of market information have broken down the factors that have made markets distinct.

At the same time, globalization has fuelled the demand for ICT. As new markets open up, buyers and sellers have turned to ICT for new financial instruments and services and faster and cheaper ways to facilitate cross-border transactions.

(d) Broadband: The emergence of the Internet has also seen the emergence of new, high-bandwidth networks and new network paradigms that are rapidly displacing the traditional, narrowband public switched telephone network (PSTN) model. Broadband services enable high-capacity communications services characterized by both high data transmission speeds and high volumes of data.

Broadband services offer significantly faster data rates and “always on” connection to the Internet.

The growth of high-speed broadband infrastructure, either wired or wireless, coupled with technological advancement in equipment, by the global proliferation of small mobile devices and other intelligent terminals that can be used to communicate and gather converged data, voice and video information and services anywhere anytime, make the lives of people more convenient. These forces have resulted in spectacular developments in nearly all fields of human endeavour, creating opportunities for countries, corporations and individuals to be creative, to flourish, and to lead even more meaningful and productive lives.

What opportunities would arise from the introduction or use of ICT for:
- Your government?
- A small company in your country?
- An ordinary citizen?
- A student?

A. ICT 4 What?

While ICTs are not a panacea for all development problems, they offer enormous opportunities to narrow social and economic inequalities, and thus help achieve broader development goals, such as the Millennium Development Goals set by the United Nations.
ICTs effectively contribute to the achievement of the goals, particularly those related to income, poverty reduction, education, health, environment and gender equity by:

- Creating economic opportunities and contributing to poverty reduction;
- Managing the processes of providing basic services (for example, health care and education) at lower cost and with greater coverage;
- Facilitating access to information and the involvement of stakeholders through greater transparency and support for networking at every stage;
- Enhancing the capacity to measure, monitor and report progress on the goals and to strategize.

Policymaking related to ICTs will vary depending on the needs, goals and socio-political and economic context that a country finds itself in.

The view of industrialized countries is that ICTs can enable the economy and all sectors of human activity.

- The United States of America for example, is a prime example of how the adoption of ICT can lead to increases in efficiency that, in turn, translate into increased rates of economic growth and GDP.
- Canada has an ambitious plan called “Connecting Canadians” which envisions and plans to make Canada the most connected country in the world and to make Canada a world leader in developing and using an advanced information infrastructure to achieve its social and economic goals in the knowledge economy.
- Newly industrialized countries of the Asia Pacific have found that ICTs are a key to an economy’s competitiveness, people’s standards of living and a country’s ability to fully participate in the global economy.

- Malaysia, for example, is committed to using ICTs to achieve its development objectives. It plans to invest more than US$2 billion over the next decade to become the multimedia hub of Southeast Asia.
- China is also moving to e-enable the country by connecting all major centres with fibre optic cabling.
- India has emerged as a powerhouse in the e-services sector.

From the point of view of small island developing states, ICT deployment is focused more on overcoming isolation, small population sizes, small markets and vast distances that separate these countries from each other and the rest of the world.

- It should be noted, too, that to some extent, rural and unserved communities in many, if not most, developing countries, share these disadvantages. Lessons and best practices can thus be shared between and among them.

**Box 1. The Millennium Development Goals**

The United Nations has set eight goals to be achieved by 2015 that respond to the world’s main development challenges. The goals are drawn from the actions and targets contained in the *Millennium Declaration* that was adopted by 189 nations and signed by 147 heads of state and governments during the *United Nations Millennium Summit* in September 2000.

- Goal 1: Eradicate extreme poverty and hunger
- Goal 2: Achieve universal primary education
- Goal 3: Promote gender equality and empower women
- Goal 4: Reduce child mortality
- Goal 5: Improve maternal health
- Goal 6: Combat HIV/AIDS, malaria and other diseases
- Goal 7: Ensure environmental sustainability
- Goal 8: Develop a Global Partnership for Development

**How can ICT be used to help meet these goals?**

- Goal 1: To provide access to information and education resources.
- Goal 2: To improve learning outcomes and access to education.
- Goal 3: To empower women by providing access to information and opportunities for networking.
- Goal 4: To improve health monitoring and reporting.
- Goal 5: To enhance maternal health monitoring and reporting.
- Goal 6: To support the delivery of health and education services.
- Goal 7: To support environmental sustainability initiatives.
- Goal 8: To promote global partnerships and knowledge sharing.
• Facilitating voice communications at low costs (Voice of Internet Protocol, VoIP), or even simple email, are therefore particularly useful.

• Community-based networking initiatives designed to increase awareness and use of ICTs, and to encourage their use by local populations and in schools are increasing. For example, community radio is also a useful application in Kothmale, Sri Lanka, where community radio and Internet connectivity have been brought together to help the radio station meet the information needs of its listeners.

Therefore, when thinking about the strategic and policy direction that countries should pursue in terms of developing, and promoting the deployment of and access to their respective ICT sectors, it is important to keep in mind that ICT is merely a tool, and not an end in itself.

What will it be used for? Why is it needed? What are the country strengths and weaknesses that will be enhanced or addressed?
III. OVERVIEW: ICT FOR SMEs

**How important are SMEs collectively to your country? What and how much do they collectively contribute – in terms of employment, revenue, and overall development?**

The information revolution has transformed the way modern business is conducted, as ICTs have enabled people to exchange large amounts of information quickly, reliably and cheaply. Success is now determined by those who can best receive, process, and innovate.

As previously stated, ICTs can spur growth, create jobs for the poor, improve market access, contribute to income generation and enhance rural productivity. The economic contribution of ICTs is two-fold - income generation and poverty reduction. ICTs enable people and enterprises to capture economic opportunities with a view to increasing process efficiency, promoting participation in expanded economic networks and creating opportunities for employment.

ICTs can enable solution-sharing among local people and communities, providing access to practical information on matters such as small-sized business accounting, weather trends or best farming practices. In addition, they can facilitate global connectivity, resulting in new ways of creating and delivering products and services on a global scale; and provide developing countries with access to new markets and new sources of competitive advantage to boost income growth.

ICT can also enhance the key role that SMEs play in national economic development strategies by facilitating flows of information, capital, ideas, people and products. A strong SME sector that is integrated into the global digital economy can lead to job creation, increased public revenue and a general rise in the standard of living. In addition, the uses of ICT to enable SMEs to participate in the knowledge economy offers enormous opportunities to narrow social and economic inequalities and thus help achieve broader development goals.

**A. Benefits of ICT to SMEs**

For SMEs in particular, the use of ICTs can provide several significant benefits, among them:

- Increasing productivity in the production process;
- Enhancing and increasing the efficiency of internal business operations; and
- Connecting SMEs more easily and cheaply to external contacts, whether locally or globally.
Concrete examples of how ICTs can benefit SMEs, include the following:

- Improve inventory management systems;
- Decrease wastage in production processes;
- Improve communication between different departments within the firm;
- Improve accounting and budgeting practices;
- Reduce communication costs and geographic barriers with global suppliers and clients;
- Expand client base through e-marketing (e.g., web sites, portals and mailing lists);
  - Link to local and global supply chains and outsourcing opportunities;
- Share and learn new business practices;
- Facilitate capacity-building of owners and employees through e-learning platforms;
- Simplify government services such as business registration and filing taxes;
- Introduce new methods of payment through e-commerce.

Simply put, Internet and e-commerce enable SMEs to gain access to new customers and to expand their markets geographically, even if they physically have to remain in local and regional markets because of lack of information and marketing capability. Through their web sites, SMEs can attract potential investors and customers by providing information on their technologies, products, services and financial positions. Moreover, the Internet can help knowledge-based small businesses convey their ideas to the whole world, allowing even micro-enterprises with ideas and technologies to remain small and profitable, or even to generate substantial global sales by exploiting their intellectual property over the Internet.

B. Barriers to SME Access and Use of ICTs

Despite the benefits, numerous barriers exist that make it difficult and challenging for SMEs to embrace these new technologies.

1. **Unsuitability for Business.** SMEs may not see the relevance or suitability of ICT to their businesses. This was the leading reason given by businesses for not engaging in e-commerce as found by a survey conducted by OECD in 2002 of SMEs with fewer than 250 employees in 19 European countries. Many may believe that their goods or services do not lend themselves to Internet transactions.

   SMEs will not take advantage of e-business unless the benefits outweigh the costs and justify establishing and maintaining the e-commerce system.

   In many instances, they may find it more difficult, relative to larger firms, to find an e-business case applicable to them because of lack of time, information and knowledge. They may also wish to retain their current business model and avoid the risks associated with new investments and new business models.

   They may also be worried that existing customers will be turned off by the changes that they may institute.

2. **Lack of ICT and Managerial Knowledge Internally.** SMEs often lack the human technological resources needed for ICT and e-commerce, especially because they have to focus on day-to-day operations, and lack the time and extra resources necessary to understand the benefits of new technologies.

   Even if they are aware of the potential benefits of adopting ICT, they would still require know-how or qualified personnel.

   SMEs may also lack managerial understanding and skills for e-business. Successful integration of e-business often requires restructuring of business processes, or changes in organizational structures. Professional IT or e-business consultants could help, but SMEs may not have ready access to them because of their relatively high costs.
3. **Costs of Developing and Maintaining e-Business Systems.** SMEs are generally concerned about the costs of establishing and maintaining e-commerce systems since they often suffer from budget constraints and are less sure of the expected returns on such investments.

Some SMEs cannot afford to adopt sophisticated ICT solutions (e.g., web sites with a secure environment allowing credit card transactions).

Outsourcing webpage design and updating are optional, but the costs of such may be difficult for SMEs to contain.

Logistics services, such as package collection and delivery, also matter. This is a real concern for small businesses, especially in remote districts where private package collection/delivery services may not be available at reasonable costs. Some items, such as software, music and books, could be delivered digitally, but it may not be feasible for an individual, business or customer with slow Internet connections, or small download capacities.

4. **Network Infrastructure – Access.** The availability of a wide range of Internet connections and other communications services, preferably at competitive prices, is very important to the extent that it allows small businesses to choose different and appropriate services according to their specific needs and expectations from on-line activities.

The availability of broadband connections may affect SMEs’ decisions to adopt e-commerce. Broadband’s faster speeds improve overall online experiences for both individuals and businesses, encouraging them to explore more applications and spend more time online. In contrast, slow internet connections and data transfers discourage SME adoption of the Internet.
Box 3. Examples of Country Initiatives to Address Barriers to SME Access to and Use of ICT

**Limited ICT literacy**
Singapore launched its Infocomm Competency Programme to increase the computer literacy of its workforce. The programme subsidized S$5.00 (US$3.00) per trainee per hour for SMEs on broad-based ICT courses such as Office applications, desktop publishing, workgroup applications, and web page design.

**High fixed cost**
To encourage SMEs to use ICT equipment to increase productivity, the Government of Japan allows corporations to deduct up to 6 per cent of total lease payment on brand new machines from annual income tax payments. The government also subsidizes up to 25 per cent (with a cap at JPY 2.5 million or US$22,000) lease payments for corporations in agri-business management, lumber supply and aquaculture.

**Poor communications infrastructure**
In May 2005, the Philippine National Telecommunications Commission, the local telecoms regulator, finally issued rules classifying VoIP as a value-added service, rather than as a traditional voice service, effectively opening the service to broader competition. Within days of the issuance of the ruling, long distance rates began falling as much as 75 per cent.

**Inexperience in integrating ICT into the business process**
The Hong Kong Productivity Council sponsors various sector-specific programmes that help businesses increase productivity through better utilization of ICT resources. Their Enterprise Resource Planning Centre provides training, consulting and a software platform for its subscribers. In addition, the Vocational Training Council of Hong Kong provides e-learning courses by sector.

The Government of the Republic of Korea created the Korean Market Place web site to showcase products of Korean SMEs to global buyers. Local SMEs can easily connect to the global network by posting offers to buy or sell products. It currently hosts over 20,000 homepages of SMEs and e-catalogues of over 120,000 products.

**Undeveloped legal policy for electronic payment and security issues**
Between 1998 and 1999, the Government of Singapore passed the Electronic Transaction Act and Electronic Transactions Regulations to legitimize electronic signatures in the legal framework. This provided a foundation for key public and private sector leaders, including the Monetary Authority of Singapore, Cisco Systems, and Visa International, to develop more secure e-payment services over a public key infrastructure.

Lesser-known SMEs are at a clear disadvantage in terms of buyer confidence when compared with large multinationals with highly recognizable brand names. Online clients view recognition of a brand or company name as an indicator of a firm’s credibility, just as they do offline. The inability to verify online sellers’ credentials ranks high among reasons for reluctance to buy online.

A professional web site can help improve a firm’s image for large-scale B2B transactions.

Moreover, consumers who use credit cards for online transactions are highly concerned about security, protection of credit-related information and secure systems. As more online clients demand secure transaction environments, SMEs are likely to face increasing costs for system protection and security measures.

Other related barriers include payment uncertainties and contract, delivery and guarantee uncertainties.

Privacy and legal protection for Internet purchases are also significant concerns, both for businesses and customers alike.

6. **Legal Uncertainties.** Legal uncertainties and conflicting regulatory environments for cross-border transactions may affect SMEs strongly. SMEs may be at risk of being sued in multiple
jurisdictions under a number of inconsistent laws. But more generally, the lack of a satisfactory redress mechanism in the event of a dispute may strongly discourage both B2B and B2C online transactions.

C. General Status of Internet Use for Business Development

Although there are limited data and studies focused on the adoption of the Internet and e-commerce by firms in developing countries, and particularly SMEs, there is ample anecdotal and case study evidence that show that SMEs generally (especially those in urban centres) can easily use and be connected to the Internet – if they want to.

According to a 2004 Report on e-Commerce and Development by the United Nations Council on Trade and Development (UNCTAD), the main uses of the Internet for business purposes are exchanging email, accessing the World Wide Web for information or transactional purposes, or setting up a company web site, which would represent their main gateway to the Internet for both B2C and B2B transactions.

The challenge is to move SMEs to go beyond these first few basic steps, and to eventually move towards integrating ICTs in more sophisticated business applications as outlined above.

This is a major step for SMEs, especially in developing countries, because these would require management and technical skills and investments (as well as organizational changes) that they may not be able to afford or for which they may not have ready access.

