UNCTAD/SDTE/ECB/2005/1

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT
Geneva

INFORMATION ECONOMY REPORT 2005

CHAPTER 5

UNITED NATIONS
New York and Geneva, 2005

Chapter 5

INFORMATION TECHNOLOGY AND SECURITY: RISK MANAGEMENT AND POLICY IMPLICATIONS

A. Introduction

Information security is the sum of the processes and technologies used to protect information assets from unauthorized acquisition, disclosure, manipulation, modification, or damage and loss.[1] Information security underlines the importance of trust and trust-building in everyday economic and civic life. Economic activities, such as trade or financial transactions, may be critically dependent on information security, as globalization encourages and directs remote or mutually unfamiliar firms and individuals to interact. As e-business becomes part of the everyday experience of large numbers of firms, who will on average tend to be more risk-averse than early adopters of technology, security in all its dimensions becomes crucially important (UNCTAD, 2003).[2]

The innovative use of information and communication technologies (ICTs) is often seen as a means for making improvements in productivity and efficiency, but in practice it is not all "strengths and opportunities". The "challenges and threats" part of the equation is mission-critical for realizing these improvements, and they can largely be seen as involving a process of active risk management of perils and hazards encountered in the application of ICTs.

Understanding information security and using a risk management approach is equally important for Governments and firms from developed and developing countries. However, developing countries may need to promote information security awareness and risk management more actively because of their relatively larger proportion of recent ICT adopters, be they firms, public bodies or individuals. Fast progress from minor ICT usage to full connectivity and access can complicate information security.

Information security also raises questions as to what combination of technical, management, regulatory and legal solutions works best. Here too, knowledge and awareness of the basic technology landscape can be an advantage, while a strategic approach built around a core of risk management notions can be a decisive asset. Proactive and strategic information security has become indispensable from a regulatory perspective as well. The international community has arrived at a common approach to information security practice and has recognized the threat of cybercrime to information economy development.[3] International forums and national regulatory bodies are formulating and advising on minimum information security standards for international commercial partners. As a result, firms from developing countries can be affected and may risk marginalization if they cannot meet the information security requirements of their counterparts in the developed world. This can be of particular importance for countries seeking to develop business process outsourcing activities, in particular in the areas of financial services, ICT services and software export.

In order to elucidate the relevant issues, this chapter will start with an overview of basic concepts and notions that explain why information security matters. It will then describe the information security business sector. It will briefly describe the chronological development of cryptographic and security technologies. This is more than academic. Newness and hype often go hand-in-hand, and an appreciation of the origins and continuity of security technology developments can be invaluable when confronted with the latest paradigm-shifting cure-all security solution. Following this, the discussion will focus on security issues from a risk management perspective. It will note the diversity of information security threats, as well as the needs of Governments as users and also as enablers of e-business and e-governance. Particular technologies will also be discussed within a risk management framework, and this will serve to highlight the need for a management-centric, as opposed to technology-centric, approach to information security. This will, in turn, permit a discussion of notions related to human resource capacity and development, as well as to the changing regulatory environments resulting from increased information security needs.

The chapter will go on to present an overview of international policy discussions on information security. It will, however, avoid a discussion of legal issues of information security, often considered under the collective term of cybercrime, as these are covered in chapter 6 of this report. The chapter will close with a discussion of policy recommendations for Governments and some reflections as to future developments and relevance for intergovernmental processes and the international community.

B. Concepts and context

1. Definition and objectives

Information security consists of processes and controls that aim to protect information and data, and their underlying infrastructures. The mission of information security is to establish trust in technologies that make possible various positive societal and commercial activities, including e-commerce, e-business and e-government. This mission is achieved by simultaneously working towards a number of objectives, including maintaining the confidentiality of ICT users, securing data integrity, securing the availability of data and information, and assuring authentication and providing non-repudiation (Menezes, van Oorschot and Vanstone, 1997). These objectives branch out into a more diverse range of goals and corresponding activities that are described in table 5.1.

The implementation of information security can focus on particular technologies that address critical issues from a problem-response or reactive perspective. As many information security threats fall into the category of cybercrime, their analysis from a legal perspective has much to offer as well, and indeed chapter 6 of this report provides just that. This chapter will however propose that information security has much to gain from using a risk management framework for information security, as it involves planning, foresight and focus on human resources, policy and process issues, as well as on actual security technologies.

Table 5.1

Information security goals and activities

Goals	Activity
Privacy and confidentiality	Information and data are rendered secret to all entities without an authorization.
Data integrity	Information and data cannot be altered by entities without an authorization.
Entity authentication	The identity of an entity is verified.
Message authentication	The source or origin of the information or data is verified.
Signature	An entity is bound to a particular message or data.
Authorization	An entity is given an official sanction to perform predefined activities using specified resources and for specified information and data.
Validation	An entity is given a time scope for performing on its authorization.
Access control	Access and privileges to data and information vary according to preset policies.
Certification	A trusted third party endorses information.
Time stamping	The time of creation, expiry or duration of validity of specified information or data is established.
Witnessing	A third party verifies the creation or existence of specified data.
Receipt	An acknowledgment is produced establishing that certain data or information have been received.
Confirmation	An acknowledgment is produced establishing that certain services have been provided.
Ownership	The legal right of an entity to use specified resources, data and information is established.
Anonymity	The identity of an entity using specified resources, data or information is concealed.
Non-repudiation	The denial of established and agreed commitments or activities is prevented.
Revocation	A specific certification or authorization is retracted

Source: based on Menezes, van Oorschot and Vanstone (1997).

2. Information security and communication

In order to fully appreciate the importance of information security, it can be useful to revisit our understanding of how our communications environment changes as we increase our use of technology.

The most basic form of human communication – spoken language among physically present persons – is endowed with a default level of security that we often take for granted. We usually know if our counterpart is a perfect stranger, a business partner or an old friend, and we habitually judge what level of confidence and trust to expect from the exchange. We will easily recognize a previous acquaintance by their appearance, behaviour and speech, and will seek and receive some indication that our counterpart has recognized us as well. Mutual authentication provides a platform of trust from which we can carry on with exchanges and discussions of substance.[4] Our physiological vocal limitations and conversational habits will limit the physical range in which a discussion can be heard and understood, and therefore guards its privacy to some degree. We would also consciously choose the level of privacy of our conversation.[5] Finally, unless it is recorded, the substance of the discussion evaporates and, at best, is committed to imperfect memory. A simple move to using written messages introduces new issues. It requires trust in the paper media to keep the message coherent, as well as confidence that the carrier transporting the message will carry out its function. The recipient needs to trust the authenticity of the message through recognizable handwriting, signatures, or a variety of stamps, envelopes and seals. Still, there is little to guarantee that a message will not be intercepted and perhaps altered, and the content copied and used beyond the scope of the author's knowledge, control or intent.

A fast-forward to modern digital communication technologies involves substantial adjustments in our behaviour, because these technologies make compromising the privacy and security of communication ever easier. Whether using the telephone or e-mail or simply browsing an interactive website, as opposed to receiving a letter or meeting in person, our confidence in who the other conversant is and the information they request or give, as well as the privacy of our exchange, may drop dramatically.

The use of digital communication technologies, while resolving the limitations of time and space, pushes to the extreme four fundamental problems. The first is that our capacity to authenticate – to be certain of the identity of our counterpart – can be severely reduced. The second is that using a communications infrastructure may compromise the privacy of the content of our exchange. The third is that it can be difficult, or nearly impossible, to establish whether the communicated files have been altered or tampered with during transmission. Finally, using digital technologies often leaves traces and trails pointing to the nature and substance of our exchanges, sometimes even lodging their full content on computer systems that are increasingly networked and accessed by many entities.

3. Why does it matter?

From a privacy and human rights perspective, information security issues matter and are being increasingly addressed through policy as well as through technology. Indeed, Article 12 of the Universal Declaration of Human Rights states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[6] More recently, United Nations General Assembly resolutions 55/63 and 56/121 specifically addressed the issues of endangering information security through cybercrime and framed the problem through the perspective of the UN Millennium Declaration and the role of information technologies in economic and social development, education and democratic governance.[7]

From a business perspective, information security issues are just as acute. Entrepreneurs or employees frequently enter into remote communications that require an appropriate level of trust that corresponds to the value of the underlying business and any associated risks and liabilities. Firms are public entities, and their public personalities are easily knowable. Firms also have exploitable assets whose value is often public knowledge. Thus, targeting their information security can be a fundamentally premeditated exercise – more so than in the case of individuals.

Governments have concerns similar to those of firms but with an overarching mandate and a fundamental responsibility towards citizens and organizations, since they administer data related to civil, fiscal, social security and other issues. Governments are often deeply involved in ICT infrastructures, at the very least from a policy and regulatory perspective, and more often in developing countries as owners and

administrators of communications and network infrastructures. While individuals and firms may be free to strike a balance between acceptable risk and investment in security technology and risk management, Governments may have absolute public policy and accountability considerations, in particular when they engage in a positive ICT development strategy and aim to support the development of e-commerce activities. Thus, understanding the security issues and the role of technology in creating trustworthy digital environments, conducive to e-business activity and benefiting the efficiency and quality of governance, matters.

A common problem for individuals, firms and public bodies occurs when the realization sets in that "something needs to be done". At this point advice may be sought on possible solutions. Individuals will struggle with off-the-shelf firewall and anti-virus software and decide to use encryption for their e-mail. They may even adventure to change their computer desktop environment and use free and open-source software (FOSS) in the hope that it will be more secure because its source code has been inspected and corrected by thousands of users and programmers. However, neither FOSS nor proprietary software provides any guarantees, much like a car manufacturer that cannot guarantee against car accidents. Nevertheless, there is an active debate about security and the openness of software and part E.2 of the chapter attempts to addresses more specifically the issue of risk avoidance through the use of FOSS.