D. The Role of Governments in Encouraging ICT Use by SMEs

The role of government is to create the enabling environment that will enable these benefits to flourish and be easily recognized.

“Creating an Enabling Environment” means addressing, in a holistic manner, the various policy, legal, market and social considerations that interact both at domestic and global levels to create fertile conditions for ICT-led growth.

Public policy is the tool by which the government can help to create an environment and remove barriers for businesses to adopt ICT. The government should take the following steps to provide a supportive legal and regulatory environment for e-business (World Bank, 2005):

- Create appropriate environments for ICT access and use, such as liberalizing markets to expand and improve network infrastructure. Increase liberalization and competition in ICT markets to stimulate investment telecommunications, such as broadband access.

- Develop e-security policies and programmes and provide supportive legal and regulatory environments. The government should set up a regulatory framework for trust, security, enforcing authentication mechanisms and combating cyber crimes, which will encourage business use of ICT. Specific policies include low-cost online dispute resolution, e-security policies such as Public Key Infrastructure (PKI) and Computer Emergency Response Teams (CERTs).

- Enhance technological diffusion, and overcome market failures by launching e-government services and e-procurement programmes to contribute to promoting trust and security in online transactions.

Box 4. Making Transactions Secure

One key indicator of the use of the Web for business purposes is the number of web sites that use the secure socket layer protocol (SSL), which supports secure transactions (although most businesses, it should be emphasized, use the Web for other purposes).

According to a Netcraft survey, this grew by 56.7 per cent between April 2003 and April 2004, reaching 300,000. Servers using SSL use it mostly for e-commerce, e-payments and e-banking transactions, as well as any other transactions for which there is a need for secure exchange of information.
• Provide and support ICT training for skill development. The government has a major role in providing basic ICT skills training, such as integration of ICT in school curriculum and conjunction with the private sector on the ICT demands of the sector.

Key policy directions in this respect should include the following:

1. **Business Environment.** As a basic requirement, a healthy business environment is fundamental for firms to thrive and benefit from ICTs. This includes:
   - A transparent, open and competitive business framework;
   - Clear, independent rule of law for all firms;
   - Easy set-up and dissolution of businesses;
   - Transparent, simple and accessible corporate regulations; and;
   - Equal and stable legal treatment for national and cross-border transactions.

   In other words, the government must develop and implement policies and regulations that will make it easy for people to set up businesses and remove barriers to help these businesses become more profitable and competitive.

2. **Network Infrastructure and Broadband Deployment.** Broadband connectivity is a key component in ICT development, adoption and use. It accelerates the contribution of ICTs to economic growth, facilitates innovation, and promotes efficiency, network effects and positive externalities. The development of broadband markets, efficient and innovative supply arrangements, and effective deployment and use of broadband services require policies that:
   - Promote effective competition and continue to stress liberalization in infrastructure, network services and applications across different technological platforms;
   - Encourage investment in new technological infrastructure, content and applications; and
   - Take a technology-neutral stance among competing and developing technologies to encourage interoperability, innovation and expand choices.

   Public financial assistance and other initiatives to expand coverage for under-served groups and remote areas could complement private investment where appropriate, provided it does not pre-empt private-sector initiative or inhibit competition.

**Regulatory Trust.** SMEs have to be certain that the regulatory system will ensure and properly balance their security, privacy and consumer protection interests. Issues that need to be addressed could include:
   - Cyber crimes and cyber-security;
   - Spam;
   - Cross-border cooperation;
   - Presence of low-cost online dispute resolution mechanisms between firms, and between firms and consumers.

**Box 5. Specific Government Initiatives and Policies to Encourage the Growth of SMEs**
   - Simplify registration and other legal processes.
   - Create incubators and science parks.
   - Provide business skills education.
   - Provide business consulting services.
   - Provide SME financing.
   - Help create SME linkages with larger companies.
   - Implement favourable tax and trade policies.

3. **Content Development.** The government and the private sector have key roles in facilitating content availability across all platforms and encouraging local development of new content, including content from public sources. This brings with it issues concerning intellectual property rights, which need to be balanced against public interests to promote creativity and innovation.

4. **Human Capital Development and Skills Enhancement.** Lack of ICT skills and business skills are widespread impediments to effective uptake once adoption decisions are made.
Governments have major roles in providing basic ICT skills in compulsory schooling and an important role in conjunction with education institutions, business and individuals in providing the framework to encourage ICT skill formation at higher levels, in vocational training and in ongoing lifelong learning.

5. **Information.** Small firms may not have enough information regarding the benefits and costs of adoption of ICT. The private sector (e.g., business associations) and government must facilitate awareness and access to services that are available, as well as provide information on the benefits of adoption and use of ICT, for example, through case studies and real-world best practices.

6. **e-Governance.** Online provision of government information and services can increase the efficiency and coverage of public service delivery to small firms and act as a model user and standard-setter for ICT adoption by small firms. As a model user of broadband, the government can demonstrate the potential of broadband-based services and content, and provide demonstrations and “pull-through” mechanism for small firms. Government demand aggregation to provide services can help spread new services more widely. Education, general government information and services and the provision of government services to businesses and citizens can all potentially benefit from the use of new high-speed infrastructure and services, and should be given priority in government strategies.

Particularly in relation to SMEs, the integration of e-government into business processes could assist SMEs in their efforts to embrace and integrate e-business. It could provide SMEs with an incentive to go online.

**IV. A FINAL POINT: THE NEED FOR SYSTEMATIC AND CONTINUOUSLY UPDATED DATA**

Currently, there is no international database that provides comprehensive information on the use of ICTs by businesses in developing countries. Statistics can more easily be found for the developed countries. The Organization for Economic Cooperation and Development (OECD) and Eurostat have been compiling information on their respective member countries for a few years now.

On the other hand, for developing countries, only a few have started to collect ICT indicators through their respective statistical systems. However, the data collected are not always comparable across countries, or with those of developed nations.

There is, therefore, a need for collective action at the international level to coordinate the methodology and work towards a global database of ICT indicators.

From a country level, policymaking will benefit from systems that enable the collection of ICT indicators and that yield better knowledge about the adoption of the Internet and e-business in developing country firms, particularly SMEs.

For example, in 2001, The Asia Foundation carried out a project to survey the use of the Internet and e-commerce in four South-East Asian countries: Indonesia, the Philippines, Sri Lanka and Thailand. Obviously, the data could very well be dated by now, but for purposes of illustration, consider how observations (if properly backed by reliable data) could lead to better policy conclusions:

1. **Observation:** Neither cost nor technical ability (to use the Internet) was found to be the main barrier preventing SMEs from going online.

   **Policy conclusion:** Subsidization to SMEs to encourage them to adopt ICTs, therefore, might not be necessary. Rather, governments should concentrate on the regulatory or legal changes, such as e-commerce legislation and deregulation of the telecommunications industry, to increase access outside the major cities.
2. **Observation**: The main perceived barrier for Internet uptake is very similar across companies from both developed and developing countries: lack of network security, and slow and/or unstable connections.

**Policy conclusion**: Clearly, these are areas where the government can and must take action. Legislation to promote network security and instil confidence in the same would be critical. Universal access strategies to enable SMEs in unserved or remote areas to obtain reliable, low cost connections (note that dial-up connections would often be sufficient) could be developed.

3. **Observation**: SMEs generally find it relatively easy to use PCs and then connect to the Internet to use email and set up web pages. However, the introduction of the Internet into their business activities (including e-commerce) does not follow easily, and larger companies are more likely to automate their business processes (and to do so earlier) than smaller companies. Note that some studies have found a positive relationship between profitability and the level of intensity of ICT tools, with firms using more advanced e-business tools achieving higher profitability.

**Policy conclusion**: While, as stated previously, SMEs would make investments if they thought it made business sense, making or encouraging SMEs to make the leap from simple (and low-cost) Internet use to building e-business systems fully integrated with customers and suppliers requires additional investments, as well as technical and managerial skills that the SMEs might not yet have. It also demands some competence in designing and implementing e-business strategies. There are areas where public and private agencies can support SMEs, through assistance for educational and training.

*Does your country have a system in place to collect, monitor and analyse data and statistics on the use of ICT in your country? Is there a need for such, and how can this be done? What sort of information is needed to develop good policymaking on Internet use for business development?*
SUMMARY: MODULE 1 IN A NUTSHELL

- Four forces continue to shape the global ICT sector:
  - Technological developments, particularly the establishment of the Internet Protocol (IP);
  - Convergence of telecommunication, broadcasting and multimedia;
  - Globalization, which allows the world to be treated as one market, regardless of national boundaries; and
  - The emergence of broadband, which provides increasingly faster data rates and “always on” connectivity to the Internet.

- ICT effectively contributes to the achievement of the Millennium Development Goals, particularly those related to income, poverty reduction, education, health, the environment and gender equality.

- ICT benefits SMEs in various ways, such as:
  - Increasing productivity in the production process;
  - Enhancing and increasing the efficiency of internal business operations; and
  - Connecting SMEs more easily and cheaply to external contacts in the local and global markets.

- Barriers to SME access and use of ICTs include:
  - Inability of SMEs to see the relevance or suitability of ICT in their business;
  - Lack of internal ICT and managerial knowledge;
  - Costs of developing and maintaining e-business systems;
  - Lack of access to the network infrastructure;
  - Difficulties in building trust and enhancing security; and
  - Legal and regulatory uncertainties.

- The key role of governments in encouraging ICT use by SMEs is to create “an enabling environment,” which means, “addressing in a holistic manner, the various policy, legal, market and social considerations that interact both at domestic and global levels to create fertile conditions for ICT-led growth”. Key policy directions in this respect include:

- Fixing the business environment to make it easy to do business;
  - Promoting the development of the network infrastructure, and encouraging broadband deployment;
  - Enhancing trust in the regulatory system;
  - Facilitating content development;
  - Supporting and promoting human capital development and skills enhancement;
  - Increasing awareness of the benefits and use of ICT, especially by small businesses;
  - e-Governance; and
  - Systematic and useful data collection on ICT as a tool for informed policymaking.
ADDITIONAL INFORMATION ON INTERNET USE FOR BUSINESS DEVELOPMENT

Asia-Pacific Development Information Programme.
- Provides various resources on e-governance, ICT4D, ICT for SMEs, open source software, policy notes on ICT for SMEs.  http://www.apdip.net/

BIZPRO.
- USAID-sponsored economic development project website with useful links related to SME training (including web-based training).  http://www.bizpro.org.vn

Convergence International.
- Includes policy briefs, papers, researches, and discussions on convergence of information.  http://www.convergence.org

Digital Opportunity Channel.

Europa Eurostat.
- Provides key statistics on SME development in developed countries.  http://www.epp.eurostat.ec.europa.eu

IFC-WB SME toolkit.
- Developed by IFC-WB, which offers free software, business forums, training, and more to help small businesses in emerging markets grow and succeed.  http://www.smetoolkit.org/

Infocomm Competency Programme.

International Telecommunications Union.
- Provides policy notes, articles, statistics and country reviews on telecommunications, convergence, and VoIP.  http://www.itu.org

Korean Marketplace Web Site.
- Provides information and online trading on SME products from the Republic of Korea.  http://www.gobizkorea.com

RRU World Bank.
- Provides resources on SME financing, policies, guidelines, case studies, surveys, toolkits, networking and linkages.  http://rru.worldbank.org/Themes/SmallMediumEnterprises

SMEs in Europe.
- Provides assistance to SMEs in Europe, frameworks, statistics, best practices and approaches in SME development.  http://sme.cordis.lu/home/index.cfm

Technonet Asia.
- A cooperative network of development support institutions, aiming to enhance the quality and competitiveness of the small and medium-sized enterprises in its member countries through information, technology transfer and human resources development.  http://www.idrc.ca

UNESCAP.
- http://www.unescap.org

UNDP.
UNDP Sustainable Development Networking Programme.

UNIDO SME web site.
➢ A portal dedicated in helping government and the private sector to cooperate in the design and implementation of programmes to promote the organisation and development of clusters and networks of SMEs. http://www.unido.org/doc

United Nations Information and Communications Technologies Task Force.
➢ Provides information of the implementation of the Millennium Development Goals, with a focus on ICT. http://www.unicttaskforce.org
MODULE 2: LEGISLATIVE AND POLICY OPTIONS TO PROMOTE E-COMMERCE AND EXPAND INTERNET USE

Table 1. How SMEs benefit from e-commerce processes and techniques

<table>
<thead>
<tr>
<th>Business Process</th>
<th>Sample Sub-processes</th>
<th>Examples of e-Commerce Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marketing and Sales</td>
<td>Market research – learn more about potential customers and competitors</td>
<td>Web searches; examination of competitors’ sites for information on pricing, problems, hiring, press releases, news articles;</td>
</tr>
</tbody>
</table>

I. WHY SHOULD SMES ENGAGE IN E-COMMERCE?

SMEs can benefit from a variety of e-commerce processes and techniques, as shown in the table below.

Box 6. What is Electronic Commerce, or e-Commerce?

For purposes of this module, e-commerce is broadly defined as

*Any use of information and communication technology by a business that helps it to improve its interactions with customers or suppliers.*

- Under this broad definition, it is possible for businesses in developing countries to reap significant benefits from e-commerce, even when legal, regulatory or infrastructure constraints make it difficult or impossible for them to actually *transact business* electronically. For example, a business in a developing country could use the Internet to figure out market prices for its products and use the information to compete better or win new customers. Many SMEs also gain a competitive edge by using the Internet to do market research, find information on competitors and track down leads for new customers.

- The definition also covers transactions or exchange of business-related information between:
  - Business-to-business (B2B)
  - Business-to-consumer (B2C)
  - Business-to-government (B2G).

- “Electronic commerce” is also not limited to the use of the Internet and/or web sites powered by computers. It also covers the use of mobile phones (m-commerce), VoIP, CD-ROMs and other computer applications with no telecommunications component. All of these can be and are being used in innovative ways by businesses in developing countries.