Firms and public bodies will be approached by vendors, each touting its own cryptographic tools and security solutions, but what will ensure that the right choices are made? Furthermore, who can predict whether the technologies will be used correctly or perhaps in an unpredictable, harmful or even negligent way and thus compromise both security and security investments? Headlines announcing "Government ICT security shows worrying lapses" or "Survey finds 81% of computer users have a common password and almost 30% note their passwords down…"[8] may worry some but hardly surprise anyone. Good decisions will be assisted by a general appreciation of security technologies as they advance together with the development of the information society. Even better choices will be exercised by embracing a risk management framework, rather than simply dealing with threats on an ad hoc basis, often when some ICT catastrophe is looming.

4. Economic incentive

Every person, firm or institution will weigh their incentives for investing effort and resources in information security. Whether intuitively, on the back of an envelope, or using formal microeconomic or risk management analysis or methods, technology users will evaluate their assets, assess their environment and explore their expectations. The level of information security achieved will be a function of the incentives faced, rather than the available scope of technologies (Anderson 2001).

Incentive failure can lead to poor security. Varian (2000) pointed out that denial-of-service attacks on commercial websites could be stopped by users operating the thousands of zombie computers used in the attacks or by their ISPs.[9] However, incentives are lacking, as the asset under attack does not belong to the computer users and, in a tragedy of the commons scenario, there is no guarantee that any of the other zombie computers would be sanitized anyway.[10] Security can never be airtight and will cost real money and it takes just one discovery of a serious flaw by any one of half a billion Internet users to cause a major security breakdown and losses. When we consider this in the context of the digital divide, we see that firms and institutions from developed countries, as well as developing countries with strategic interest in technology development, will have incentives for using and developing security technologies. For developing countries that have only recently made progress in ICT adoption, disincentives may need to be counteracted with a positive policy approach whereby e-strategy frameworks need to be supported by domestic political commitment and through international policy and technical cooperation.

Moving to the supply side, the amount of security built into technology products may be suboptimal because of network externalities. First-mover advantages in markets that have high network externalities provide incentives for early if buggy releases. Compounding the problem is the conventional wisdom that security strength and usability are almost in contradiction with each other when it comes to desktop platforms and programmes that need to focus on being user-friendly. In other cases, where security is specifically required as a primary product feature, producers may have an incentive to go with proprietary solutions, rather than with tested public standards, in order to differentiate their product and lock-in consumers. Finally, software producers typically

decline any liability beyond the amount paid for the software, or its repair or replacement.[11]

Disincentives to reveal critical information abound and are yet another cause of suboptimal investment in information security (Cashell et al, 2004). Financial markets may react very negatively to news of security breaches, in particular those affecting financial services companies. A loss of reputation and consumer confidence can be detrimental. Firms that have suffered security breaches may fear litigation and will not have much motivation to release any details of the event. Security breaches may indicate that a firm is in violation of information security regulations or laws. A publicized breach of security may invite further attacks, as it could signal that defenses are weak in the firm and perhaps in the sector or region. Finally, technical personnel can be reluctant to report security failures if it may lead to getting fired.

A risk management approach to information security involves the economic assessment of the information assets at risk before looking at possible solutions. Thus, while it will not provide any additional incentives, it should clearly outline and define existing incentives and juxtapose them against the investment needed and the value of the proposed improvement of security. Once this has been done, policy processes at the level of a firm, an industry association or a Government, at the national or international level, may consider possible action to improve incentives for better information security.

C. The information security industry

The global information security market is estimated at around $40 billion, half of which is represented by the United States.[12] The corresponding estimates of economic damage caused by security breaches in 2003 vary from $12.5 billion for viruses only to over $200 billion for all forms of digital attack. While damage from viruses is likely to decrease because of better and broader deployment of anti-virus software, total digital damage is likely to rise if only because of the continuously expanding use of Internet-based technologies.[13]

While demand for information security may be sticky as spending on security technology increases, a decrease in such spending can be related to an overall decrease in information technology budgets. In this sense, the economic slump of 2001-2002 cooled all expectations of strong growth for the beginning of the decade. Sales of security technology accelerated after 2003 and are expected to account for 5 to 6 per cent of ICT budgets, which should reach $1 trillion before the end of the decade.[14] However, prudent pessimism may be the right approach, taking into consideration the various disincentives for investing in information security explained above.

The information security market is heterogeneous, with various firms developing particular mixes of security activities that broadly fall into four categories. The first is identity management. The second is securing communications and transactions either by using Internet-based virtual private networks[15] (VPNs) or public key infrastructures (PKI). A third sector is security information management – tools and processes that help organizations manage an often diverse and heterogeneous amalgamation of security technologies. Finally, application-specific integrated circuits are increasingly being designed and deployed to perform security-specific tasks, as in VPNs or firewalls, as hardware appliances, supplanting discrete security applications.

The security technology sector is not as concentrated as that of computer software or hardware. Nearly all software and many hardware companies provide services around their own or licensed security products, including industry giants such as IBM and Microsoft. Nevertheless, several companies have established themselves as market leaders in information security and are often cited as bellwethers for the sector. Table 5.2 gives an overview of several basic parameters for a number of these companies while omitting firms that generate important revenues outside the information security services niche.[16] The diversity in size is significant, with the largest companies providing comprehensive security solutions, while smaller ones occupy the innovative niches of biometrics or encryption technologies. From a financial perspective, since the dot.com bubble burst in March 2000, investors have generally not resumed the positive expectations for the sector that were common in the late 1990s, in spite of frequently alarming news coverage about the vulnerability of ICT networks, infrastructures and appliances brought on by a diversity of viruses, malicious codes and direct hacking activities.

The larger firms are well-known because they are industry leaders and produce popular anti-virus software and firewall systems. RSA Security is interesting

Table 5.2
Selected vendors of information security technology

Company	Market capitalization on 2 September 2005 *(billions of dollars)*	Revenue* *(millions of dollars)*	Number of employees *(2003)*
Computer Associates	15.74	3,600	15,300
Symantec	25.35	2,730	6,500
Verisgn	5.73	1,530	3,206
McAffee	4.99	94	2,950
Check Point Software	5.48	55	1,344
RSA Security	0.90	31	1,144
Entrust	0.35	98	491
Viisage	0.21	76	211
Identix	0.43	74	480
Watchdata Technologies	n/a	39	258

* Trailing twelve months.
Source: Yahoo Finance, Hoovers.com.

from a historical perspective. It was founded by Ron Rivest, Adi Shamir and Len Adleman, who pioneered the development of an algorithm for asymmetric encryption and signing and commercialized the first technology enabling PKI. A discussion on the RSA algorithm is presented in part D of this chapter. Verisign, a 1995 spin-off of RSA Security, is a diversified company that offers a range of ICT products and PKI services, and operates a large array of network infrastructure, including two of the Internet's 13 root servers and the generic top-level domains for .com and .net. Entrust is a Canadian company that develops PKI technologies and uses them for secure messaging, identity management, and authentication solutions. Viisage and Identix develop biometric authentication technologies. While most of the technology developments and use originates in developed countries, information security services are increasingly present in developing countries. For example, Watchdata Technologies, a Chinese company, has developed a proprietary smart card operating system and is a provider of electronic transaction applications, data security, and encryption and PKI technology. The service and interdisciplinary nature of information security provides opportunities for companies like WIPRO from Mumbai or Odyssey from Chennai, Comtrust from Abu Dhabi or Infocus Consulting Group from Buenos Aires, to establish and develop local business operations and seek growth in their regions and internationally. Box 5.1 provides an overview of information security issues in several developing countries.

Aside from firms, government and academic institutions are often heavily involved in information security and infrastructure development, since the issues of standards, interoperability and regulation validating the use of electronic signatures fall squarely within their research interests or political mandates. Examples of such activity are the EuroPKI project, the Dartmouth College PKI Lab or the Internet2 PKI Labs.[17] Outside the traditional business or mainstream public sector, information security technology is also being developed in free and open-source frameworks such as the Open Source Security Information Management project, the OpenCA Lab, CAcert or the Smartsign Project.[18] National computer emergency response teams (CERTs) have been established in many developed and developing countries, and their cooperation has been encouraged through various international agreements and treaties.

The sector will most likely be subject to a vast array of acquisitions aimed at diversifying existing business portfolios, as well as buying new or breakthrough technologies from more innovative and typically smaller companies.[19] While the current crop of firewall, anti-virus or PKI products will certainly maintain their brand profile, in the near term information

Box 5.1

Information security in developing countries: Mainstreaming Latin America? [i]

The need for information security in developing countries is growing constantly. Security has become a big issue today, not only because of school children trying to understand and embrace the cyber world but also because Latin America is suffering from organized crime which has discovered the virtual world as its new medium. Kidnap, ransom and fraud are some of the real world crimes that are assisted by information extractions from our ICT infrastructure with increasing frequency. This extraction of vital information from personal archives is often achieved without the concerned knowing about it. The need for information security is rising, and it will continue growing because of the change in social structures and commercial relations that technology has brought to everyday life.

In managing the challenges of information security, Latin American firms and Governments are investing in security technologies but are unfortunately under-investing in personal training for their employees. Having started with firewalls, many have moved to managed security services, and a fast-growing market is emerging for virtual private networks, intrusion detection, penetration testing and cryptography. In addition, the maturing of many open-source platforms and applications has led many companies to implement security by using software such as GNU/Linux, which can provide a solid, robust, fail-safe platform at very small cost.

If we look at particular countries, we see that there is a variety of experience. In Mexico, awareness building and security training in general is insufficient, and while companies are aware of the possible threats, they are not investing money for their security. Only government and financial institutions are willing to invest in information security. Nevertheless, demand for security consulting and education and training services is expected to rise during the next six to twelve months.