- The definition encompasses both domestic and international business. It is very important to realize that SMEs may find benefits to e-commerce to enhance their relationships with domestic customers and suppliers, and not necessarily internationally.
<table>
<thead>
<tr>
<th>Marketing techniques to reach more customers and partners</th>
<th>Website; email follow-ups; prospect database; links with other sites; electronic marketplaces; web-events; one-to-one marketing techniques; electronic newsletters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generating sales</td>
<td>Email; advertisements product catalogues; descriptions of services, credentials, current customers</td>
</tr>
<tr>
<td>Order placement</td>
<td>Electronic Transaction Processing</td>
</tr>
<tr>
<td>Payment</td>
<td>Invoicing; Electronic Transaction Processing</td>
</tr>
<tr>
<td></td>
<td>Settlement; Electronic settlement technique; third-party service</td>
</tr>
<tr>
<td>Product/Service Delivery</td>
<td>Set-up; Electronic mail, electronic transactions, shipment notification, directly or via third-party service</td>
</tr>
<tr>
<td></td>
<td>Actual delivery; For electronic goods and services, electronic transmission</td>
</tr>
<tr>
<td>Customer Service</td>
<td>Post-sales support, including add-on sales; Web-based FAQs and databases; web-forms; email; call centres</td>
</tr>
<tr>
<td>Production</td>
<td>Creating the product or service to be sold; For documents or electronic goods – web-based collaboration, document sharing, email. Computer-aided design or remote production services</td>
</tr>
<tr>
<td></td>
<td>Enhancement of an existing product or service</td>
</tr>
<tr>
<td></td>
<td>Buying materials / procurement; e-Procurement techniques including catalogue orders, auctions, requests for information</td>
</tr>
<tr>
<td>Back Office</td>
<td>Financial management; Web-based computer applications, either in-house or via third-party provider</td>
</tr>
<tr>
<td></td>
<td>Payroll/personnel</td>
</tr>
</tbody>
</table>


From a public policy perspective, the immense impact of SME fortunes or failures on the economy makes it critical for SMEs to be prepared for and take full advantage of any benefits offered by electronic commerce. Note that according to the United Nations Conference on Trade and Development, SMEs account for 60 to 70 per cent of all employment in developing countries.

e-Commerce can give SMEs a better chance to find new customers and suppliers and to compete, especially in markets that they have not easily been able to reach before – either internationally or regionally.

**II. WHAT CAN THE GOVERNMENT DO TO ENCOURAGE SMES TO ENGAGE IN E-COMMERCE?**

1. The government itself should engage in e-commerce.

In most countries, the government is one of the largest buyers of goods and services. Many governments also buy a share of their goods and services from domestic SMEs. If governments begin using e-procurement techniques to do so, it can provide an important incentive for SMEs to begin using e-commerce as well. In fact, several developing countries are now implementing or planning e-procurement projects (e.g., Chile, the Philippines, Romania and the Russian Federation).
2. The government can use ICT to provide a better and more transparent service.

Businesses turn to the government for a wide variety of services, from customs clearances to business licenses to dispute resolution mechanisms. Today, the length of time needed to obtain these services and, in some cases, the lack of transparency in the process (corruption), can and often does thwart SME efforts to compete internationally.

3. The government also provides the legal and regulatory framework and public services that can encourage, or discourage, the growth of e-commerce, and the use thereof by SMEs.

Each of these roles bring with them different sets of issues that would need to be addressed in different ways, depending on the prevailing social, political, and economic context.

This module relates to the third role of the government, and provides a brief introduction to the need for and primary rationale behind e-commerce legislation – to recognize the legal validity and enforceability of electronic documents and signatures.

III. E-COMMERCE LEGISLATION

Providing for Rules that Will Give Functional Equivalence to Electronic Signatures and Documents

A. From a Legal Perspective, What Should SMEs Be Concerned about If They Plan to Engage in e-Commerce?

The growth of e-commerce depends on the legal enforceability of electronic contracts and electronic signatures. Without such legal clarity, people and companies will and should be very hesitant to engage in electronic commerce.

Without this assurance, SMEs will not be able to fully assess the risks of doing e-business: such as whether there is a likelihood of the transaction being able to be successfully completed, whether it can be challenged, and whether the recipient will have legal recourses in such circumstances, irrespective of the location of the parties.

B. What Sort of Legal/Regulatory Regime Should Be in Place to Provide This Assurance?

The legal regime that will allow e-commerce to grow to its potential, therefore, must first and foremost be one that gives electronic transactions, contracts and signatures the same validity and enforceability as traditional transactions, contracts and signatures.

For this to happen, there must first be a mechanism that will (a) reliably and securely prove the origin, receipt and integrity of information, (b) identify the parties involved, and (c) associate those parties with the contents of the communication.

Without such a mechanism, it would be very difficult to rely on electronic contracts and electronic signatures, especially in cases where the parties have not met or do not really know each other – which would likely be the case in a globalized economy.

In other words, electronic documents and signatures must be functionally equivalent to traditional documents and signatures.

To illustrate, if Person A sends an electronic document over the Internet to Person B, ideally, Person B should be assured of the following:
(a) **Data Origin Authentication.** First, that the message really did come from Person A. That is, Person B must have some assurance that the message has in fact come from its purported sender, Person A.

(b) **Message Integrity.** Second, that the message received by Person B is the exact message that Person A sent. Person B should be able to verify that the message has not been intentionally or accidentally altered during transmission.

(c) **Non-Repudiation.** Finally, that Person A cannot later deny that he or she did in fact send the message. No one else should have been able to send the message but Person A, and Person B should be able to prove it unequivocally.

Whatever the methods or technologies used to achieve these objectives, the crucial factor is trust. The issue then, for electronic commerce, is how to build trust and confidence in electronic transactions on open networks between parties who may have no pre-existing relationship.

**C. What Are Electronic and Digital Signatures?**

“Electronic signature” generally refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document” (Philippines Republic Act 8792, or the Electronic Commerce Act of 2000).

There are many methods for creating an electronic signature. These methods range from simple ones – such as typing a name at the bottom of an email message – to more complex and secure ones – for example, biometric technologies, such as fingerprints or retinal scans.

There are yet more types of authentication methods, such as magnetic strip cards with personal identification numbers (PIN), user names and passwords, public key cryptography, writing tablets with electronic pens and even smart cards that generate a unique access code every few seconds. As technology advances, the list of viable electronic signature alternatives is sure to grow.

**D. Are Electronic Signatures the Same as Digital Signatures?**

Note that technically speaking, electronic signatures are different from digital signatures. A “digital signature” does not refer to the image of a signature in any way. Unlike both an “electronic signature” which is simply any form of mark intended to be a signature, and a “digitized signature” which refers to an electronic image of a signature, a “digital signature” is actually a term of art that refers to scrambling data in order to provide security and authentication.

Digital signatures are created and verified using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and then back into its original form.

**E. How Do Digital Signatures Work?**

Military communications have relied on encryption for thousands of years. In fact, Alexander the Great communicated with his generals by sending messages in which each letter was shifted a certain number of positions. This was a form of “secret key encryption,” i.e., anyone who knew the secret code (or key) would be able to send and receive messages securely.

Today, commercially available encryption software creates encryption so strong that it is all but impossible to break the code and ascertain the original message without the use of the authorized software.
To be secure, a secret-key coding system requires some method of distributing the secret key to intended users, without it falling into the hands of other parties.

Now, before going further into the basics of cryptographic and digital signature technology, a few terms need to be defined first.

“Encryption” is simply the process by which information is scrambled by use of a code.

A “hash function” is a process that creates a relatively small number that represents a much larger amount of electronic data. For instance, if I had a ten-page word processing document on my computer, I could use special hashing software to derive a particular number associated with that document.

If even one comma is changed on the document, the resulting hash number from the changed document would be completely different. This number is called the “message digest.”

Digital signatures use a “one-way hash function,” i.e., there is no way to reverse engineer or derive the content of the message based on the resulting message digest. When a digest is sent along with the message, the recipient can check to see if the message had been tampered with by using the same hashing software to make her own digest of the message and then checking to see if the two numbers match.

1. Public Key Cryptography

By its nature, the Internet is poorly suited for a secret-key system because it is an “open” network in which a message may make several “stops” or “hops” before arriving at its final destination.

This creates a serious risk that a third party could intercept a secret key at some point along its routing, which would allow the third party to read messages, or even send encoded messages purporting to be from the authorized holder of the key.
Physically delivering a secret key to every user through a secure channel, on the other hand, would be slow, expensive and unwieldy. It would effectively rule out one-time transactions between people and firms that have not previously exchanged secret keys.

Public key cryptography eliminates the need for users to share a secret key, which makes it ideally suited for communications over open networks such as the Internet.

In a public key system, each user has a type of software that generates two related keys, a public key and a private key. The fundamental characteristic of this pair of keys is that only this particular public key can decrypt a message encrypted with its corresponding private key and vice versa. Similarly, only this particular private key can decrypt a message encrypted with its corresponding public key.

The process is illustrated in the two diagrams below.

Let us assume that (1) an SME owner has a business proposal that he wants to digitally sign and send to you. He would then (2) run his message through one of several standard algorithms known as a “hash function” that performs a series of mathematical operations on the original message. The hash function produces a number called a (3) “message digest” which can be thought of as a fingerprint of the message, because any change in the message, no matter how slight, will cause the hash function to produce a completely different message digest. (4) Using his private key, the SME owner then encrypts the message digest. The message digest encrypted with the SME owner’s private key forms the actual (5) “digital signature” for the message. Both the digital signature and the actual message are then sent to you.

Figure 2. Sending a digitally signed message
Upon receipt of the message, your computer and software would then perform two separate operations to verify the SME owner’s identity and to determine if the message had been altered in transit.

To verify his identity, your system would (1) take the digital signature and (2) use the SME owner’s public key to decrypt the digital signature, which would then (3) produce the message digest. If the operation is successful, you would then know for a fact that the SME owner (who alone has access to his private key) must have sent the message.

In order to ensure that the message had not been altered, your system would (4) run his message through the (5) same hash function that was used, which would then (6) yield a message digest of the message. You would then be able (7) to compare the two message digests, and if they are identical, confirm that the message has remained unaltered in transit.

Generally then, users of this system would keep their private key very safe (perhaps password-protected, or even embedded in a smartcard) but they would make their public key freely available by sending it to all potential recipients of messages or posting it to an Internet public key directory.

In this way, the private key holder (in the example, the SME owner) can send a message to anyone on the Internet, and, if his public key decrypts the message, the recipient knows it must have come from the private key holder.

Conversely, anyone on the Internet who wants to send the private key holder a message can encrypt the message with his public key and send the message with the knowledge that only the private key holder can read the encrypted text.

Note that all the above processes would actually happen automatically and in the background, and you would only be made aware if something is wrong with the verification and the process reveals that there is reason to doubt the integrity of the message or sender – as in the case of credit card verification processes.

2. Public Key Infrastructures and Certification Authorities

The process of public key cryptography described above can work well between parties who know each other.

But what happens in transactions between parties who have never met each other before?
In the example above, how would you know for certain that the SME owner, and not someone else posing as him, did in fact send the message?

In general terms, how can one bind the identity of a particular party to a particular public key? This need has been widely perceived in the marketplace, and several companies are stepping into the so-called “trusted third party” business. Such a company is known as a “certification authority” (CA).

The CA essentially vouches for the identity of a person who subscribes to their service. It issues a certificate that, in effect, guarantees the identity of the person (or subscriber) associated with a given public key. The CA is responsible for undertaking certain measures to ascertain the identity of the person to whom it issues a certificate. The certificate issued by the CA:

- Identifies the CA issuing it;
- Identifies the subscriber;
- Contains the subscriber’s public key; and
- Is digitally signed with the CA’s private key.

The digital certificate may also contain additional information, including a reliance limit, or a reference to the CA’s “certification practice statement” that gives relying parties notices of the level of inquiry conducted by the CA before issuing the certificate.

Thus, if the SME owner wished to use a CA to vouch for his identity on the Internet, he would have to present the CA with a copy of his public key along with sufficient proof of his identity (or else the CA could also issue his private and public keys). Once satisfied with the identity of the SME owner, the CA would issue him a digital certificate.

Going back to our example, and as shown in the diagram below, the SME owner will send you, along with his digital signature, a copy of his digital certificate.

In addition to the steps described above, upon receipt of the message, you may also confirm with the CA identified in the digital certificate that the sender is who he says he is, and that his certificate has not expired or been revoked.

Again, note that all these activities would be happening in the background, and nearly instantaneously, such that you may not even be aware, or might take for granted, that all these verification processes are actually happening.
Figure 4. Certificate authorities, digital certificates and digitally signed messages
F. A Note on the Concept of “Technological Neutrality”

One key issue that often arises when governments attempt to make rules related to the Internet is the question of technological neutrality. That is, when crafting laws or rules, governments must be aware that their actions could have an effect on the development of technology itself to the extent that the laws or rules they craft encourage or discourage use of, or investments in, particular technologies.

The subject of electronic authentication presents a good example.

Rule-makers are more confident in the security and reliability of known electronic authentication methods (such as public key infrastructures). This confidence allows them greater room to grant legal benefits and presumptions to the use of those techniques. They are generally less willing to grant the same level of legal benefits to as yet unknown techniques or to technologies that are not as well known or used.

G. Should the Government Formally Endorse the Validity of Digital (or PKI) Signatures?

1. The arguments for formally recognizing the validity of PKI signatures

Advocates of legislation to govern CAs argue that laws and rules are needed to address a number of key issues even before such signatures are widely used. First, digital signatures must be given the same legal force as traditional signatures. Second, CAs need to be licensed, or at least regulated by the State, to ensure that they are technically proficient, financially sound and operationally secure. And finally, legislation is needed to shield CAs from potentially crippling liability if they have complied with the requirements set by law.

Moreover, they believe that pro-active rule-making is preferable to allowing the validity of digital signatures to be determined by the evolution of technical standards or business practices in the market. Legislation would produce uniformity among different jurisdictions, whereby they argue, not only domestically, but internationally as well. With such a legal infrastructure in place, they believe electronic commerce will gain a broader acceptance because parties to online transactions will be able to use digital signatures that are not only secure, but are also legally enforceable.

2. The arguments against CA legislation/rules

Critics of the legislation point out that prescriptive, technology-specific legislation runs the risk of distorting the market, thus preventing the natural evolution of best business practices, technological innovations and competitive pricing. Many observers believe that detailed statutory and regulatory treatment is simply inappropriate in an infant industry undergoing rapid change.