In Argentina, opportunities for ICT business are stabilizing, in part because North American and European companies are migrating their ICT product development there. Argentina today is increasingly playing host to international security firms such as Core Technologies, which has established a development centre in Buenos Aires that works on software applications for comprehensive penetration testing to accurately identify specific information security risks. This is, in turn, assisting the development of local ICT and security skills and transforming Argentina from a consumer market into an ICT producer market.

Brazil is perhaps the country with the highest potential for firms providing security training, security hardware, penetration testing, etc. In the past, the small size of the ICT security market was perhaps due to language barriers or commercial issues. Medium-size and large enterprises, as well as many government institutions, are now concerned about information security and have increasing economic resources to invest in it as their security awareness matures and financial strength improves. A good indicator is the use of the Internet for filing income tax declarations and Brazil has managed an impressively high level of 16.5 million fillings, representing 95 per cent of the total. This was achieved using Giss online technology[ii] developed by Eicon Auditoria e Consultoria LTDA, a 100 per cent Brazilian technology firm specializing in networked intelligence business applications.

[i] The overview was provided by Mr. Eduardo Moreno Lopez, Chief Executive Officer, Infocus Consulting Group, an information security consulting firm active in the Latin America region; http://www.infocuscg.com/.

[ii] See http://www.gissonline.com.br.

security is likely to be increasingly integrated in contracts for ICT network or infrastructure products and services. However, as security threats and challenges evolve with commercial and public use of IT, new threats and problems may require appropriately innovative solutions, and this could motivate the development of novel technologies and the entry of new competitors. From a developing country perspective, it is important to appreciate the dual growth opportunities resulting from an increase in security needs as local governments and businesses increasingly adopt the Internet as a communications and commercial medium, as well as the potential for innovation in the area of new security applications and technologies.

Developing a strategic and policy approach to information security requires, among other things, a basic understanding of what is on offer from the information security industry. Appreciating the current palette of solutions can be facilitated by understanding how they evolved within their own historical context, rather than by categorizing them according to technology or functionality type and diving into technical detail.

D. Development of security technologies

1. Early development

Security technology develops and progresses hand-in-hand with information and communication technology. As the written word was, in a sense, the first communication technology, cryptography became its security partner. For centuries it relied on simple

cyphers that used monoalphabetic transposition or substitution of letters to convert the original text into an encrypted cyphertext.[20] Monoalphabetic cyphertexts, by their nature, gave away data that could be statistically analysed and were thus easily unlocked without the cypher. But the security was good enough as long as a point-to-point transport (e.g. a private courier) was used instead of a communications infrastructure,[21] such as a postal service.

The first real change and challenge for modern information security came about with wireless communications, as the airwaves presented the first truly global and public communications infrastructure.[22] Wireless technology immediately drew the attention of military establishments, as instant communication meant remote command and feedback. Unfortunately, ease of communication also meant ease of interception (Singh, 2000), as anyone could eavesdrop on radio transmissions without any sign of an intrusion. The "public" nature of the airwaves rendered existing encryption technologies inadequate. What resulted was the development of mechanical computer or encryption "rotor" machines that produced polyalphabetic cyphertext based on keys. "Polyalphabetic" meant several substitution tables were used in the same message. A secret key indicated what number, sequence and combination of substitution tables were to be used. While polyalphabetic encryption was theoretically proposed as early as the fifteenth century, its mechanical "computerization" using rotor machines in the early twentieth century made it usable for everyday communications by operators uninitiated in the underlying mathematical complexities.[23] In practice, any two users that had the same encryption machine would merely have to synchronize the use of a secret key that, when punched in, would reset both machines to identical states that would then provide automatic encryption and decryption.

The most famous of all rotor machines was Enigma. It was developed by Scherbius and was awarded a patent in 1918. Mass production had to wait until after Churchill's *The World Crisis* was published in 1923, explaining the achievements of British cryptography experts and the resulting and detrimental high level of intrusion in German communications during the First World War. This realization prompted large orders of Enigma machines by the German military. Another historically important machine was the Lorenz SZ40/42. Somewhat more complex and less portable than Enigma, it produced text output on a teleprinter. The effort to crack the Enigma and Lorenz codes during the Second World War by allied cryptographers at Bletchley Park[24] using electromechanical "bombes" and the Colossus computer is important for security experts, as it draws attention to several fundamental issues that have not lost their validity more than 60 years later and are presented in box 5.2.[25]

2. Recent history

As the Colossus computer was top secret and a German prototype called Z3 was destroyed during the Second World War, the ENIAC – designed and constructed at the University of Pennsylvania between 1943 and 1946 – was deemed, for many years, the first fully electronic computer. The invention of the transistor and the resulting improvements in speed and reliability, the move towards binary logic and the development of programming languages in the late 1940s and 1950s accelerated the development of information technologies to the point where, by the late 1960s, many government and commercial entities began to rely on ICTs for data processing tasks and communications.

The development of the Internet and the universality of its protocols (e.g. TCP/IP, http, ftp) enabled the networking of disparate computer resources and further boosted intensity of use and innovation in computer technology. The problem with Internet-based communications is that they use infrastructures and public protocols that are, much like radio waves, easy to access but also open to interception. Furthermore, the Internet was designed to be failsafe and reliable while security was not given a high priority as, in its early stages, all the network nodes were trusted entities. Therefore, security needed to be purposefully designed and deployed in order to maintain the safety of data and information handled, as well as the integrity of the associated computers and networks. The question of the standardization of security technology arose in the early 1970s, when establishing a standard that would allow different institutions to communicate with each other became an important concern, as it could help avoid the complexity of establishing numerous bilateral protocols. Thus, in 1973 the United States National Bureau of Standards formally requested proposals for the establishment of a data encryption standard (DES) algorithm.[26] The algorithm that was eventually accepted in 1976 was proposed by IBM and was based on the work of Fiestel and his development of the so-called "Lucifer" cipher. The strength of the DES was eventually

Box 5.2

Lessons learned from the past – Still valid half a century later?

An obvious first lesson is that Enigma's security came from the strength of its keys, not the secrecy of its electro-mechanical design or encrypting process √ these were known quantities.[i] This axiom, often referred to as Auguste Kerckhoffs'[ii] second law, remains valid, and many present-day experts advise against placing excessive confidence in proprietary security systems that have not undergone public scrutiny, while recommending public-domain or free and open-source technologies (Diffie, 2003; Perens, 1998; Schneier, 2000). A misguided trust in secret systems and protocols is often referred to as ≈security through obscurity∆

A second lesson is that underestimating the technological capacity of your opponent is a source of failure. Cracking the Enigma and Lorenz codes was greatly assisted by brute force computing. Turing, a pivotal expert at Bletchley Park and considered by many to be the father of modern computing, designed a method of electronically interconnecting 12 Enigma machines into a device called a ≈*bombe*∆ By the end of 1942 there were 49 *bombes* in operation that were capable of cracking the current key within an hour (Singh, 2000; Khan, 1996). In order to crack the Lorenz cypher, Newman and Flowers set out to design and construct the world's first electronic computer. The Colossus could perform 5,000 calculations per second, thus helping to break the Lorenz code in about two hours (Good, Michie and Timms, 1945/2000).[iii]

A third lesson is that people are the weakest point of a security system. Breaking security often relies on human error and physical espionage; technology is needed but is insufficient. Cracking the Enigma cyphers often relied on ≈cribs∆√ an obvious match of non-encrypted text to encrypted text √ that could be found at the start or end of a communication in the from of a topic or greeting or from repeated transmissions of slightly altered messages using the same key and cypher. Physically stealing codebooks that contained key and transmission instructions and data was also a significant contributor to the success of Bletchley Park operations.

A fourth lesson is that security systems that do not actively monitor for suspicious traffic or interference, will fail. Hackers will avoid leaving trails or indications of intrusion. Intelligence from Enigma cracks was not always acted upon, and redundant scouting missions would be ordered to cover up the fact of a successful decryption.

---

[i] The user instructions for an early model of Enigma machine were revealed to the French authorities in 1931 by a disgruntled German government employee (Singh, 2000).

[ii] Auguste Kerckhoffs was a 19th century Flemish linguist and cryptographer. Kerckhoffs' law is widely embraced by cryptographers as contrary to ≈security through obscurity∆

[iii] The estimate is based on a quote from Anthony Sale, Director of the Colossus Rebuild Project, and as posted on the National Valve Museum website. See http://www.r-type.org/static/valvecpu.htm and the BBC news story on http://news.bbc.co.uk/1/hi/technology/3754887.stm .

improved through an increase in its key size from 56 to 168 bits in 1999, and the resulting standard is commonly known as Triple DES.[27] Today, that standard has been largely superceded by the Swiss-developed International Data Encryption Algorithm (IDEA)[28] and the Advanced Encryption Standard (AES) that was adopted in November 2001 by the United States National Institute of Standards after a five-year standardization process.[29] The main weakness of these systems is that they are symmetric: the same cryptographic key is used to encrypt and decrypt the communication, and this key has somehow to be shared between the two parties, thus providing a point of attack. Information security is decreasing with the increase in the use of and reliance on the Internet and telephony networks, and thus using these for a key exchange *and* the ensuing communication is a fundamentally flawed and unwise practice.[30]