They also point out that the non-regulatory environment of the Internet allowed it to evolve solely in response to advances in technology, the creativity of providers and the needs of users, rather than in conformance with detailed strictures laid down by government bureaucrats. Freed from government mandates, producers and consumers were able to quickly and easily adapt to new technologies and business models. This was the dynamic that caused such an explosive growth in the Internet and it should not be ignored by policymakers when they consider the best ways to promote electronic commerce and/or authentication.

Furthermore, particularly following the events of 9/11, there has been a growing recognition that other means of electronic authentication, including biometrics and voice authentication, may take on equal or even greater importance in the years ahead. In fact, some of these techniques – and particularly, those that are based on biometric features – may prove to be more reliable and less susceptible to compromise than digital signatures.
The danger then is that specific rules for public key infrastructures could in effect be seen as an endorsement of a specific technological option. This legislative or state-sanctioned endorsement could have the unintended effect of stunting the development of other authentication mechanisms.
Box 7. Case Study: The Document Hub

The Development Bank of the Philippines (DBP) in a partnership with a local company called Smetrix proposed an online trading system for SMEs.

This online e-trade finance marketplace is intended to provide SMEs with rapid and less costly access to credit by taking advantage of ICT, and more particularly secure and reliable digital authentication procedures.

Central to this approach was the proprietary Implementation Document Hub system, which enables the creation and verification of legally enforceable trade documents in a digital form. The clearing house permits SMEs to have their online receivables discounted, or to receive structured finance (handling the risk of a given transaction) from a participating bank, or to securitize those receivables, capitalizing on the higher corporate rating grades of their major trading partners.

In simple terms, this means that because of the system, SMEs will have access to much-needed capital faster (from the two to four weeks it takes banks to verify and rediscount their receivables to as little as two days), and at lower cost (by some estimates as much as 12 percentage points less in interest).

A major technology provider has been selected to support digital warehousing of the trade documents as well as interfaces with payment systems, while an international bank plays the role of the central registry for the originated trade receivables/securities. A major Philippine multinational has also agreed to be the first user by bringing its trading community into the marketplace.

It is anticipated that when the transaction history of the SMEs is built up, the information could be the starting basis for the online credit evaluation system for the SME receivables.

Note: Even with all the systems and technologies in place, the Document Hub would have been useless and could not have got off the ground without the laws and rules that formally recognized digital documents and signatures as legally valid and enforceable.
SUMMARY: MODULE 2 IN A NUTSHELL

- Electronic commerce, or e-commerce, is broadly defined as any use of information and communications technology by a business that helps it to improve its interactions with customers and suppliers.

- What can the government do to encourage SMEs to engage in e-commerce?
  - The government itself should engage in e-commerce;
  - The government can use ICT to provide better and more transparent services; and;
  - The government can provide the legal and regulatory framework to encourage the growth of e-commerce, and the use thereof by SMEs.

- The growth of e-commerce depends on the legal enforceability of electronic contracts and electronic signatures. Without such legal clarity, people and companies will be very hesitant to engage in e-commerce.

- There are many ways of creating electronic signatures, ranging from the simple ones – such as typing one’s name at the end of an e-mail message – to the more sophisticated, such as public key infrastructures and biometric technologies.

- The important thing is that electronic documents and signatures must be functionally equivalent to their traditional counterparts.

- When crafting laws or rules, governments must be aware that their actions could have an effect on the development of technology itself. As a general rule, therefore, they must remain technology neutral.
ADDITIONAL INFORMATION ON LEGISLATIVE AND POLICY OPTIONS TO PROMOTE E-COMMERCE AND EXPAND INTERNET USE

Asia-Pacific Development Information Programme.
- Provides various resources on e-governance, ICT4D, ICT for SMEs, open source software, policy notes on ICT for SMEs.  [http://www.apdip.net/]

Asia-Pacific Economic Cooperation (APEC) Electronic Commerce Steering Group.
- Useful for development professionals in the Asia-Pacific region, keeping them up to date on issues and progress related to electronic commerce.  [http://www.ita.doc.gov/td/industry/otea/ecommerce/apec/]

BIZPRO.
- USAID-sponsored economic development project website with useful links related to SME training (including web-based training).  [http://www.bizpro.org.ua]

Bridges.org.
- Reports and analyses, training material and guides, and statistics, including online resources for ICT training.  [http://www.bridges.org/]

Digital signatures.


e-Commerce legislation and regulatory regime.

e-Marketplace Services.
- Contains reports, articles, case studies. Focused on helping SMEs understand and use e-marketplaces.  [http://www.emarketservices.com/]

EMPREC, UNCTAD’s programme to promote the sustainability of small and medium-sized enterprises.
- Provides information on general business training to SMEs and provides an Electronic Trade Opportunity capability.  [http://www.empretec.net/]

IFC-WB SME toolkit.
- Developed by IFC-WB which offers free software, business forms, training, and more to help small businesses in emerging markets grow and succeed.  [http://www.smetoolkit.org/]

International Financial Corporation programme for SMEs.
- Provides statistics on SME development and activities in Asia. Includes framework and approaches in developing and assisting SMEs.  [http://www.ifc.org/sme]

News@SEI.
Philippine SME statistics.

Philippine SME portal.
- Provides resources on how to establish an SME in the Philippines; includes business, management and accounting tools and a guide to government requirements for SMEs. http://www.sme.com.ph

Public Key Infrastructures and Certification Authorities.
- Information on PKI and CA laws, CA licenses, regulations, definitions, statistics, and issues. Also hosts links to various websites on PKI and CA. http://www.pki-page.org/

OECD SME portal.

SME for development.
- A portal of resources of SME development, including forums for discussions, policy articles, and research on ICT technology for SMES. http://www.sme.com

UNESCAP.
- www.unescap.org

UNIDO SME web site.
- A portal dedicated in helping governments and the private sector to cooperate in the design and implementation of programmes to promote the organization and development of clusters and networks of SMEs. http://www.unido.org/doc
MODULE 3: CYBER CRIME AND SECURITY

The huge potential for e-business brings with it a dark side that SMEs – and policymakers – should not ignore. Just as the Internet opens opportunities for entrepreneurs and SMEs to engage in e-commerce and transact with ever growing numbers of clients, so too does it create chances for mischief or worse damage.

Just as in the “real” world, there are those who would exploit the Internet for their own selfish interests. This type of conduct makes users vulnerable to a host of possible attacks that compromise the confidentiality, integrity and availability of information that they exchange through the Internet. As a result of such illicit activities, people tend to lose trust on the security of doing business in the Internet and thus forego its huge potential for business, as well as its potential as a tool to promote social justice and equality.

It is therefore necessary that security measures be set in place to thwart would-be attackers who make Internet use unsafe and insecure. Along this line, it becomes of paramount import to establish mechanisms about the standards, policies, rules, and enforcement and dispute resolution procedures to apply to global internetworking activities in order to make the Internet free, fair, reliable, transparent and accessible to all.

e-Commerce can never prosper unless a secured environment for doing business exists. But this can only happen if the correct policies for securing the Internet are put in place.

This is especially true for developing countries. As the level of technological sophistication needed to penetrate (and deter such penetration of) networks in developed countries continues to rise, would-be attackers are shifting their focus to networks found in developing countries. In many cases, developing countries do not yet possess a general awareness of security issues, much less the legal and regulatory issues, nor the technical capability to effectively deter cyber threats.

Is your country equipped to deal with cyber crime, and if not, how is this lack of capability affecting your country’s ability to attract investments and encourage Internet use for business development?

I. INCIDENTS/ATTACKS – TRENDS AND INTERNET GROWTH

The same technology that allows us to block spam and set firewalls to prevent unauthorized access to our networks is also available to unscrupulous individuals who manipulate the same technology in order to find cracks in the system that allow them access.

Moreover, the tools available to launch an attack have become more effective, easier to use, and more accessible even to people without an in-depth knowledge of computer systems. Then, too, sophisticated programmers intent on online mischief often embed an attack procedure in their programs and widely distribute the same to the intruder community. Thus, people who have the desire but not the technical skill are increasingly able to break into systems.

Below is a list of observable trends in Internet attacks listed in the Open Regional Dialogue on Internet Governance research paper “Network Stability and Security”.

Trend 1 – Automation; speed of attack tools
The level of automation in attack tools continues to increase. Automated attacks commonly involve four phases, each of which is changing.

- Scanning for potential victims. Widespread scanning has been common since 1997. Today, scanning tools are using more advanced scanning patterns to maximize impact and speed.

- Compromising vulnerable systems. Previously, vulnerabilities were exploited after a widespread scan was complete. Now, attack tools exploit vulnerabilities as a part of the scanning activity, which increases the speed of propagation.

- Propagate the attack. Before 2000, attack tools required a person to initiate additional attack cycles. Today, attack tools can self-initiate new attack cycles. We have seen tools like Code Red and Nimda self-propagate to a point of global saturation in less than 18 hours.

- Coordinated management of attack tools. Since 1999, with the advent of distributed attack tools, attackers have been able to manage and coordinate large numbers of deployed attack tools distributed across many Internet systems. Today, distributed attack tools are capable of launching denial of service attacks more efficiently, scanning for potential victims and compromising vulnerable systems. Coordination functions now take advantage of readily available, public communications protocols such as Internet Relay Chat (IRC) and instant messaging (IM).

**Trend 2 – Increasing sophistication of attack tools**

Attack tool developers are using more advanced techniques than previously. Attack tool signatures are more difficult to discover through analysis and more difficult to detect through signature-based systems such as antivirus software and intrusion detection systems. Three important characteristics are the anti forensic nature, dynamic behaviour, and modularity of the tools.

- Anti-forensics. Attackers use techniques that obfuscate the nature of attack tools. This makes it more difficult and time-consuming for security experts to analyze new attack tools and to understand new and rapidly developing threats. Analysis often includes laboratory testing and reverse engineering.

- Dynamic behaviour. Early attack tools performed attack steps in single defined sequences. Today’s automated attack tools can vary their patterns and behaviour based on random selection, predefined decision paths, or through direct intruder management.

- Modularity of attack tools. Unlike early attack tools that implemented one type of attack, tools now can be changed quickly by upgrading or replacing portions of the tool. This causes rapidly evolving attacks and, at the extreme, polymorphic tools that self-evolve to be different in each instance. In addition, attack tools are more commonly being developed to execute on multiple operating system platforms.

As an example of the difficulties posed by sophisticated attack tools, main common tools use protocols like IRC or HTTP (Hypertext Transfer Protocol) to send data or commands from the intruder to compromised hosts. As a result, it has become increasingly difficult to distinguish attack signatures from normal, legitimate network traffic.

**Trend 3 – Faster discovery of vulnerabilities**

The number of newly discovered vulnerabilities reported to the CERT Coordination Centre (CERT/CC) continues to more than double each year. It is difficult for administrators to keep up to date with patches. Additionally, new classes of vulnerabilities are discovered each year. Subsequent reviews of existing code for examples of the new vulnerability class often lead over time to the discovery of examples in hundreds of different software products. Intruders are often able to discover these exemplars before the vendors are able to correct them. Because of the trend toward the automated discovery of new vulnerabilities in technologies, the so-called “time to patch” is becoming increasingly small.
Table 2. Vulnerabilities reported by CERT/CC

<table>
<thead>
<tr>
<th>Year</th>
<th>1995-1999</th>
<th>2000-2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities</td>
<td>171</td>
<td>345</td>
</tr>
</tbody>
</table>

Total vulnerabilities reported (1995 - Q2, 2006): 26,713.

Trend 4 – Increasing permeability of firewalls

Firewalls are often relied upon to provide primary protection from intruders. However, they are not as secure as before:

- Technologies are being designed to bypass typical firewall configurations, for example, IPP (the Internet Printing Protocol) and WebDAV (Web-based Distributed Authoring and Versioning).
- Some protocols marketed as being “firewall friendly” are, in reality, designed to bypass typical firewall configurations.
- Certain aspects of “mobile-code” (ActiveX controls, Java, and JavaScript) make it difficult for vulnerable systems to be protected and for malicious software to be discovered.

Trend 5 – Increasingly asymmetric threats

Security on the Internet is, by its very nature, highly interdependent. Each Internet system’s exposure to attack depends on the state of security of the rest of the systems attached to the global Internet. Owing to advances in attack technology, a single attacker can relatively easily employ a large number of distributed systems to launch devastating attacks against a single victim. As the automation of deployment and the sophistication of attack tool management both increase, the asymmetric nature of the threat will continue to grow.

Trend 6 – Increasing threat from infrastructure attacks

Infrastructure attacks are attacks that broadly affect key components of the Internet. They are of increasing concern because of the number of organizations and users on the Internet and their increasing dependency on the Internet to carry out day-to-day business. Four types of infrastructure attacks are briefly described below.

Attack 1 – Distributed denial of service

Denial-of-service attacks use multiple systems to attack one or more victim systems with the intent of denying service to legitimate users of the victim systems. The degree of automation in attack tools enables a single attacker to install the tools and control tens of thousands of compromised systems for use in attacks. Intruders often search address blocks known to contain high concentrations of vulnerable systems with high-speed connections. Cable modem, digital subscriber lines (DSL), and university address blocks are increasingly targeted by intruders planning to install their attack tools. Denial-of-service attacks are effective because the Internet is comprised of limited and consumable resources, and Internet security is highly interdependent.

Attack 2 – Worms

A worm is self-propagating malicious code. Unlike a virus, which requires a user to do something to continue the propagation, a worm can propagate by itself. The highly-automated nature of the worms coupled with the relatively widespread nature of the vulnerabilities they exploit allows a
large number of systems to be compromised within a matter of hours. (Code Red infected more than 250,000 systems in just 9 hours on July 19, 2001.)

Some worms include built-in denial-of-service attack payloads (Code Red) or website defacement payloads (sadmind/IIS, Code Red); and others have dynamic configuration capabilities (W32/Leaves). However, the biggest impact of these worms is that their propagation effectively creates a denial of service in many parts of the Internet because of the huge amounts of scan traffic generated. They also cause much collateral damage (examples include DSL routers that crash; cable modem ISPs whose networks are completely overloaded, not by the scanning itself but by the burst of underlying network management; traffic that the scanning triggers; and printers that crash or print reams of junk output).