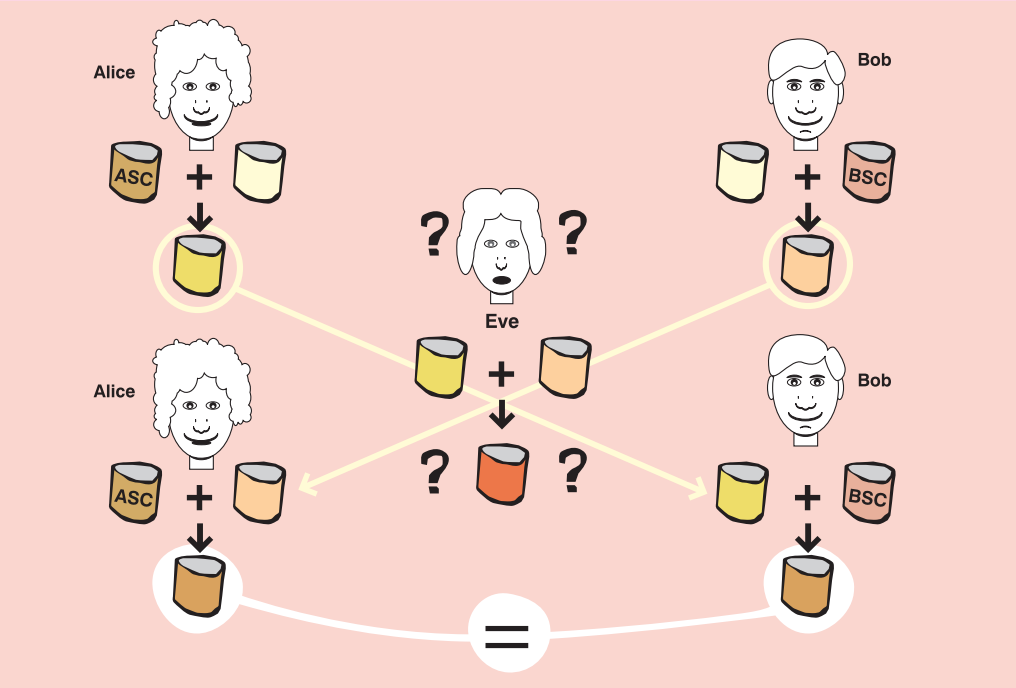
To resolve this problem, in 1976 Diffie and Hellman proposed a key exchange system in their seminal study *New Directions in Cryptography,* for which, together with Merkle, they received a patent in 1980.[31] The ideas presented enabled the evolution of a plethora of asymmetric key technologies and were foundational for the development of commercial and secure Internet use. The task was simple: how can two people establish and share a secret without telling it to each other. The partners in communication, often called Alice and Bob in cryptographic research, would each have a private and public key. The exchange of their public keys could be conducted over a public, non-encrypted, communications network. Once the public keys are exchanged, Alice and Bob would, each on their own, combine the other's public key with their own private key using a one-way mathematical function – a function that is difficult to reverse – to create the final key to be used to encrypt and decrypt their messages. The process is analogous to agreeing to a secret color of paint. Box 5.3 illustrates this example in more detail with an analogy proposed by Singh (2000). Details of the underlying modular mathematics are provided in the annex to this chapter.

Unfortunately, the so-called Diffie-Hellman key exchange was not practical for remote communications. Both Alice and Bob would need to enter into

non-encrypted contact, share their public keys and perform calculations in order to establish the common secret key, upon which they could start an encrypted and secure exchange. This system is also bilateral, as each pair of partners would need to establish a separate set of private and public key pairs, thus creating key management problems. The proposed solution to this problem was for Alice to have only two separate and distinct keys: a public key to encrypt and a private key to decrypt the message. The keys would be related, but it would be impossible, or more precisely unfeasible, to derive the private – and secret – key from the public one. If Bob wished to send a secret message to Alice, he would retrieve Alice's public encryption key from a public key repository and use it to encrypt. When Alice receives Bob's message she will use her private key to decrypt it. This process also solves the authentication problem: how can Alice know that a message is really from Bob? In this case Bob would do the opposite. He would establish a public-private key pair for authentication. His public key could be used by anyone to decrypt Bob's messages, while Bob would use his private – and secret – key to encrypt his message. Alice would retrieve Bob's public decryption key that, by definition, only works on Bob's messages, and a successful decryption would therefore confirm that the message could only be from Bob.

Box 5.3

A colourful public key exchange system analogy of Diffie-Hellman



Both Alice and Bob start off with a litre of identical paint to which they each add another litre of paint of a secret color. They then swap the two- litre mix and to each add another liter of their own secret colour. They should now both have the same colour. An eavesdropper, often called Eve, would find it very difficult to discover the new secret color even if she intercepted both exchanges: it is plainly difficult to unmix paint, at least with the same technology used for mixing it. Even if Eve intercepts the pots, she cannot learn their key. She can get hold of what Alice sends (Y + ASC) and what Bob sends (Y + BSC), but she has no way of removing the yellow from either pot, and no way of combining the two to get the secret colour. If she mixes them, she will end up with 2Y +CA+CB, which is altogether too yellow. There is also no way of knowing which precise shade of yellow, blue or green was used to mix up the public colors; indeed an infinite variation of different greens and yellows can be used to produce Alice's public lime green or Bobs aquamarine (Singh, 2000).

The mathematics allowing the derivation of such a public-private key pair were developed by Rivest, Shamir and Adleman (RSA) while working at the Massachusetts Institute of Technology Laboratory for Computer Science and were published in 1977.[32] The RSA system relies on a *public key* that is arrived at by multiplying two prime numbers – a number that can be divided only by 1 and by itself.[33] The *private key* is derived using the original pair of prime numbers. If the prime numbers are sufficiently large, say 100 digits each, and thus produce an enormous public key, it becomes unfeasible to discover them. In 1977, a challenge appeared in *Scientific American* magazine asking its readers to discover the two prime numbers that when multiplied give a number 129 digits long. At the time of the challenge it was thought that the prime pair would never be found. The pair was eventually calculated in 1994, thus enabling the key to hold up for 17 years (Atkins, Graff, Lenstra and Leyland; 1995).[34] RSA Laboratories have continued posting challenges and prizes for factoring ever-larger keys. Currently, the largest cracked key is 174 digits or, in binary form – 574 bits long, and its pair of primes was discovered by Franke and Kleinjung in 2003.[35] It is widely accepted that minimum encryption security needs a public key at least 309 digits or 1,024 bits long.

Asymmetric key systems coupled with ever-increasing key size currently provide reliable security.[36] However, in practice they are often used to encrypt and decrypt a more efficient and smaller symmetric key, such as the aforementioned IDEA or AES, instead of the actual message.[37] This was the approach used by Zimmermann when he set out to design Pretty Good Privacy (PGP) – a widely used e-mail encryption and authentication (i.e. signature) tool. Before PGP, cryptography-based information security was the domain of large corporations and government. PGP allowed individuals using personal computer hardware to take advantage of security technologies. PGP ran into several problems early on. One issue is that PGP provides full privacy to all citizens, including those engaged in legally questionable activities. Thus, if government security authorities wish to monitor communications, they would need to find some way of obtaining the private key beyond reverse engineering the public key. A range of solutions have been debated without convincing outcomes – from the creation of a government key escrow repository to embedding hardwired or software "back-door" technologies in appliances, ICT infrastructures and programmes.

While developments in cryptography algorithms often receive significant attention in professional and, on occasion, popular media, the true workhorse of online security applications is the cryptographic hash function. A hash function takes a data string of any length as an input and produces a fixed length data string as an output – a digital fingerprint. In conjunction with public-key algorithms, hash functions are used for digital signatures and integrity checking. In 1990, Rivest invented the MD4 hash function that was eventually evolved and adopted with modifications by the United States National Security Agency (NSA) as the Secure Hash Algorithm (SHA) in 1993. In 1995, the NSA revised SHA to SHA-1, which remained unbroken until February 2005.[38] SHA-1 is employed in a large variety of popular security applications and protocols, including the Secure Socket Layer (SSL) and its successor the Transport Layer Security (TLS) protocols used to secure the transfer of payment data in e-commerce, the Secure Shell (SSH) programme and protocol for network log-in and access, the S/MIME public key standard for signing email, and IPSec – a standard for securing Internet communications by encrypting and authenticating data packets,[39] thus providing security at the network layer and enabling the design and implementation of VPN infrastructures (Schneier, 1996).

Other notable developments include the ElGamal encryption algorithm of 1984[40] and elliptic curve cryptography. An evolution of the Diffie-Hellman key exchange system, ElGamal was used as the base for the NIST Digital Signature Algorithm (DSA) (Adams and Lloyd, 2003) and in the GNU Privacy Guard – a free and open-source personal cryptography tool and replacement for PGP.[41] Elliptic curve cryptography (ECC) was pioneered by Koblitz and Miller in 1985.[42] The main benefit of ECC is that under certain situations it uses smaller keys than other methods – such as RSA – while providing an equivalent or higher level of security. Use of ECC is still in its early phases, perhaps because its key algorithms are still subject to patent protection (Zwicky, Cooper and Chapman, 2000).[43] Its best-known use is in the Blackberry handheld e-mail device.[44]

In conclusion, cryptographic technologies are being used to achieve many of the goals of information security described in table 5.1. They have served historically as a starting point for reflecting on information security concerns. They have become so successful that security threats have adapted and evolved to take aim at weaknesses beyond actual cryptographic

technology. While it is inconceivable for Eve to unmix the paint in the illustration in box 5.3, she may decide to continuously taint the paint exchange, for example by adding her own colors, and frustrate Alice and Bob's dialogue to such an extent that they will give up on their scheme and revert to using unsecured paint exchange. Or she may befriend Bob. Or corrupt Alice. Or get a job in the paint factory.

3. Current issues

Given the steady improvement of cryptographic technologies, one would be forgiven for being puzzled at seemingly everyday news about some criminal or malicious event compromising some well established and regarded commercial or public institution's computers and data. Headlines such as "Instant messaging viruses and worms up 271% in Q1 2005"[45], "Have hackers recruited your PC?"[46] or "Cost of malware soars to $166 billion in 2004"[47] have become commonplace.