Attack 3 – Attacks on the Internet Domain Name System
The Internet Domain Name System (DNS) is the distributed, hierarchical global directory that translates names (www.example.com) to numeric IP addresses (192.168.13.2). The top two layers of the hierarchy are critical to the operation of the Internet. In the top layer are 13 "root" name servers. Next are the "top-level domain" (TLD) servers, which are authoritative for ".com", ".net" and others, as well as the country code top level domains (ccTLDs – ".us", ".uk", ".ru" and so forth.)

Threats to the Domain Name System:

1. Cache poisoning. If DNS is made to cache bogus information, the attacker can redirect traffic intended for a legitimate site to a site under the attacker’s control. A recent survey by CERT/CC shows that over 80 per cent of the TLD domains are running on servers that are potentially vulnerable to this form of attack.

2. Compromised data. Attackers compromise vulnerable DNS servers, giving them the ability to modify the data served to users. Many of the TLD servers run a software program called BIND, in which vulnerabilities are discovered regularly. A CERT/CC survey indicates that at least 20 per cent of TLD domains are running on vulnerable servers; another 70 per cent are "status unknown".

3. Denial of service. A large denial-of-service attack on some of the name servers for a TLD (for example, ".com") could cause widespread Internet slowdowns or effective outages.

4. Domain hijacking. By leveraging insecure mechanisms used by customers to update their domain registration information, attackers can co-opt the domain registration processes to take control of legitimate domains.

Attack 4 – Attacks against or using routers
Routers are specialized computers that direct traffic on the Internet (similar to mail routing facilities in the postal service). Threats fall into the following categories:

- Routers as attack platforms. Intruders use poorly secured routers as platforms for generating attack traffic at other sites, for scanning or reconnaissance.

- Denial of service. Although routers are designed to pass large amounts of traffic through them, they often are not capable of handling the same amount of traffic directed at them. (Think of it as the difference between sorting mail and reading it.) Intruders take advantage of this characteristic attacking the routers that lead into a network rather than attacking the systems on the network directly.

- Exploitation of trust relationship between routers. For routers to do their jobs, they have to know where to send the traffic they receive. They do this by sharing routing information between them, which requires the routers to trust the information they receive from their peers.

As a result of these vulnerabilities, it would be relatively easy for an attacker to modify, delete, or inject routes into the global Internet routing tables to redirect traffic destined for one network to
another, effectively causing a denial of service to both (one because no traffic is being routed to them, and the other because they are getting more traffic than they should). Although the technology has been widely available for some time, many networks (Internet service providers and large corporations) do not protect themselves with the strong encryption and authentication features available on the routers.
II. INCIDENTS/ATTACKS – THEIR SOURCES AND TYPES

The following diagram describes the sources of threats.

![Vulnerabilities Diagram]

---

Incidents can be broadly classified into several kinds: the probe, scan, account compromise, root compromise, packet sniffer, denial of service, exploitation of trust, malicious code, and Internet infrastructure attacks.

1. **Probe**
   A probe is characterized by unusual attempts to gain access to a system or to discover information about the system. One example is an attempt to log in to an unused account. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry. Probes are sometimes followed by a more serious security event, but they are often the result of curiosity or confusion.

2. **Scan**
   A scan is simply a large number of probes done using an automated tool. Scans can sometimes be the result of a misconfiguration or other errors. Nonetheless, they are often a prelude to a more directed attack on systems that the intruder has found to be vulnerable.

3. **Account Compromise**
   An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges (privileges a system administrator or network manager has). An account compromise might expose the victim to serious data loss, data theft or theft of services. The lack of root-level access means that the damage can usually be contained, but a user-level account is often an entry point for greater access to the system.

4. **Root Compromise**
   A root compromise is similar to an account compromise, except that the account that has been compromised has special privileges on the system. The term root is derived from an account on UNIX systems that typically has unlimited, or "super-user" privileges. Intruders who succeed in a root compromise can do just about anything on the victim’s system, including run their own programs, change how the system works, and hide traces of their intrusion.

5. **Packet Sniffer**
   A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travel...
over the network in clear text. With perhaps hundreds or thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require privileged access. For most multi-user systems, however, the presence of a packet sniffer implies there has been a root compromise.

6. Denial of Service
The goal of denial-of-service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial-of-service attack can come in many forms. Attackers may “flood” a network with large volumes of data or deliberately consume scarce or limited resources, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data.

7. Exploitation of Trust
Computers on networks often have trust relationships with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.

8. Malicious Code
Malicious code is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious code includes Trojan horses, viruses and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of security incidents.

9. Internet Infrastructure Attacks
These rare but serious attacks involve key components of the Internet infrastructure rather than specific systems on the Internet. Examples are network name servers, network access providers, and large archive sites on which many users depend. Widespread automated attacks can also threaten the infrastructure. Infrastructure attacks affect a large portion of the Internet and can seriously hinder the day-to-day operation of many sites.

III. LEGISLATIVE AND POLICY CONSIDERATIONS IN EFFORTS TO ADDRESS CYBER CRIME AND SECURITY ISSUES

Is there a need to establish laws, policies or rules to govern cyber crime and security issues?

<table>
<thead>
<tr>
<th>Country</th>
<th>Law(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>CRIMES ACT 1914 (PART VIA), Sections 76B, 76D</td>
</tr>
<tr>
<td>Austria</td>
<td>Privacy Act 2000 (effective as of January 1, 2000)</td>
</tr>
<tr>
<td>Belgium</td>
<td>The Belgian Parliament in November 2000 adopted new articles in the Criminal Code (effective from 13 February 2001) Article 550(b)</td>
</tr>
<tr>
<td>Brazil</td>
<td>Law no. 9.983 of 14 July 2000, Art. 313-A &amp; B</td>
</tr>
<tr>
<td>Canada</td>
<td>Canadian Criminal Code Section 342.1</td>
</tr>
<tr>
<td>Chile</td>
<td>Law on Automated Data Processing Crimes no. 19.223, published 7 June 1993</td>
</tr>
<tr>
<td>Country</td>
<td>Legal Reference</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hong Kong, China</td>
<td>Telecommunication Ordinance</td>
</tr>
<tr>
<td>Denmark</td>
<td>Penal Code (Section 263)</td>
</tr>
<tr>
<td>Estonia</td>
<td>Estonian Criminal Code (Sections 269 to 273)</td>
</tr>
<tr>
<td>Finland</td>
<td>Penal Code Chapter 38 (Section 8)</td>
</tr>
<tr>
<td>France</td>
<td>New Penal Code, in effect since 1 March 1993 Chapter III (Articles 323-1 to 323-4)</td>
</tr>
<tr>
<td>Germany</td>
<td>Penal Code Section 202a, 303a, Section 303b</td>
</tr>
<tr>
<td>Greece</td>
<td>Criminal Code Article 370C§2</td>
</tr>
<tr>
<td>Hungary</td>
<td>Penal Code (Section 300 C)</td>
</tr>
<tr>
<td>Ireland</td>
<td>Criminal Damage Act, 1991</td>
</tr>
<tr>
<td>Iceland</td>
<td>Penal Code (§ 228 Section 1)</td>
</tr>
<tr>
<td>India</td>
<td>Information Technology Act 2000 (No. 21 of 2000)</td>
</tr>
<tr>
<td>Israel</td>
<td>The Computer Law of 1995,</td>
</tr>
<tr>
<td>Italy</td>
<td>Penal Code (Article 615)</td>
</tr>
<tr>
<td>Latvia</td>
<td>The Criminal Law (Section 241)</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>The Act of 15 July 1993, relating to the reinforcement of the fight against financial crime and computer crime</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Computer Crimes Act 1997</td>
</tr>
<tr>
<td>Malta</td>
<td>ELECTRONIC COMMERCE ACT (Sections 337 (C) (1) to 337 (F) (1)</td>
</tr>
<tr>
<td>Mauritius</td>
<td>Information Technology (Miscellaneous Provision) Act 1998 (Act No. 18 of 1998), Penal Code (Section 369A)</td>
</tr>
<tr>
<td>Mexico</td>
<td>Penal Code Part 9 (Chapter II)</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Criminal Code (Article 138a)</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Crimes Amendment (No. 6) Bill is introduced (Section 305ZE &amp; 305ZF)</td>
</tr>
<tr>
<td>Norway</td>
<td>Penal Code (§ 145, 151 b, § 261 &amp; § 291)</td>
</tr>
<tr>
<td>Pakistan</td>
<td>Electronic Transactions Ordinance 2002</td>
</tr>
<tr>
<td>Poland</td>
<td>Penal Code (Article 267 to 269)</td>
</tr>
<tr>
<td>Portugal</td>
<td>Criminal Information Law of 17 August 1991</td>
</tr>
<tr>
<td>Philippines</td>
<td>Republic Act No. 8792, or the e-Commerce Law</td>
</tr>
<tr>
<td>Singapore</td>
<td>Computer misuse Act</td>
</tr>
<tr>
<td>Sweden</td>
<td>The Data Act of 1973 (amendments in 1986 and 1990)</td>
</tr>
<tr>
<td>Switzerland</td>
<td>Penal Code (Article 143bis)</td>
</tr>
<tr>
<td>Turkey</td>
<td>Penal Code (Section 525/a)</td>
</tr>
<tr>
<td>United Kingdom of Great Britain And Northern Ireland</td>
<td>Computer Misuse Act 1990</td>
</tr>
<tr>
<td>Venezuela</td>
<td>SPECIAL STATUTE AGAINST COMPUTER RELATED CRIMES (Published in Official Gazette of Bolivarian Republic of Venezuela, 30 October 2001)</td>
</tr>
</tbody>
</table>

Do existing laws support the preservation and use of electronic evidence of cyber crimes? Is procedural law aligned with substantive law? What challenges face cyber crime enforcers?
Note the challenges to international as well as State prosecution of cyber crimes, as classified by the United States Department of Justice:

- **Technological challenges** – While it is possible to trace an electronic trail, the task has become very difficult because of the skill and technology that allow near-absolute anonymity for the cyber-culprit.

- **Legal challenges** – Laws and other legal tools to combat crime lag behind the rapid changes afforded by technology.

- **Resource challenges** – These refer to the problem of lack of sufficient experts or the lack of adequate budget for new technologies as well as for the training of personnel.

**Innovative practices for combating cyber crime can be found everywhere. Here are a few:**

- In Japan, the 2005 “Antiphishing Japan” campaign was launched to protect consumers against fraudsters using a fake website to get credit card details.

- Similarly, in the fall of 2005, the United States Federal Trade Commission and public and private sector partners launched “OnGuard Online”, a multimedia and interactive consumer education campaign to help consumers stay safe online. The comprehensive website of the campaign, available in both English and Spanish, uses straightforward, plain-language materials to help computer users be on guard against Internet fraud and secure their computers and to protect their personal information.

- In Austria, videos were shown in 2004 on information screens in underground railway stations to inform consumers about the Internet, indebtedness and prize draws.

The transnational nature of cyber-crimes requires international cooperation on laws and jurisdiction. International cooperation is important because cyber crimes do not respect State, sovereign or national borders.

- The 41-nation Council of Europe approved a convention on cyber crime. The treaty provides for the coordinated criminalization of the following:
  - Offences against the confidentiality, integrity and availability of computer data and systems, such as illegal access, illegal interception, data or system interference, and illegal devices;
  - Computer-related offences like computer-related forgery and computer-related fraud;
  - Content-related offences like child pornography; and
  - Copyright-related offences.

The treaty also urges its members to enter into cooperative efforts, through mutual assistance, extradition agreements and other measures, in order to combat cyber crime.

- Similarly, the Asia Pacific Economic Cooperation (APEC) has endorsed the following action items to combat the growing threat of cyber crime:
  - Immediate enactment of substantive, procedural and mutual assistance laws to cyber security;
  - Making cyber crime laws as comprehensive as those proposed in the Council of Europe Cyber Crime Convention;
  - Assistance between and among economies in developing threat and vulnerability assessment capabilities;
  - Security and technical guidelines that can be used by governments and corporations in their fight against cyber crime; and
  - Outreach programmes to economies and consumers regarding cyber security and cyber ethics. This year, APEC has embarked on a project that aims to train judges and prosecutors in handling cyber crime cases. This is aimed at familiarizing the
legal system with the nuances of cyber crime so that more successful prosecutions may happen.

- In the Association of South-East Asian Nations (ASEAN), member countries have agreed to create an ASEAN Network Security Coordination Centre that will help combat cyber crimes and cyber terrorism. Computer emergency response teams have also been established in each ASEAN country to serve as early warning systems against viruses and illegal network intrusions. ASEAN CERTs Incident Drills (ACID) have been conducted to test the preparedness of the various CERTs.

- An excellent example of collaboration in the effort to enhance network security and address cyber crimes is the Asia-Pacific Computer Emergency Response Team. Its mission in the Asia-Pacific Region involves the following activities:
  - Enhance regional and international cooperation on information security,
  - Jointly develop measures to deal with large-scale or regional network security incidents,
  - Facilitate information sharing and technology exchange, including information security, computer virus and malicious code among its members,
  - Promote collaborative research and development on subjects of interest to its members,
  - Assist other CERTs in the region to conduct efficient and effective computer emergency response, and
  - Provide inputs and recommendations to help address legal issues related to information security and emergency response across regional boundaries.
ANNEX: TIPS ON HOW TO AVOID BECOMING A VICTIM OF A CYBER CRIME

Auction Fraud
- Before you bid, contact the seller with any questions you have.
- Review the seller's feedback.
- Be cautious when dealing with individuals outside of your own country.
- Ensure you understand refund, return and warranty policies.
- Determine the shipping charges before you buy.
- Be wary if the seller only accepts wire transfers or cash.
- If an escrow service is used, ensure it is legitimate.
- Consider insuring your item.
- Be cautious of unsolicited offers.

Counterfeit Cashier's Check
- Inspect the cashier's check.
- Ensure the amount of the check matches in figures and words.
- Check to see that the account number is not shiny in appearance.
- Be watchful that the drawer's signature is not traced.
- Official checks are generally perforated on at least one side.
- Inspect the check for additions, deletions, or other alterations.
- Contact the financial institution on which the check was drawn to ensure legitimacy.
- Obtain the bank's telephone number from a reliable source, not from the check itself.
- Be cautious when dealing with individuals outside of your own country.