The world of Alice, Bob and Eve has changed. Until recently, the use of ICTs and the need for security was limited to the few that had access, usually as tools for their professional activities. Cryptography may have been the main and usually sufficient tool used to provide security. In contrast, today's computers and computer-like appliances, the Internet, and the software that runs them are commonplace. Cryptography seems to be less effective in an environment where multitudes of unsupervised users develop a broad spectrum of interaction with ICTs. Security threats have thus moved away from exploiting weaknesses in technology to exploiting weaknesses in the *use of technology* (Schneier, 2000) – a fertile field of opportunity, in particular when we consider the positive growth of the Internet population in developing countries.

This shift means three things. First, it alerts us to a general need for education and awareness building about information security issues and how we encounter various threats at home, in our private lives, as citizens, as firms and as public entities. Public policy and government action may follow with varying levels of practical application. Secondly, it highlights the need to adjust national legislation and international conventions to accommodate and deter malevolent activities. Chapter 6 of this Report, on cybercrime, as well as chapter 6 in UNCTAD's *E-Commerce and Development Report 2004*, on protecting privacy rights, describe recent developments from a legal perspective. Thirdly, and most importantly, the approach to information security is changing from a technology focus to a risk management focus. Still, the technologies themselves remain important, and their scope and use will be briefly described within the risk mitigation component of an overall risk management approach to information security in the following section.

E. Information security and risk management

Risk is the uncertainty as to the outcome of an event when there are several possibilities (Outreville, 1997).[48] In other words, risk is the variability of an occurrence of an event around its statistical probability. The larger its uncertainty, or variance, the more risky the event is. In less formal terms, risk is a "... condition in which there is a possibility of an adverse deviation from a desired outcome that is expected and hoped for." (Vaughan, 2002) The objective of risk management is to devise and implement a system that will support the operational and financial stability and effectiveness of an individual, firm or public body in the case of an unfortunate, loss-generating event. In practice, risk management is the process of identifying and assessing risk and developing strategies to manage it – i.e. to decrease variance. A risk management strategy would be a defined process that would guide us through several decisions.

Initially we would need to identify and quantify a risk. After this first phase of risk assessment, we may try to find ways to avoid the risky event – often referred to as a "peril" in risk management literature. We would also attempt to lessen the hazardous conditions under which the peril materializes. Having exhausted avoidance options, we may try to find ways to reduce the frequency of the threats and the severity of the damage we may face, if and when the peril materializes. This often relates to using safety and emergency features and tools. Inevitably, we must accept that some damage will occur at some point, and we may choose to transfer some risk using insurance, thus securing a source of financial compensation for part of the loss. Having done all this, we have probably reduced the potentially negative financial outcome of the risk to such an extent that we can decide to internalize what remains within the cost structure of the core business. Chart 5.1 outlines the basic elements of the risk management process flow.

In order to gain some insight about implementing a risk management approach to owning and using ICTs,

it is useful to highlight the basic elements of the process in greater detail. In practice, risk management can demand inputs from diverse fields and competencies and thus should not be limited to exchanges between management and technical staff, such as network administrators or programmers. The same will apply to government policy and governance: a risk management approach to information security policy is multi-stakeholder by nature.

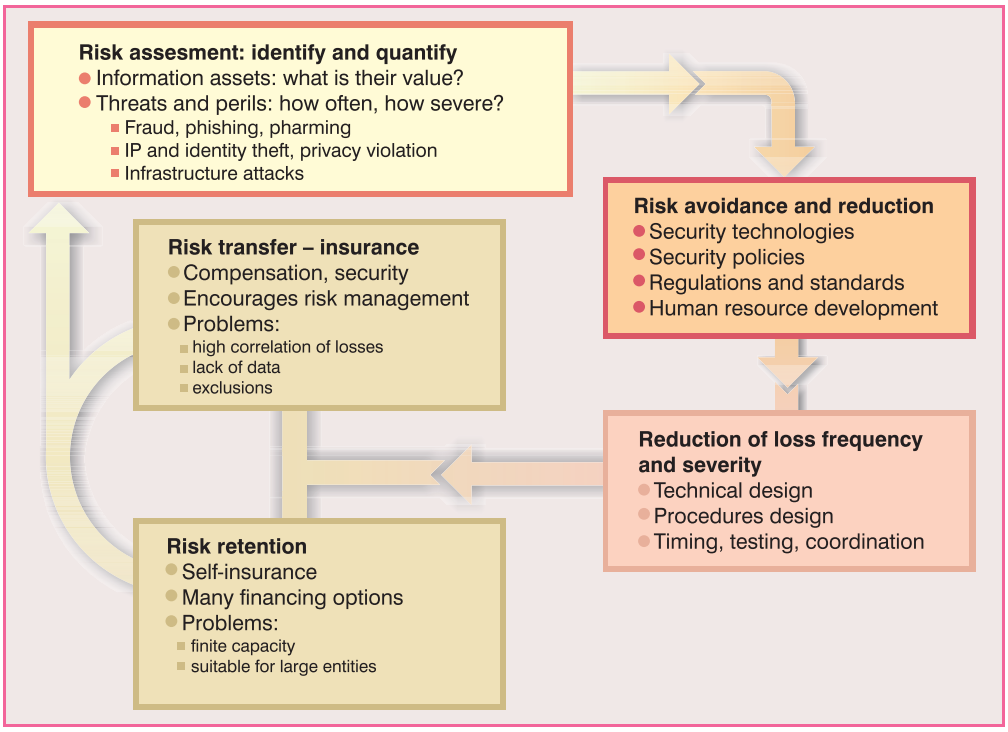
1. Risk assessment

In order to use a risk management approach, it is fundamental to define risks, to evolve ways to keep risk perceptions current, and to measure or develop methodologies to quantify risks. It is immediately apparent that the task at hand may be more difficult for information security and ICT risks than, for example, for physical property risks. Part of the problem lies with the ever-expanding scope of use of ICTs. It is therefore important to maintain flexibility and alertness to the changing notions and categories of information assets and threats. At the same time, Governments and their statistical offices may choose to institutionalize some aspects of information security risk measurement within their efforts to provide quantitative data for policy makers involved in information society and economy issues, in the same way that physical traffic data will be complemented by statistics on traffic accidents. Chapter 1 of this report provides an overview of current progress in e-measurement issues.

In order to establish a risk, it is important to define the asset and the perils and threats it is subject to. From an information security perspective, assets can be data, software, hardware and network infrastructure, and the resulting connectivity. General accounting concepts such as those applied to physical assets will have difficulty accommodating information assets, as the cost of the technical components of an information technology system will not be a measure of its value. Resolving the problem of how to evaluate information assets may require a major review of accounting practice to include intellectual capital and to evaluate information in the light of its contribution to management or to core financial indicators, in particular if information products or services are an inseparable part of a firm's main activity or business (Wilson, Stenson and Oppenheim, 2000). A number of approaches have been proposed for short-term evaluation of intangible intellectual assets, such as market capitalization methods, whereby the difference between a firm's market capitalization and its stockholders' equity is the value of its intangible

Chart 5.1

Risk management and information security



assets, or return on assets methods, whereby the earnings of a company in one period divided by its tangible assets value and then compared with the industry average, with the difference indicating earnings from the intellectual capital (Sveiby, 2004). The problem of isolating the information asset component from the intellectual capital is also unresolved. It is also obvious that these methods are limited in that they would apply only to publicly listed firms. The use of hedonic demand theory has been proposed for valuing information technology investment in public sector organizations (Cilek, 2001).[49]

By comparison, defining perils and threats seems simpler. Threats usually appear as disclosure, modification, loss or destruction, and interruption of one or several information assets. A risk management approach requires research and analysis of possible threats to information security. The research should consider and evaluate sources of threats and perils that relate to an entities interaction with people, operational processes and the deployment and use of technology (Siegel, Sagalow and Serritella, 2002). It requires an estimation of frequency: how often do particular threats occur during, say, one year? Furthermore, the determination of maximum exposure is also necessary: what is the worst-case damage scenario per threat? Answering these two questions is an exercise specific to a firm or institution, and generalizations are therefore difficult to make. Information security threats may present themselves as one or a combination of several risk types.

First party risks manifest themselves as losses arising from the damage, destruction, temporary malfunction or corruption of an entity's own information assets.

Third party risks materialize as losses arising from liability claims against the entity, its management or employees. These can include a broad range of perils such as distributing malicious code or breach of privacy related to, say, credit card information or health records. Thus, third party claims can result directly from security failures.

Business interruption risks are those that prevent a planned or contracted delivery of goods or services. From an information security perspective, business interruption risks will be affected by infrastructure risks, and this may be influenced by a number of factors, such as a diversity of hardware, bespoke and proprietary software, overall reliability and uptime, and the ultimate dependency of business processes on ICT infrastructure.[50]

Reputation risks occur when a firm suffers damage to its reputation or brand identity. They are sometimes considered separately because they can be difficult to assess as they involve quantifying difficult variables such as expected business revenue or future market capitalization. More practically, they may need to be treated separately, as insurance cover for first party risks is unlikely to cover this class.[51]

Catastrophic risks can generate losses of such severity that, should they occur, they can on their own terminate an entity. As such, if suffered by an entity, they necessarily render its business or activity unsustainable.[52] Accordingly, actively managing catastrophic risk often leads to using risk transfer mechanisms, such as insurance. From an information security perspective, catastrophic risks can affect users, perhaps more so than ICT service providers. A typical case would be identity theft or theft of confidential information. From the perspective of an ICT service provider, data services and even certain information security applications can create *catastrophic points of failure* if they function using centralized databases and thus become identifiable targets for attack. However, beyond an irrecoverable breakdown or clogging up of the Internet, very few risks can be termed truly catastrophic in the traditional sense, as the value of ICT services is only partly reflected in the value of its technical infrastructures.