Credit Card Fraud
- Ensure that the site is secure and reputable before providing your credit card number online.
- Do not trust the site just because it claims to be secure.
- If purchasing merchandise, ensure it is from a reputable source.
- Promptly reconcile credit card statements to avoid unauthorized charges.
- Do your research to ensure legitimacy of the individual or company.
- Beware of providing credit card information when requested through unsolicited emails.

Debt Elimination
- Know who you are doing business with – do your research.
- Obtain the name, address and telephone number of the individual or company.
- Research the individual or company to ensure they are authentic.
- Contact the Better Business Bureau to determine the legitimacy of the company.
- Be cautious when dealing with individuals outside of your own country.
- Ensure you understand all terms and conditions of any agreement.
- Be wary of businesses that operate from P.O. boxes or mail drops.
- Ask for names of other customers of the individual or company and contact them.
- If it sounds too good to be true, it probably is.

DHL and UPS
- Beware of individuals using the DHL or UPS logo in any email communication.
- Be suspicious when payment is requested by money transfer before the goods will be delivered.
- Remember that DHL and UPS do not generally get involved in directly collecting payment from customers.
- Fees associated with DHL or UPS transactions are only for shipping costs and never for other costs associated with online transactions.
- Contact DHL or UPS to confirm the authenticity of email communications received.

Employment/Business Opportunities
- Be wary of inflated claims of product effectiveness.
- Be cautious of exaggerated claims of possible earnings or profits.
• Beware when money is required up front for instructions or products.
• Be leery when the job posting claims "no experience necessary".
• Do not give your social security number when first interacting with your prospective employer.
• Be cautious when dealing with individuals outside of your own country.
• Be wary when replying to unsolicited emails for work-at-home employment.
• Research the company to ensure they are authentic.
• Contact the Better Business Bureau to determine the legitimacy of the company.

Escrow Services Fraud
• Always type in the website’s address yourself rather than clicking on a link provided.
• A legitimate website will be unique and will not duplicate the work of other companies.
• Be leery when a site requests payment to an "agent", instead of a corporate entity.
• Be leery of escrow sites that only accept wire transfers or e-currency.
• Be watchful of spelling errors, grammar problems, or inconsistent information.
• Beware of sites that have escrow fees that are unreasonably low.

Identity Theft
• Ensure web sites are secured prior to submitting your credit card number.
• Do your homework to ensure the business or web site is legitimate.
• Attempt to obtain a physical address, rather than a P.O. box or mail drop.
• Never throw away credit card or bank statements in usable form.
• Be aware of missed bills which could indicate your account has been taken over.
• Be cautious of scams requiring you to provide your personal information.
• Never give your credit card number over the phone unless you make the call.
• Monitor your credit statements monthly for any fraudulent activity.
• Report unauthorized transactions to your bank or credit card company as soon as possible.
• Review a copy of your credit report at least once a year.

Internet Extortion
• Security needs to be multilayered so that numerous obstacles will be in the way of the intruder.
• Ensure that security is installed at every possible entry point.
• Identify all machines connected to the Internet and assess the defence that is engaged.
• Identify whether your servers are utilizing any ports that have been known to represent insecurities.
• Ensure you are utilizing the most up-to-date patches for your software.

Investment Fraud
• If the "opportunity" appears too good to be true, it probably is.
• Beware of promises to make fast profits.
• Do not invest in anything unless you understand the deal.
• Do not assume a company is legitimate based on the "appearance" of the website.
• Be leery when responding to investment offers received through unsolicited e-mails.
• Be wary of investments that offer high returns at little or no risk.
• Independently verify the terms of any investment that you intend to make.
• Research the parties involved and the nature of the investment.
• Be cautious when dealing with individuals outside of your own country.
• Contact the Better Business Bureau to determine the legitimacy of the company.

Lotteries
• If the lottery winnings appear too good to be true, they probably are.
• Be leery when dealing with individuals outside of your own country.
• Be leery if you do not remember entering a lottery or contest.
• Be cautious if you receive a telephone call stating you are the winner in a lottery.
• Beware of lotteries that charge a fee prior to delivery of your prize.
• Be wary of demands to send additional money to be eligible for future winnings.
• It is a violation of federal law to play a foreign lottery via mail or telephone.
Nigerian Letter or "419"
- If the "opportunity" appears too good to be true, it probably is.
- Do not reply to e-mails asking for personal banking information.
- Be wary of individuals representing themselves as foreign government officials.
- Be cautious when dealing with individuals outside of your own country.
- Beware when asked to assist in placing large sums of money in overseas bank accounts.
- Do not believe the promise of large sums of money for your cooperation.
- Guard your account information carefully.
- Be cautious when additional fees are requested to further the transaction.

Phishing and Spoofing
- Be suspicious of any unsolicited e-mail requesting personal information.
- Avoid filling out forms in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link that you are actually directed to.
- Log on to the official web site, instead of "linking" to it from an unsolicited email.
- Contact the actual business that supposedly sent the e-mail to verify if the email is genuine.

Ponzi or Pyramid
- If the "opportunity" appears too good to be true, it probably is.
- Beware of promises to make fast profits.
- Exercise diligence in selecting investments.
- Be vigilant in researching with whom you choose to invest.
- Make sure you fully understand the investment prior to investing.
- Be wary when you are required to bring in subsequent investors.
- Independently verify the legitimacy of any investment.
- Beware of references given by the promoter.

Re-shipping
- Be cautious if you are asked to ship packages to an "overseas home office".
- Be cautious when dealing with individuals outside of your own country.
- Be leery if the individual states that his country will not allow direct business shipments from the United States.
- Be wary if the "ship to" address is yours but the name on the package is not.
- Never provide your personal information to strangers in a chat-room.
- Do not accept packages that you did not order.
- If you receive packages that you did not order, either refuse them upon delivery or contact the company where the package is from.

Spam
- Do not open spam. Delete it unread.
- Never respond to spam, as this will confirm to the sender that it is a "live" email address.
- Have a primary and secondary e-mail address – one for people you know and one for all other purposes.
- Avoid giving out your e-mail address unless you know how it will be used.
- Never purchase anything advertised through an unsolicited e-mail.

Third-Party Receiver of Funds
- Do not agree to accept and wire payments for auctions that you did not post.
- Be leery if the individual states that his country makes receiving these types of funds difficult.
- Be cautious when the job posting claims "no experience necessary".
- Be cautious when dealing with individuals outside of your own country.
SUMMARY: MODULE 3 IN A NUTSHELL

The module on cyber crime and security identifies the broad challenges we all face as we attempt to make Internet use safe and secure. It provides a basic description and explanation of some key concepts, as well as a discussion of important key issues, hopefully in order to enable the participants have a better grasp of the realities of misconduct in the Internet and make available to them the technical, legal and regulatory tools to help prevent or minimize these attacks.

Specifically, the module deals with the following:

- **Cyber crime:**
  - Internet and security concepts;
  - Types of incidents and attacks;
  - Improving security.

- **Cyber law:**
  - Statutes, laws and policies: challenges to enforcers;
  - Substantive and procedural law;
  - International and other efforts to combat cyber crime.
ADDITIONAL INFORMATION ON CYBER CRIME AND SECURITY

APEC Cyber Crime Survey.
- A survey commissioned by the APEC to identify offences and cyber crimes in the Asia-Pacific region. http://www.apectelwg.org/e-securityTG/Downloads

CERT.
- A centre of Internet security expertise, located at the Software Engineering Institute. A federally funded research and development centre operated by Carnegie Mellon University. It studies Internet security vulnerabilities, researches long-term changes in networked systems, and develops information and training to help improve security: http://www.cert.org

Cyber Security and Cyber Crime

International Telecommunications Union.
- Provides information and resources on cyber security, ICT laws, Internet governance, and articles on network security: http://www.itu.int
MODULE 4: OTHER KEY ISSUES TO BE ADDRESSED IN CREATING AN ENABLING LEGAL AND REGULATORY FRAMEWORK TO ENCOURAGE INTERNET USE FOR BUSINESS DEVELOPMENT

A holistic legal, regulatory and policy framework is a critical part of the fully enabling environment that governments should seek to create. This module provides brief overviews and examples of other key issues that can also be considered and explored as governments move to truly encourage internet use for business development, especially by SMEs.

I. PROMOTING COMPETITION

The elimination of barriers to entry, and the introduction of competition in the ICT sector, will generally provide benefits not only to ICT-related SMEs, but to all SMEs in general.

Box 9. Case Study: Voice over Internet Protocol – The Philippine Experience

In May 2005, the Philippines’ telecommunications regulator issued rules which classified Voice over Internet Protocol (VoIP) as a value-added service (VAS). Under Philippine laws, its classification as a VAS, rather than as a telecommunications service, effectively meant that the commercial offering of VoIP to the public was not limited to traditional telecommunications carriers and opened the VoIP business to competition.

The mere prospect of competition led to immediate results, as long distance costs plummeted as much as 75 per cent within days of the ruling that opened VoIP to competition.

To date, at least six additional VoIP providers have applied with and been approved by the regulator. It is likely that the rules have also helped to spur the major telecommunications companies to proceed aggressively with broadband deployment, as demand for better bandwidth to accommodate data-related services, particularly VoIP, continues to increase. Already, the top two wireless providers – in heavily advertised campaigns – are competing to offer SMEs and micro-enterprises very affordable turnkey solutions to provide broadband wireless internet facilities.

Note that the benefits of competition in VoIP extend even to SMEs that are not part of the ICT sector per se, as they too now enjoy greater choice and lower telecommunications costs especially with customers/suppliers in other countries. In a globalized economy, this benefit is bound to grow even more – and would make it also easier to go multinational, as VoIP allows SMEs to coordinate their operations domestically, regionally and globally.

It is, to be sure, not a simple matter to introduce competition, especially in the telecommunications market.

In most instances, dominant carriers can use their superior position to engage in unfair methods of competition that deter (or are likely to deter) new entry into the market, or restrict (or are likely to restrict) existing competition in the market, for reasons unrelated to the availability, price and quality of service that operators offer or seek to offer. Moreover, it is important to note that even in markets where a single major supplier does not exist, two or more suppliers could cooperate to engage in anti-competitive practices.
For example, a major supplier which provides essential inputs to its competitors can take advantage of its dominant market position by engaging in anti-competitive cross-subsidization – shifting costs from its competitive activities to its non-competitive activities (the operation of essential facilities), or obtaining products and services from its non-competitive arm on advantageous terms and conditions.

Another common example is when a major supplier is in a position of dominance over other suppliers in interconnection negotiations. Competition goals are often frustrated when dominant players refuse or make it difficult for new entrants to interconnect and effectively offer competing services to the public.

The two anti-competitive practices below are also common:

- **Price Squeezes**
  A price squeeze happens when a major vertically integrated supplier sells inputs to its downstream competitors at a price so high, relative to its own retail price, that they cannot be expected to compete profitably in the same retail market. It can occur when operators with market power control certain activities that are key inputs for competitors in downstream markets and where those same key inputs are used by such operators or their affiliates to compete in the same downstream market.

- **Predatory Pricing**
  Predatory pricing occurs when the major supplier sells services below marginal cost to drive competitors away and prevent new ones from entering the market, and then subsequently, increases prices to re-coup the amount lost during the price cut.

A policy choice to promote competition therefore requires both the political will and clear mandate, and technical capability to monitor – and enforce – compliance with competition rules.
**II. BRIDGING THE DIGITAL DIVIDE**

“The digital divide” refers to the gap between those with regular, effective access to digital technologies and those without. The digital divide results from the socio-economic differences between communities that in turn affect their access to digital information – mainly but not exclusively through the Internet.

The presence of a digital divide, particularly between rural communities and urban centres, directly affects the ability of SMEs to reach and compete in the larger domestic and even global markets.

The digital divide is also an example of a problem that likely requires more from the government than other ICT-related concerns, which can be left more to the private sector.

In many instances, market mechanisms alone will not suffice to ensure widespread individual access to the network, since much of the population often lacks the income required to obtain the services or they are otherwise located far from places where private sector investment is present. A digital divide exists in these areas precisely because the market is too small or insignificant for private sector players to consider. Low-income and rural communities are increasingly left behind, which in turn limits the ability of SMEs in these areas to use the Internet for business development.

Beyond the moral duty of governments of bridging this gap, however, it should also be pointed out that numerous examples exist of the Internet being used by SMEs in rural and unserved areas – leading not only to better lives and opportunities in these places and for these people, but also contributing to overall socio-economic development.

- Internet access will enable SMEs and entrepreneurs to use e-mail and VoIP to coordinate directly with buyers of local goods and products in the cities, effectively bypassing middlemen and earning a greater share of the revenues.

- Numerous websites allow local artisans to sell directly to the mature markets in the developed countries where their products are likely to fetch higher prices. Examples abound from for-profit sites like Novica.com (which is a partner of National Geographic) to non-profit marketplaces like PEOPLink ([www.peoplink.org](http://www.peoplink.org)).

- The Internet also helps to level the playing field for SMEs in remote areas by providing them with key information and ideas on market prices, opportunities and trends.

Therefore, bridging the digital divide – or, putting it in another way, providing rural communities with access to information and communications technology (especially the Internet) – is therefore an important policy goal to the extent that it assists SMEs in these areas to grow. From a broader viewpoint, it helps enterprises to make a more meaningful contribution to overall countryside development.

**A. Key Policy Considerations**

- What are possible policy options for providing connectivity to rural and remote communities?
  - Competition policy;
  - Universal Access Fund and other related schemes;
  - CD-based applications.
Ease of access to the Internet is a fundamental aspect, but it is not the sole factor. Effective access also depends on the ability to use ICT effectively, and on the quality of digital content that is available and can be provided. Once an appropriate level of access is achieved, the individual, community or SME then requires an education that includes literacy and technological skills to make effective use of it. What programmes need to be in place in terms of relevant education and training? How can these be effectively funded, made sustainable and documented?

The availability of broadband connections may affect SMEs’ decisions to adopt e-commerce. Broadband’s faster speeds improve overall online experiences for both individuals and businesses, encouraging them to explore more applications and spend more time online. In contrast, slow internet connections and data transfers discourage SME adoption of the Internet.

III. PROTECTING THE CONSUMER

For e-commerce to take off, consumer trust in online businesses is essential. Without the confident e-consumer, there can be no e-commerce. Thus it is imperative to ensure that the online traders observe specific rules and guidelines to allay the fears of the consumer and promote ethical online transactions.