It is important to note that not all entities in all countries will be subject to the same perils, nor will the same threats appear with similar frequency or severity. In spite of global interconnectivity, differences in the value and nature of underlying information assets and in the thoroughness of the implementation of a risk management strategy will result in vastly different outcomes. Table 5.3 uses an example of three Asian countries to describe just how varied these may be. Such differences among developing countries should be expected, as they would necessarily reflect the diversity of their development and adoption of ICTs in everyday social, business and governance activities.

An overview of several known threats and perils that may present one or a combination of the outlined risks follows. Their scope and numbers are not fixed. Some overlap is possible, and new threats are likely to develop in the future. All of the listed threats can present one or several of the described types of risks.

Table 5.3

Security attacks by type of threat in 2003

	China	Thailand	Malaysia
Number of reported incidents	28.424	386	4.294
Type of attack as a % of reported incidents	25.35	2.730	6.500
Virus or worm	5.73	1.530	3.206
Spam	4.99	94	2.950
Scans of probes	5.48	55	1.344
Denial of service attacks and Intrusion	0.90	31	1.144

Source: APCERT Annual report for 2003, MyCert.org.my.

Fraud

Fraud regularly attracts media coverage, as the consequences are easily described in money terms, rather than in terms of technology. Fraud is the crime of deliberate deception in order to unjustly obtain property or services. Quite a few threats fall into this category. Credit card fraud is the classic example and continues to grow with the development of e-commerce activities. Recent reports indicate that merchants from the United States expect to lose an estimated $2.6 billion to online fraud in 2004, $700 million more than in 2003 and more than the prior fraud loss record of $2.1 billion established in 2002.[53] Recent reports also indicate that almost 85 per cent of fraudulent transactions on the Internet originate from computers in the United States. Canada is in second place with 5 per cent, while Australia, Germany and Japan hover around the 1 per cent mark.[54]

Phishing and pharming

Phishing is a more recent phenomenon. It consists of masquerading as an official-looking and trustworthy telephone service, e-mail or website in order to acquire someone's sensitive personal information such as passwords and credit card details. According to a recent Anti-Phishing Working Group (APWG) report on phishing activity, 37 per cent of phishing web sites were hosted in the United States. China was in second place with 28 per cent and the Republic of Korea was third with 11 per cent. Other top countries were Brazil with 4 per cent, Germany with 3 per cent, Japan with 2.5 per cent and Canada with 2.3 per cent.[55]

Pharming is the exploitation of vulnerability in domain name server software that may enable a hacker to gain control over the domain name of a legitimate web site (e.g. Unctad.org) and to redirect traffic from that web site to another bogus, defamatory or competitive web site. If the phony web site is a copy of a website of a trusted organization, such as a bank, a hospital or a government institution, it can be used to phish users' passwords, personal identity numbers or account numbers and gain access to their personal data or access to the organization's computer resources.

Infrastructure threats

At a basic level, infrastructure depends on the reliability of power supplies, hardware, operating systems and network connectivity. This issue is often of concern to developing countries, as it underlies efforts to establish universal access to ICTs. However, the energy crisis in California during 2000 and 2001, and the accompanying shortages and price volatilities, indicates that even in developed countries, overconfidence can be misguided and risk management should not assume away risks related to the provision of public utilities.[56]

This category also compromises the whole range of viruses and worms – often jointly referred to as malware – and any other type of attack aimed at destroying or seriously reducing the functionality of ICT resources. Often, the objects of attack are particular software applications or websites and portals. Material gain may not be an objective, although reports have recently surfaced of blackmail advanced by criminals threatening to take down websites using denial-of-service attacks if demands are not met.[57] The major vendors of anti-virus programmes maintain current information on the activity and danger level of various types of malware. A number of portals monitor ongoing developments in common applications, such as operating systems, web servers and database applications. Attacks will aim to take advan-

tage of an unintended functionality to cripple or gain control over an ICT system.[58]

Intellectual property theft

This is an important and significant issue in itself. UNCTAD (2003, 2004) has described the intellectual property issues that occur when the Internet interfaces with software development or the music industry, and has considered the issues related to domain name assignments and disputes from a trademark perspective. Here too, the democratization of computing power and the availability of bandwidth change everything. While it is perfectly reasonable that individuals, firms and organizations want to control the distribution of and access to any creative content they may produce, such control is "...contrary to what the digital world is all about" (Schneier, 1996). The Internet is functionally and fundamentally designed to facilitate the copying of files using a robust communications infrastructure: even the simple act of viewing a web page means that a browser will copy a file from a server into its local memory and often hide an extra copy (in its "cache") on its hard disk in order to speed up browsing. Creative content industries and organizations may appreciate these notions and choose to consider them within their risk management strategies.

Identity theft

Identity theft is the deliberate assumption of another person's identity. The underlying problem is that, as technology increases its use of identity recognition, identity theft becomes a more commonplace and tempting criminal activity. For individuals, identity theft can present a catastrophic risk. People whose identities have been stolen can spend enormous time and resources re-establishing their good name, credit and legal record. In the meantime, they may lose job opportunities, be refused finance, education and other benefits, and they may even get arrested for crimes they did not commit. Techniques for obtaining identification information range from rummaging through rubbish to infiltration of organizations that store large amounts of personal information. Identity theft often works together with privacy violations.

Privacy violation

Privacy violations can be divided into targeted attacks and data harvesting. Targeted attacks are difficult to defend against, in particular if the attackers have large resources at their disposal. The digital nature of communications also allows attackers to leave few if any traces of a violation, making post-event detection difficult. Therefore, defenses must be pro-active and based on monitoring. Cryptographic tools may also be useful to the extent that the data and the associated ICT infrastructure are under the control of the owner. Using encryption in e-mail correspondence is one example – provided the recipient is trustworthy and exercises a similar level of prudence. Aside from violating content, traffic analysis of Internet-based communications can reveal significant information. Changing reaction times, message lengths and patterns of communications can indicate activity and organizational or command structures.

Broad surveillance activities coupled with data harvesting are generally increasing and are becoming easier with improving technology and increasing technology use. Wireless LANs can easily be subject to surveillance. A biometric identity system can exclude unauthorized staff from company premises, but it is necessarily powered by a database of personal details that, in itself, can become a point of attack. Commercial entities can, and often do, record and track everything purchased with a credit card. E-commerce firms use such private information to propose a more personalized level of service, but at what cost to privacy? More and more data are being collected as people leave increasingly larger digital footprints during their online activities. Legislation protecting privacy and databases can be an important deterrent and has been discussed in a previous edition of this report (UNCTAD, 2003).

Regulatory threat

Compliance with new and expanding regulations on information security may be seen as a threat in the sense that it may require adjustments in operations and improvements in security, security audits and certification, and corresponding expenses. Regulatory change may also be perceived as a threat if requirements evolve to become significantly different in one country or when required adjustments are above or even contrary to regulatory requirements in other countries. However, regulation can be better appreciated as a policy tool for risk avoidance and hazard reduction and will be discussed as such in the next section.

2. Risk avoidance and hazard reduction

Risk avoidance and hazard reduction policies and activities will be developed on the basis of a successful understanding of the frequency and potential damage of predetermined information security threats. They may span a wide range and would include:

- Using information security technologies;
- Developing institution-level information security policies and procedures;
- Implementing information security regulation and self-regulation; and
- Training and developing human resources to understand information security and use the technology, execute information security polices and comply with regulations.

Information security technologies

The development of modern security technologies was described in part D of this chapter. Most of that discussion covered the development of cryptographic tools and applications, as these were central to most security concerns until recently. Part D.3 noted that the Internet and the ubiquitous use of networked computers introduce greater diversity in the security technology landscape, which necessarily corresponds to the increasing diversity of security threats.

Information security technologies can be categorized by the object they control or monitor. The five basic categories are:

- System access controls;
- Content access and cryptography controls;
- System integrity controls and monitoring;
- System audit and monitoring technologies; and
- System management controls.

An individual, firm, or public or civic organization will need to implement a certain mix of several of the listed technologies. Not all of these technologies will scale perfectly, and their successful use will depend on the ICT readiness of administrators and users. It is important to implement several technologies at the same time, thus creating security density and depth through a layered system. System access controls restrict access to computer resources to authorized users. Content access and cryptography achieves a similar goal but can make fine distinctions in terms of the accessibility of particular information and content, and authorization can be generated by individual users as well as administrators. System integrity and monitoring defends against unwarranted and often illicit modification or corruption of system and data files. System audit and monitoring technologies are used to investigate security breaches and their impact. System management controls are used to effect and verify security settings and implement defensive measures when encountering a threat. Box 5.4 describes the individual technologies in brief. Public key technology and free and open-source software merit some additional attention, as they have been advanced as solutions for improving information security, with public key technology being particularly necessary for developing e-business activities (UNCTAD, 2001, 2003).

The technological development of asymmetric key or public key cryptography was discussed in part D.2 of this chapter. In application, public key cryptography may use an infrastructure to provide for third-party confirmation of user identities and the matching of public keys to users. The purpose of a public-key infrastructure is to manage keys and certificates and consists of a public-private key pair generator, a registry and a certification authority.[59] Going back to the traditional naming scheme, Alice will register her identity and request a key pair. Alice will then digitally sign messages using her private key. Bob, the recipient, will read the digital signature using Alice's public key, which will be certified as belonging to Alice by the PKI's certification authority. The certificate will unambiguously match up Alice to her key because Alice has already established her identity with the PKI's registrar. Thus, Bob will have established the integrity and authenticity of the message without having exchanged any secret information in advance with Alice. Certain definitions of public key infrastructures will include the legislation on electronic signatures (Ford and Baum, 2000).

There is a diversity of PKI infrastructure types, and firms and Governments are often presented with difficult choices on what could be a good match for their activities and would scale well. Questions as to how many certification authorities there should be, whether there would be a hierarchical relationship between them or would they be peers, how they will relate to certification authorities in other PKIs etc., await managers and administrators.[60] Given the sometimes impenetrable complexities and corre-

Box 5.4

Information security technologies

1. **System access controls** are designed to exclude unknown or unauthenticated and unauthorized users from gaining access to computer system resources and forbidden data and content from entering into the system. In this sense, all five categories of security technologies can be broadly understood to be access controls. Passwords are an authentication tool, as are biometric tools and smart cards and tokens. However it may be exaggerated to call them a security technology, given that they favour convenience at the expense of security.

   Firewalls control communication between different zones of trust. Typically they are placed between zones of no trust, such as the Internet, and zones of high trust, such as a firm's internal local network. Firewalls prevent or allow communication according to a prescribed security policy.

   Content screening applications monitor communications for inappropriate content such as Spam or unauthorized file types and thus deny access to content that may be offensive or constitute a non-productive use of resources.

   Biometric security tools measure and analyse personal physical characteristics, such as fingerprints, eyes, voice or facial patterns, signature, gait and keyboard typing patterns that are processed for entry into a database. Authentication will require a match between the user requesting access and one or several biometric characteristics stored in the database. Biometrics have raised concerns about privacy, as the databases contain personal data. From a risk management perspective, if the databases are centralized, they then present a single point of potential catastrophic failure.

   Smart cards and security tokens are distributed devices that store and process authentication data and have some level of imbedded cryptography technology. They will typically be used in conjunction with a personal identification number or a biometric screen and this may, to some extent, decentralize the access authentication process and thus ease catastrophic failure concerns.

   Rights and privileges policies are designed to give authenticated users access to particular data or resources. This process is often called authorization √a process by which one entity attempts to confirm that another entity is allowed access and thus becomes a trusted party.

2. **Content access and cryptography** controls embrace digital signatures and certificates, encryption applications and the use of virtual private networks. They are different from the access controls described above in that they function within existing system resources and their policies can be highly individualized and controlled by actual users or groups of users.

   Digital signatures are electronic signatures that use some cryptographic technique to assure the integrity or authenticity of a message. Public key cryptography has become the choice technology because it removes the need to establish public-private key pairs between each and every party; in this sense it is a multilateral rather than a bilateral construct.[i]

   Secure virtual private networks (VPN) are private communications infrastructures providing remote users with the functionalities of a local private network. A secure VPN will tunnel a private communications network through a public one, such as the Internet, by encrypting and authenticating all data packets using security protocols such as IPsec, SSL or PPTP. IPsec has become a part of IPv6, the new protocol standard for Internet traffic.

3. **System integrity controls and monitoring** applications consist of anti-virus software and integrity checkers. Anti-virus software attempts to detect foreign and malicious applications that may try to corrupt, destroy or exploit a user's computer or data. Integrity checkers monitor any alterations to files that are considered critical to the system.

4. **System audit and monitoring technologies** include systems for intrusion detection and prevention, event monitoring and forensics. Intrusion detection and prevention will identify inappropriate, incorrect, or anomalous activity on a network or computer system and will take action to prevent them from being successful.

   Monitoring applications will document actions on network devices and analyse the actions to determine if an attack is ongoing or has occurred, which enables an organization to determine if and with what effectiveness information security activities are operating according to prescribed security policy.

   Computer forensics tools are used to identify, preserve, extract, and document computer-based evidence.

   Countermeasure applications or aggressive network self-defense are a set of graduated responses that include strike back capabilities.[ii]

5. **System management controls** include applications that assist administrators to enforce security policies, manage computing resources, provide failsafe continuity of operation, scan for vulnerabilities and provide remedies. System controls consist of a number of distinct tools and applications.

   Policy enforcement applications enable system administrators to engage in centralized monitoring and enforcement of an organizations security policies.

   Network management tools are used to control and monitor networks, including the management of faults, configurations, performance, and security.

   Continuity of operations is supported by a scope of tools that provide for a complete backup infrastructure to maintain the availability of systems or networks in the event of an emergency or during planned maintenance.

   Scanners are tools that analyse computers or networks for security vulnerabilities.

   Patch management tools acquire, test, and apply multiple patches to one or more computer systems.

[i] Electronic signatures are a broader category and may include cable and Telex addresses, as well as facsimile transmissions of handwritten signatures.

[ii] For more details on countermeasure application, see Nathan (2004).

sponding difficulty in matching existing PKI solutions to market needs (Gutmann, 2002), it may not come as a surprise that the deployment of PKIs has not met the expectations of the late 1990s.[61]

In recent years, a number of IT firms or firms notable for their intensive use of information technology have been increasingly using free and open-source software (FOSS), in part because of perceived security benefits. The software used is often for infrastructural computing tasks, such as operating systems, web servers or database applications. When assessing competing proprietary and FOSS applications for security, technical experts and decision makers will need to appreciate the various quantitative and qualitative issues that make cross-comparisons between software difficult. A security flaw can attract few or many attacks. Flaws may be more or less critical, depending on the amount of damage they invoke. There is therefore a certain scope for judgment and for weighing the different factors in a final evaluation of comparable solutions. There is also the subjective user experience to contend with, as the most dissatisfied users are the most vocal ones as well, while it is entirely possible that the majority can be untroubled or content with a programme's security performance. Anderson (2002) suggests that there should be no difference from the perspective of achieving technical reliability, all other things being equal. However, in practice things are not equal, and due to information asymmetries, network effects and imperfect markets, actual outcomes may vary. UNCTAD (2003) has analysed these issues and suggests that the FOSS development model may have some hypothetical advantages, while there are no practical guarantees. Wheeler (2003) advances that FOSS has more security potential.[62] Free and open code allows users to inspect and fix bugs, including security vulnerabilities, should they have the resources and competencies. Certain FOSS applications are less likely to be targets of attacks because of either design principles or their still relatively small install base.[63] Malicious hackers would logically choose to exploit systems that have been broadly deployed, as this increases the chances of success. As previously noted in box 5.2 of this chapter, the simple fact that certain technologies are proprietary and that their inner workings and logic are not easily knowable is not a security feature. On the contrary, the secret source code of proprietary software may in itself be a security liability, in particular when public reporting by third parties on exploits and vulnerabilities may be in conflict with anti-circumvention provisions of international treaties and national legislation.[64]

Policies and procedures

An information security policy is a document that defines the rules and requirements that must be followed and met and identifies what behaviour is appropriate when accessing the computing resources of an institution. A policy will document potential threats and define responses to a security attack or failure, often specifying detailed procedures for particular types of incidents or security breaches. Information security policies are a fundamental component of and an input into the risk management process. In order to be successful, information policies need to be integrated into institutions' and companies' overall strategic and operational planning and procedures.

Policies will usually address very specific use issues such as "acceptable use" or "dial-in access", and should outline what tools and procedures are needed to deal with them. It will often be important to have policies define and communicate a state of consensus reached between users and administrators, as the ownership of a policy will be crucial to its success. Information security policies provide a foundation for human resources development, as their design can help identify where training and education may be needed to meet the policy's requirements, as well as broader issues related to the use of computer technology. The process of policy design will also define responses for certain types of behaviour of users and administrators that are incompatible with its prescriptions. Accordingly, a policy will also serve as a reference for establishing factual circumstance in the case of a policy breach.

Information security policies may be constructed in accordance with an international standard of best practices, such as ISO/IEC 17799, in particular where international commerce will depend or indeed focus on information technology. Such standards and related regulations are discussed in the next section. There are also technical standards, such as the ITU X.800 series; these will not be explored in this chapter.[65]

Self-regulation

Self-regulation is established through standards and voluntary quality certifications. Their function is dual: they indicate a certified level of performance, and they present a path for improving managerial and operational activities. Self-regulation can have a number of potential advantages over government

regulation. It can be easier to evolve and faster to implement. Commitment may be stronger when the actual stakeholders participate in its conception. It is often in response to a market need, and funding may be more accommodating from those with a vested interest in its success. There are a number of standards that may be used.[66] The discussion will however focus on a selected few that seem to be attracting particular attention from specialized media.

The International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 17799 standard issued under the title "Information technology - Code of practice for information security management" is an important information security standard. ISO/IEC 17799 was published in 2000 and a revision is planned for 2005. It provides best practice recommendations for initiating, implementing or maintaining information security management systems. ISO/IEC 17799 specifically addresses a number of issues, some of which have been discussed in this chapter, such as security policies, asset classification or access control. For each issue, objectives are specified and best practice means of achieving them are outlined. Specific actions are not recommended, as an institution seeking certification is expected to perform an information security risk assessment before selecting actions relevant to its information security profile. ISO/IEC 17799 has a number of equivalent national standards.[67]

Another international standard for computer security is the Common Criteria, also registered as ISO/IEC 15408.[68] The Common Criteria originated out of three standards: ITSEC, a European standard developed in the early 1990s by the United Kingdom, France, the Netherlands and Germany, TCSEC – or the "Orange Book" – the Unites States' standard, and CTCPEC, the Canadian standard. By unifying these pre-existing standards, companies selling computer products for defense or intelligence use only need to have them evaluated against a single standard. The Common Criteria allow users to specify their security requirements, allow developers to specify the security attributes of their products, and allow evaluators to determine whether products actually meet their security claims. The Common Criteria Mutual Recognition Agreement was signed in 1998 and recognizes evaluations against the Common Criteria standard done by other parties other than the original signatories.[69]

The Generally Accepted Information Security Principles (GAISP) project is an initiative aimed at self-regulation, in particularly with a view to preparating for the possible impact of a number of regulatory developments discussed later in this subsection. It aims to promote information security principles and practices that are scalable to varying levels of risk tolerance and that would apply equally to government or corporate infrastructure assets or the equipment and environment of a home user. GAISP is managed by the Information Systems Security Association, a not-for-profit industry-based information security resource with members in 89 countries.[70] The GAISP provides three levels of guiding principles addressed to security professionals of all levels of technical and managerial responsibility. The first level, "Pervasive Principles", targets government policymakers and executive-level management and provides guidance to help organizations achieve an effective information security strategy. The second level, "Broad Functional Principles", defines more precisely the elements needed to build effective security architecture. Finally, the third level, "Detailed Principles", serves as a framework for action for information security professionals and provides specific, comprehensive guidance for consideration in day-to-day information risk management activity.