A. What Are the Main Concerns of Consumers with Regard to Online Transactions?

The primary concerns for the consumer that would need to be addressed by SMEs and by the broader legal and policy framework include:

- The consumer’s exposure to unfair marketing practices;
- Insufficient information disclosure; for example, refund policies, cancellation terms, warranty information;
- Contract terms; for example, their enforceability;
- Merchandise and delivery practices; for example, failure to perform and lateness;
- Payment; for example, recovering fraudulent charges if credit card information falls into criminal hands;
- Transaction confirmation and cancellation policies; for example, the consumer’s lack of knowledge on cancellation rights for online transactions.

Box 11. A Balancing Act

Note that there exists a challenge for SMEs and for government policymakers in balancing sometimes competing interests.

For instance, the Internet creates a huge and highly affordable opportunity for small or new SMEs to market themselves to the global market. How should this interest be balanced against the desire to curb spamming and unwanted sales pitches?

To give a second example, how can governments assure consumers that their private information, for instance, credit card data, would be protected; and at the same time encourage the deployment and use of online payment mechanisms to promote e-commerce?

How can consumers be protected from fraud in the context of an Internet that knows no boundaries and where the perpetrators may lie out of the reach of the law?
transactions, including for mistakenly made purchases;

- Fraud and deception: for example, lack of means to authenticate merchandise purchased online;
- Unsafe products;
- Insecure payment methods;
- Loss of personal privacy and protection of confidential data;
- Risk misuse of personal information;
- Other concerns include computer fraud, hacking, virus, interception and alteration of financial data, and misuse of personal information.

**B. General Principles for Protecting Consumers Online**

The OECD’s *Guidelines for Consumer Protection in the Context of Electronic Commerce* was approved back in December 1999 and is designed to help ensure that consumers are no less protected when shopping online than they are when they buy from their local store or order from a catalogue. The guidelines establish the core characteristics of effective consumer protection for online business-to-consumer transactions, thereby eliminating some of the uncertainties that both consumers and businesses encounter when buying and selling online.

The guidelines feature eight categories of general principles:

- **Transparent and Effective Protection** – Consumers who participate in electronic commerce should be afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce.

- **Fair Business, Advertising and Marketing Practices** – Businesses engaged in electronic commerce should pay due regard to the interests of consumers and act in accordance with fair business, advertising and marketing practices.

- **Online Disclosures** – Clear and obvious disclosures should be available for consumers.

- **Confirmation Process** – To avoid ambiguity concerning the consumer’s intent to make a purchase, the consumer should be able, before concluding the purchase, to identify precisely the goods or services he or she wishes to buy; identify and correct any errors or modify the order; express an informed and deliberate consent to the purchase; and retain a complete and accurate record of the transaction.

- **Payment** – Consumers should be provided with easy-to-use, secure payment mechanisms and information on the level of security such mechanisms afford.

- **Dispute Resolution** – Consumers should be provided meaningful access to fair and timely alternative dispute resolution and redress without undue cost or burden.

- **Privacy** – Business-to-consumer electronic commerce should be conducted in a manner that provides appropriate and effective protection for consumers’ privacy.

- **Education and Awareness** – Governments, business and consumer representatives should work together to educate consumers about electronic commerce, to foster informed decision-making by consumers participating in electronic commerce and to increase business and consumer awareness of the consumer protection framework that applies to their online activities.

**IV. PROMOTING PUBLIC-PRIVATE PARTNERSHIPS**

Authentic partnership with the private sector is the key to developing effective e-business policies for SMEs.
In public-private partnerships, there is a recognition that the government’s primary role in ICT development is to provide an enabling policy, legal and regulatory environment that levels the playing field and allows the private sector to take the lead.

Therefore, while public authorities play a crucial role in promoting the adoption of the Internet for business purposes, it is important to note that ultimately, the private sector is better positioned and qualified to undertake implementations.

Initiatives and projects to develop the ICT sector will have a higher chance of success and sustainability if these are market-led, rather than government-led. The private sector should provide leadership through investments, capitals and other resources.

Market forces alone, however, cannot guarantee the full development of an inclusive Information Society. As noted previously, for example, the objective of ensuring free and fair competition may be thwarted by large or dominant players in the market. Programmes to promote access to ICT, particularly in rural and remote areas, may fail if the private sector does not feel ready or inclined to invest in places where there is little profit to be made.

The government, therefore, must remain vigilant in its role of verifying that, at any time, implementation is proceeding consistently with its policy objectives. As an enabler, its involvement in the markets should be predictable, developmental, transparent and efficient. Regulation, where necessary, should promote a level playing field and should not hinder companies from competing in free and fair markets. It is equally critical to ensure that public-private partnerships should not compromise the independence and impartiality of the public authorities.

It is therefore important that the partners – both private and public – are in agreement, or at least are aware, of the overall goals of government and its ICT programmes, and that there is a good understanding of their respective roles.

V. EARNING GLOBAL CONFIDENCE

A. Privacy and Data Protection

In information economies, the task of protecting data is of paramount importance. While secure storage and transparent use are important for many categories of public information, managing personal data also involves important issues of privacy.

There is therefore a need to strike a balance between privacy and the various needs to transmit personal data.

Indeed, the transmission of such data is fundamental to the conduct of e-business, but it needs a great deal of trust and confidence.

Note that with the growth of computing, the expanded use of the Internet and the rapid development of new technologies, there is also an increased potential for violations of online privacy. Therefore, some form of legal protection of privacy is important for generating trust in e-commerce.

Furthermore, beyond generating trust, developing countries who wish to participate in the global information economy, will increasingly need to consider laws that protect personal data in order to even have a chance at helping to facilitate the flow of information from developed to developing countries. Note that in European jurisdictions, for example, it is forbidden to transfer data to a jurisdiction that does not provide adequate protection for personal data.
Box 12. What is the European Union Data Protection Directive?

The European Union Data Protection Directive was enacted in 1995 with member States required to implement its provisions by October 1998. The Directive’s primary goal was to create a common European standard of privacy protection for the processing of personal data. The Directive establishes a series of protections for individuals including the right to know why information is being collected and how the information will be used and disclosed. Individuals are also entitled to compensation for any damages that arise from failure to abide by the Directive’s requirements.

Although the Directive does not have direct effect outside the European Union, it does contain an “adequacy clause” that has had a significant effect on the privacy law frameworks of non-European Union countries. Article 25 provides that member States must ensure that the transfer of personal data to non-European Union countries takes place only if the non-European Union country provides an adequate level of privacy protection.

B. Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data

The OECD privacy guidelines were created in 1980, well before the Internet boom and the emergence of e-commerce. Although more than 20 years old, the principles found in the guidelines continue to serve as the basis for most privacy initiatives worldwide.

The guidelines feature eight privacy principles:

- **Collection Limitation Principle** – There should be limits to the collection of personal data. Such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- **Data Quality Principle** – Personal data should be relevant to the purposes for which they are to be used. To the extent necessary for those purposes, data should be accurate, complete and kept up-to-date.

- **Purpose Specification Principle** – The purposes for which personal data are collected should be specified no later than the time of data collection. The subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified at each occasion of change of purpose.

- **Use Limitation Principle** – Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the data quality principle except with the consent of the data subject; or by authority of law.

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

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

- **Individual Participation Principle** – An individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her. An individual should have the right to receive that data and to challenge it if incorrect.

- **Accountability Principle** – A data controller should be accountable for complying with measures that give effect to the principles stated above.

What other interests need to be balanced against the need to protect private data?
C. Intellectual Property Rights

Public policy on intellectual property rights poses an interesting challenge to governments, especially in developing countries, given the rapid developments in technology.

Today, however, technology is complicating this process and undermining many of the mechanisms that governed the system in the past. This trend is likely to continue; today’s technologies are the beginning, not the end, of the information revolution. Computers, two-way interactive cable, fibre optics, optical disks, communications satellites, and other devices are becoming steadily more sophisticated and powerful; and their uses are expanding almost daily. The greatest impact, however, will come not from single technologies, but rather from their use in combination.

These new information and communications technologies are challenging the intellectual property system in ways that may only be resolvable with substantial changes in the system or with new mechanisms to allocate both rights and rewards. Once a relatively slow and ponderous process, technological change is now outpacing the legal structure that governs the system, and is creating pressures on the United States Congress to adjust the law to accommodate these changes. The pressures are coming from a number of different parties, and they are motivated by a wide range of concerns:

- Authors, publishers, film makers, and producers; representatives of the recording industry; and other copyright holders whose works can be delivered electronically: This group is concerned that technologies such as tape recorders, videocassette recorders and compact discs are so widely used that they undermine their ability to enforce their copyrights. They are calling on Congress to adopt stronger enforcement measures. Alternatively, some group members would like Congress to provide new ways to protect their incomes, such as imposing taxes or royalties on blank tapes.

- Designers and producers of computer software and other functional works that do not fit comfortably into existing categories of intellectual property law: This group is concerned that, given the uncertainties in the law, their works will be inadequately protected. They are calling for more explicit and extensive protection under new or existing laws.

- Database producers, information analysts, and others who package existing information for specific uses: This group opposes restrictions on the use and re-use of copyrighted materials. They also want incentives to be reallocated so that they receive a greater financial return for the value that they add to information by analyzing, reorganizing and packaging it.

- Manufacturers of equipment capable of copying, reproducing or recording (paper copiers, satellite antennas, videocassette recorders, audio tapes, and blank CDs and DVDs): Members of this group oppose the imposition of taxes or royalties on tapes and any other actions that might increase the cost of their products to the consumer, or that make them less convenient to use. They claim that they aid copyright holders by creating new markets for products and so should not be penalized by having taxes imposed.

- Educators and scientists: Members of this group generally oppose extensions of the law, arguing that such extensions would make the resources and materials they need to do their work prohibitively expensive. Some members of this group seek to exempt educational uses from the law. Others are calling for licensing agreements that would allow them to use copyrighted materials at reduced rates.

- The general public: Many people are becoming increasingly accustomed to having new technology available at low cost to use as they please in their homes and offices. They want assurance that they can continue to copy films, records, and other information for their private use.

- For SMEs, the interests could be conflicting: On the one hand, human innovation and creativity has increasingly led to the introduction of new products, brands and creative designs in the market. Small and medium-sized enterprises (SMEs) are often the driving force behind such
innovations, and intellectual property rights help them to enjoy fuller benefits from their creativity. Adequate protection of the SME’s intellectual property is a crucial step in deterring potential infringement and in turning ideas into business assets with a real market value. On the other hand, SMEs, especially in developing countries, may have far greater interest in having access to useful technologies and applications, but may not be able to afford them. Note, too, that some argue that an inappropriately strong intellectual property rights system increases the costs of access to many products and technologies (particularly in health, agriculture, education and information technologies) that developing countries (and SMEs) need.

D. Capabilities and Challenges Posed by the New Technologies

To understand the legal and political pressures that new technologies place on the intellectual property system, one needs to understand their unique capabilities. A few examples convey the scope and pace of technological progress and the problems that it poses:

- **A problem of identifying authorship** – A group of authors using personal computers connected by a telephone network can collaborate in writing an article, a piece of software or a database. This work can exist in various forms, in different places and can be modified by anyone having access to the network. This networking technology provides new opportunities to combine talents, resources and knowledge. In such a world where there are many authors of one work, worldwide collaboration and ever-changing materials, how are intellectual property rights to be allocated or awarded?

- **A problem of identifying infringements and enforcing rights** – The increased communications capacity (in terms of speed, bandwidth, and distance) made possible by fibre optic technology, will allow computer users to rapidly transmit incredible amounts of information at a rate of 100 average-length pages in a second. These high-speed communications media, combined with large capacity optical disk storage technologies, will also pose enforcement problems for the intellectual property system. They allow individuals to trade vast quantities of copyrighted materials without the knowledge or permission of the copyright holders. With these technologies, the situation is no longer simply one of an individual trading or giving away a book to someone else; rather, it is one in which individuals can inexpensively and privately share the contents of an entire library.

- **A problem of private use** – If a private citizen copies information – a film or record, for example – should this be considered an infringement of copyright? At present, the law gives little guidance in this area – nor, until recently, did it need to. Such private use was so limited it posed no threat to

---

**Box 13. Free and Open Source Software Development**

The open source movement, like digital technologies generally, presents both opportunities and challenges within the intellectual property context. Over the past decade or so, a large, global community of software developers has turned itself into a major economic and political force by developing new software on a collaborative model, known variously as “open source”, “libre” and “free” software. While open source technologies have not yet become a major player in the desktop computing space, the majority of web pages, for instance, are served using open source technologies.

Open source presents opportunities to countries that are growing their ICT infrastructure because it is often a low-cost software choice (and free, at least in its simple form), more secure than some proprietary technology choices (according to many technologists, though this assertion is controversial) and can foster a local technology development community rather than sending license streams to large technology companies in other countries, frequently in the United States.

On the other hand, proprietary systems like Microsoft applications are easier to find and to use. Many corporate and government electronic systems already run on proprietary software. Migrating to open source would both be expensive and time-consuming and would require re-training and re-tooling of employees.

Is promotion of open source technologies, rather than proprietary choices, sound public policy? Does the intellectual property regime, whether in individual countries or in a global sense, need to be adjusted to support open source technology development? What do local software developers have to gain from a legal and policy regime supportive of open source technologies?
industry profits. Second, if it were decided that home copying infringed copyright, how could a ban against it be enforced? Since many people could be engaged in this kind of behaviour in the privacy of their own homes, their activities would be impossible to track.

- **A problem of derivative use** – A major newspaper maintains its index on computer. A user of this index takes the information in it and analyses it for another client, giving him up-to-date, timely information that is precisely tailored to his needs. Using electronic technology, a research chemist can search all bibliographic data on a particular chemical in a matter of hours, instead of the weeks it once would have taken. An investor who must make a snap decision about whether to buy or sell can call up a constantly updated database; and use the information to pursue his profits.

The new information technologies, which allow for this kind of customized information on demand, are creating a wide range of new opportunities to expand the variety, scope and sophistication of information-based products and services.

In fact, a whole new industry has developed to provide these services; and it is now one of the fastest growing sectors in the economy. As the opportunities to create derivative works increase and as this sector comes to play a larger role in the economy, questions arise about what kinds of information can legally be used to create secondary information products. Under existing intellectual property law, copyright holders have the right to benefit from all subsequent works based on their original works. If interpreted broadly, it is possible, however, that this approach will inhibit the production and use of secondary materials.

- **A problem of meeting educational goals** – The intellectual property system was originally designed to enhance learning and the useful arts. This goal is more difficult to meet today because of the increasing market value of intellectual properties.

The technologies provide numerous opportunities for educational use. However, because software development is often expensive, it is in the interest of the developer to concentrate on products for customers who can pay the most – businesses, not schools. The schools then have the choice of doing without software, diverting money from other equally needed educational materials, or developing their own software, since they cannot legally copy copyrighted works. The copyright problem in this situation is simple: Copyright, designed as a policy tool to enhance learning, fails to meet its goal.

- **A problem of integrity** – Assisted by the computer, a film maker can create scenes that were never actually filmed, or take existing images and place them in entirely new contexts. These capabilities open new avenues for creativity. But at the same time, they may be used to misrepresent a work or undermine its integrity. An unscrupulous artist, for example, might use technology to distort a well-known piece of art for his own purposes or profit without the knowledge of the original artist.

In this electronic environment, creators may become as concerned about the integrity of their works as they are about their profits. To be effective, intellectual property law may need to take into account the problem of artistic integrity, as well as that of financial rewards.

- **An international problem:** All of the capabilities and problems that characterize domestic use of the new technologies are equally prominent – sometimes even more so – when they are used internationally. Satellite technology permits global communication, but it also beams in programming that nations may not want. Satellites collect valuable agricultural and environmental information about the developing world. But once it has been analyzed by a commercial company and copyrighted, it may be priced too high for developing countries to afford. A nation near the United States is able to pick up and unscramble satellite programming that viewers want – and do so without paying the fee charged by the company. Domestic companies have no way to monitor use or enforce their copyright claims. These problems are exacerbated by considerable disagreement among nations about intellectual property issues.

E. Cross-border Cooperation and Harmonization
Different countries will have different approaches to the challenge of policymaking in the policy areas discussed above. Given the “borderless” nature of the Internet, conflicting rules and regulations will only serve to hamper and discourage participation in e-commerce, especially by SMEs.

The following cases provide vivid illustrations on the need for cross-border cooperation and harmonization of laws and rules.

- **Privacy and Data Protection.** India has been extremely successful in developing an outsourcing industry, from basic data entry processing to more sophisticated services such as customer call centres and financial services. Indian businesses have attracted a wide range of Western companies to relocate various business processes to the subcontinent. However, concerns have recently been voiced in the European Parliament about the vulnerability of personal data being transferred under such outsourcing arrangements. Some view outsourcing as a process that effectively circumvents European safeguards. As a consequence, Indian companies are now pressuring their government to take regulatory action to forestall any adverse reaction from Europe.

To give another example, Ms Mugure Mugo, founder of PrecissPatrol, a Kenyan outsourcing enterprise dealing with IT services, has already received requests from European-based clients specifically wanting to know her company’s policy on the collection and security of collected data. Ms Mugo recognizes that the fact that Kenya does not have specific data protection laws may constitute a barrier to the development of the country’s e-business.

- **Intellectual Property Law.** With annual revenues of more than US$1 billion, Adobe is the second-largest PC software company in the United States. In an effort to lead the market for software that enables the digital distribution of books, Adobe developed the Adobe Acrobat eBook Reader which was designed as a “trusted system”, offering publishers a spectrum of copyright protection options when encoding their content.

Meanwhile, founded in 1990 and headquartered in Moscow, ElcomSoft is a software company that "specializes in producing Windows productivity and utility applications for businesses and individuals". Among the many software products developed by ElcomSoft is the “Advanced eBook Processor (AEBPR)”, which used to be available for download from their site (but seems to now have been removed). The program enables users to (a) disable the copyright protection controls deployed by book publishers using Adobe's software and (b) repackage their digital books in a variety of common formats without copyright controls.

Dmitry Sklyarov is a young programmer and cryptographer formerly employed by ElcomSoft who has been researching cryptanalysis in furtherance of a Ph.D. he hopes to earn from a Moscow university. He is allegedly responsible for much of ElcomSoft's AEBPR, most notably, the decryption algorithms it employs to circumvent Adobe's copyright protection controls.

[Sklarov] was invited to give a presentation at the DEF CON conference in Las Vegas about the electronic security research work he has performed as part of his Ph.D. research. His presentation concerned the weaknesses in Adobe's eBook technology software. Dmitry was arrested at his hotel in Las Vegas, on 16 July [2001,] as he was leaving to return to Russia.

In its 28 August 2001 press release, the United States Department of Justice (DOJ) reported:

*The United States Attorney's Office for the Northern District of California announced that Elcom Ltd. (also known as Elcomsoft Co. Ltd.) and Dmitry Sklyarov, 27, both of Moscow, Russia, were indicted today by a federal grand jury in San Jose, California on five counts of copyright violations. The defendants were each indicted on one count of conspiracy to traffic in technology primarily designed to circumvent, and marketed for use in circumventing, technology that protects a right of a copyright owner, in violation of Title 18, United States Code, Section 371; two counts of trafficking in technology primarily designed to circumvent technology that protects a right of a copyright...*
owner, in violation of Title 17, United States Code, Section 1201(b)(1)(A); and two counts of trafficking in technology marketed for use in circumventing technology that protects a right of a copyright owner, in violation of Title 17, United States Code, Section 1201(b)(1)(C).

Sklyarov's arrest prompted outcries of outrage from software developers, civil libertarians and all who generally oppose the Digital Millennium Copyright Act (for ideological or "practical" reasons). He faced a maximum fine of $2.25 million and up to 25 years imprisonment. Not surprisingly, the DOJ promptly reached an agreement with Sklyarov, under the terms of which they have agreed not to prosecute him personally if he assists in their (criminal) prosecution of ElcomSoft.

On 17 December 2002, a federal jury acquitted ElcomSoft of all criminal charges against it and Sklyarov was released subject to a plea agreement.

This case is highly fact-specific and unlikely to be repeated. But it demonstrates the power and reach of copyright-related laws outside the geographic boundaries of a given jurisdiction, especially when a country like the United States demonstrates a willingness to extend its competence beyond state and national boundaries to enforce its intellectual property jurisprudence interpretation into other jurisdictions.

- **Cyber Crime.** Cyber crime presents one of the most complex and exigent circumstances for international cooperation. For example, an e-mail sent to a colleague across town may be routed via packet switching through China, Argentina and South Africa before reaching the recipient's inbox. Cyber criminals can intentionally "weave" their communications through several carriers and countries before attacking a network or system. Likewise, a cyber stalker can route his communication through several jurisdictions before reaching the victim. A child pornographer can hide his identity and route materials over networks of multiple countries before reaching the intended recipients. Someone can also commit a cyber crime against persons in several countries.

A cyber criminal does not have to leave his own home – or cross a national boundary – to commit an act in several countries around the globe. His communications may be routed through local phone companies, long distance carriers, Internet Service Providers and wireless and satellite networks and may go through computers located in several countries before attacking targeted systems around the globe. Evidence of the cyber crime may even be stored on a computer in a different country from where the criminal executed the act.

Law enforcement, however, is stopped at the borders of nation states and must go through proper legal channels to receive assistance in cyber crime investigations -- which is often dependent upon the skill levels of law enforcement in that country. Assistance is also dependent upon that country's legal system. Foreign assistance may be needed even if the act is local. Frequently, communications may pass through several countries; requiring law enforcement to seek international assistance just to find out the perpetrator is a local person.

Recent examples of the need for international cooperation and assistance include these:

- Officers in Wales, working in coordination with the Federal Bureau of Investigation (FBI), arrested two persons for intrusion into e-commerce sites and theft of information pertaining to 26,000 credit cards. Losses were estimated to be as high as US$3 million. In developing the case, the FBI worked closely with the Dyfed-Powys Police Service in Britain, the Royal Canadian Mounted Police in Canada, and private industry and involved seven FBI field offices, the United States Legal Attaché in London, and the National Infrastructure Protection Centre.

- A hacker in the United States recently pled guilty to illegally accessing computers belonging to the United States Postal Service, the State of Texas, the Canadian Department of Defence and a publishing company located in the state of Wisconsin. The conviction of the hacker was the result of a joint investigation involving the Texas Department of Public Safety, the Royal Canadian Mounted Police, the Canadian Forces National Investigative Service and the United States Postal Service Office of the Inspector General.
While it is important for developing countries to have cyber crime laws in place, it is equally important that countries have the legal authority to assist foreign countries in an investigation, even if the country at issue has not suffered any damage itself and is merely the location of the intruder or a pass-through site. "Inadequate regimes for international legal assistance and extradition can therefore, in effect, shield criminals from law enforcement: criminals can go unpunished in one country, while they thwart the efforts of other countries to protect their citizens" (American Bar Association 2002).

To conclude, and to repeat, there is no one set of policies that will be correct or appropriate for every nation. Best practices and experiences in other countries will surely help, but such lessons should be taken in the context of your nations’ respective social, political and economic environments. Ultimately, nations will have to choose the mix of policies that can best balance competing interests and goals.
SUMMARY: MODULE 4 IN A NUTSHELL

Promoting Competition

- The elimination of barriers to entry, and the introduction of competition in the ICT sector will generally provide benefits not only to ICT-related SMEs, but to all SMEs in general.

Bridging the Digital Divide

- The digital divide refers to the gap between those with regular, effective access to digital technologies and those without. The digital divide results from the socio-economic differences between communities that in turn affect their access to digital information – mainly but not exclusively through the internet.

- The digital divide is an example of a problem that likely requires more from the government than from the private sector.

- Bridging the digital divide is an important policy goal to the extent that it assists SMEs in remote and unserved areas to grow and contribute more meaningfully to overall countryside development.

Consumer Protection

- The primary concerns for the consumer, which would need to be addressed by SMEs and by the broader legal and policy framework, include the following:

  - Consumer’s exposure to unfair marketing practices;
  - Insufficient information disclosure, for example, refund policies, cancellation terms, warranty information;
  - Contract terms, for example, their enforceability;
  - Merchandise and delivery practices, for example, failure to perform and lateness;
  - Payment, for example, recovering fraudulent charges if credit card information falls into criminal hands;
  - Transaction confirmation and cancellation policies, for example, consumer's lack of knowledge on cancellation rights for online transactions, including for mistakenly made purchases;
  - Fraud and deception, for example, lack means to authenticate merchandise purchased online;
  - Unsafe products;
  - Insecure payment methods;
  - Loss of personal privacy and protection of confidential data;
  - Risk misuse of personal information;
  - Other concerns include computer fraud, hacking, virus, interception and alteration of financial data and misuse of personal information.

- General principles for protecting consumers online:

  - Transparent and effective protection;
  - Fair business, advertising and marketing practices;
  - Online disclosures;
  - Confirmation process;
  - Payment;
  - Dispute resolution;
  - Privacy;
  - Education and awareness.

Privacy

- Countries that wish to participate in the global information economy will increasingly need
to consider laws that protect personal data to compete.

- The European Union’s Data Protection Directive, enacted in 1995, requires member states to ensure that the transfer of personal data to non-European Union countries takes place only if the latter country provides an adequate level of privacy protection.

- The OECD privacy guidelines feature eight privacy principles:
  - Collection limitation principle;
  - Data quality principle;
  - Purpose specification principle;
  - Use limitation principle;
  - Security safeguards principle;
  - Openness principle;
  - Individual participation principle;
  - Accountability principle.

**Intellectual Property Rights**

- New ICTs are challenging the intellectual property system in ways that may only be resolvable with substantial changes in the system or with new mechanisms to allocate both rights and rewards. New ICTs, for example, create problems in certain areas:
  - Identifying authorship;
  - Identifying infringements and enforcing rights;
  - Private use;
  - Derivative use;
  - Meeting educational goals;
  - Integrity.

**Cross-border Cooperation and Harmonization**

- Different countries have different approaches to the challenge of policymaking. Given the borderless nature of the Internet, conflicting rules and regulations only serve to hamper and discourage participation in e-commerce, especially by SMEs.
ADDITIONAL INFORMATION ON OTHER KEY ISSUES TO BE ADDRESSED IN CREATING AN ENABLING LEGAL AND REGULATORY FRAMEWORK TO ENCOURAGE INTERNET USE FOR BUSINESS DEVELOPMENT

Asia-Pacific Development Information Programme.
- Provides various resources on e-governance, ICT4D, ICT for SMEs, open source software, policy notes on ICT for SMEs.  http://www.apdip.net/

Cyber Security and Cyber Crime.

Development Gateway (World Bank) portal.
- The website includes a wide variety of documents on ICT and development; e-commerce and development; e-commerce and arts and crafts; among others. http://www.developmentgateway.org/all-topics

Digital Dividend portal.
- A site offering innovative examples of SMEs using e-business techniques. The site also offers a clearinghouse to match investors/sponsors with prospective projects. http://www.digitaldividend.org/

Network World.
- Provides information on VoIP and convergence, network security and solutions, SME networking, and white papers on convergence and internet policies. www.networkworld.com

Networkworld Partners.
- Includes solutions and alternatives on VoIP technology. www.networkworldpartners.com

OECD SME portal.

SME portal in Malaysia.
- A one stop information portal for small and medium-sized enterprises. It provides information on all aspects of SME development, including financing, advisory services, training programmes, business and networking opportunities. www.smeinfo.com.my

Technonet Asia.
- A cooperative network of development support institutions, aiming to enhance the quality and competitiveness of SMEs in its member countries through information, technology transfer and human resources development. http://www.idrc.ca
http://www.abanet.org/scitech/computercrime/cybercrimeproject.html


Commission of the European Communities, the Economic and Social Committee and the Committee of the Regions, Communication from the Commission to the Council, the European Parliament. 2002. “Helping SMES to ‘Go Digital’”.


National Telecommunications Commission (NTC), August 2005. Memorandum Circular 05-08-2005 on VoIP.

http://oberon.sourceoecd.org/vl=8791980/cl=22/nw=1/psv/∼6681/v2000n3/s1/p1


UNDP-APDIP eNote, April 2005. “Why should countries embed ICTs into SME policy?”