Regulation

Regulation, in comparison to self-regulation, has its strengths as well. Enforcement may be simpler, as there is often legislative backing. Adherence is frequently obligatory and can reduce selection problems – whereby only the willing and successful come forward – in evaluating the overall impact of the prescribed standards or activities.[71] Regulation can be better aware of its societal context, as the regulatory body will itself be accountable to higher government instances, while regulations would need to be compatible with other accepted legal notions and rights, such as civil liberties and privacy. Firms outsourcing to clients under such regulation need to appreciate the current regulatory environment and develop competencies on the emerging standards, and achieving compliance may become a central marketing message (UNCTAD, 2003).[72] As notions of trust habitually decrease with distance and dissimilar business environments, firms from developing countries may have to make relatively greater efforts in supporting importers and clients in developed economies when these need to validate their own regulatory compliance. Such support and cooperation would necessarily involve the application of risk management concepts

in information security activities. Four regulatory developments have been singled out in this subsection, three of which are related to the United States, as it is an important outsourcing market.[73] The regulations discussed relate to information security issues and are complementary to cybercrime legislation as discussed in chapter 6.

Basel II is a capital adequacy framework agreement among banking regulators from 55 countries, of which 18 are from developing countries. Chapter 3 of this report deals with the implications of its new financial rating system on enterprises' access to bank-related trade finance and e-finance. Basel II proposes improved methodologies for accurately calculating capital provisions made against credit and commercial, and operational risk and asserts that the framework "…will promote the adoption of stronger risk management practices by the banking industry, and views this as one of its major benefits."[74]

Basel II is not overly explicit about information security measures *per se*. Information security in Basel II needs to be understood within the context of operational risk: the more effective a bank's operational risk management effort is, the less money it needs to set aside in reserve. Basel II defines operational risk as "…the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputation risk."[75] Recent computer security failures, such as hacked databases or virus and worm infections, are meaningful examples of the operational impacts of failed or insufficient information security controls. In this sense Basel II positions information security controls as a useful tool for operational risk management.

Information is critical to the operation of every financial institution. If the confidentiality of sensitive or private information is compromised, lawsuits or regulatory sanctions may result in penalties, and violated trust may result in loss of business. The integrity of critical information can be corrupted. When critical information is not available where and when it is needed, important processes may fail completely, with similar results. Recovery costs that follow such failures can become a major, or even detrimental, issue if damages turn out to be catastrophic. Thus, the degree of risk mitigation from a formal and well-organized information security programme can be significant. In practice, many of the Basel II operational risk principles can be met through use of the information security standards such as the ISO/IEC 17799 or the Organization for Economic Cooperation and Development (OECD) Guidelines on Information Security that are discussed in part F of this chapter.[76]

The United States Federal Information Security Management Act (FISMA) was enacted in 2002. The objective of the act is to improve computer and network security within the Federal Government and government contractors by mandating yearly security audits. Federal agencies will "develop, document, and implement an agency wide information security program … [in order] to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."[77] This will include periodic assessments of risk policies and procedures, security awareness training, periodic testing and evaluation, remedial action, and implementing measures to mitigate risks associated with security incidents before substantial damage is done, as well as plans and procedures to ensure continuity of operations when information security is under threat.

The United States Public Company Accounting Reform and Investor Protection Act of 2002, more commonly known as the Sarbanes-Oxley Act (SOx), was enacted after a series of corporate financial scandals, including those affecting Enron, Arthur Andersen, and WorldCom. Through its Titles VIII and XI, SOx aims to prevent third parties or corrupt management from destroying or falsifying financial documents. Information security aspects and audit ability are important for its realization, as many firms will use electronic means to store and analyse financial data. The deadline for compliance with SOx was 15 April 2005, but an online poll at a SOx discussion forum shows that almost 60 per cent of companies surveyed have not started any kind of implementation.[78]

More specifically, SOx article VIII criminalizes destroying, altering, concealing or falsifying records, in particular audit records, with intent either to obstruct or influence an investigation, and the failure of an auditor to maintain audit or review work papers for a five year period. Article XI takes issue with tampering with records and impeding official proceedings by, among other, altering, destroying, mutilating, or concealing a record, document, or other object, with the intent to impair the object's integrity or availability for use in an official proceeding. As certain outsourcing activities may involve data management that can include financial and accounting data, service provid-

ers from developing countries may consequently be affected.

Another regulation that can impact outsourcing firms is the Statement on Auditing Standards No. 70 (SAS 70) of the American Institute of Certified Public Accountants. Established in 1993, SAS 70 elucidates how external auditors should assess the information security in an outsourcing firm and the nature of the attestation. While the attestation implies that an in-depth audit of controls over information technology and related processes was performed, much like the ISO/IEC 17799 standard, SAS 70 does not provide a predetermined set of objectives or activities that a firm must achieve. The full "Type 2" SAS 70 report would include, besides the auditor's opinion, the firm's description of its security controls, a description of the auditor's tests of operating effectiveness, the results of those tests and any other information provided by the firm.[79]

However, the SAS 70 Type 2 audit may not be sufficient for SOx compliance. The SAS 70 standard was developed long before SOx regulations and does not focus on SOx controls and issues. An important distinction is that the burden of SOx compliance is with the entity receiving an outsourced service. For the outsourcing service provider, a single SAS 70 audit could cover multiple clients. However, recipients may demand additional controls and documentation beyond the requirements of SAS 70 Type 2 in order to achieve a satisfactory level of SOx compliance. SAS 70 requirements may eventually change to achieve compatibility with SOx, and outsourcing firms in developing countries may need to keep track of related developments.[80]

Human resource development and training

Without the knowledge conveyed through training and test exercises, users may inadvertently expose parts of the organization to security threats. For example, users might reveal sensitive information if they contact the wrong person when observing an intrusion. The term "social engineering" is often used to describe the practice of obtaining confidential information by manipulation of legitimate users to perform actions that are against established information security policies (Schneier, 2000). "Social engineers" will exploit the natural tendencies of people to be trustful and helpful, rather than attempt to discover and attack computer security flaws.

The human factor in information security manifests itself as intentional or involuntary employee transgression of established conduct norms and security policies. The proverbial disgruntled employee is the most obvious source of intentional security breaches, and an awareness of the criminal consequences and the forensic traceability of online activity may act as deterrents. To mitigate such risks, human resources policy will need to interface with risk management policy, and employee training may need to include issues related to intentional and criminal information security breaches. Enhancing recruitment processes, gauging levels of acceptance and trust in information security reporting systems and taking into account subjective levels of satisfaction as related to recognition of merit and financial reward will support the development of well-targeted human development and training policies and content at the firm or institutional level.

Moving to the notion of involuntary actions, employees may not be focused on information security threats as they go about performing their duties and doing their work. Security risks can be compounded by ignoring or not respecting poorly applied or designed policies and technologies in order "to get the job done". Involuntary transgressions can also result from a fundamental lack of training and awareness of security issues. While information resources and technologies are growing and improving daily, accessing them securely is becoming an issue of some complexity. It is therefore not surprising that demand is growing for biometric technologies and identity management systems that promise to simplify authentication and authorization.[81]

Firms and organizations need to provide training and education on applying prescribed policies in order to minimize response times and even pre-empt certain threats.[82] Employee buy-in is crucial to validate any investment in information security risk management, hardware and software technologies and the establishment of policies to support them. However, incentives for buying in and the consequences of opting out are management issues, and thus the human factor introduces the problems of information security into the managerial and strategic levels of an organization and warns against leaving its application to insular and detached computer departments. Consistent reporting on security threats can be achieved if employees do not face disincentives; they need to be confident that they can report incidents without fear, ridicule or retribution.

Human resource development will usually start with an awareness-building programme designed to develop an information security mindset. The awareness-building phase can be used to gauge aptitudes and competencies and generate feedback for the design of more practical training. Practical training may follow on from the basics of security and how information and privacy are protected. This is particularly relevant when a business or public institution is responsible for private or sensitive information. There may be a need to educate on the importance and application of privacy laws, both domestically and in the country of the client, in particular if a firm is involved in outsourcing activities.

Building an understanding of security-related policies and their logic can be an important role for government, in particular in guiding public administration and public sector enterprises towards better security.[83] For such entities, market incentives may be non-existent, and security valuation and cost-benefit analysis may be complex and difficult. Accordingly, a clear security strategy and policy commitment may be needed and would necessarily be supported through human capacity and awareness building activities. For many developing countries that have already established e-strategies or information economy development policies, embracing or strengthening information security and the respective human resources development perspectives would increase the spectrum of possibilities for practical implementation.

3. Reduction of frequency and severity of loss events

From an information security perspective, reduction of the frequency and severity of loss events will be related to the design and implementation of policies that govern the use of an information system, as well as with the fundamental technical design of the system. While technical design issues are beyond the scope of this chapter, suffice it to say that any security that users need should be actively implemented within their own environment. Relying only on legislation, regulation or audits of third parties may not be a sufficiently prudent strategy.

Decreasing the response time from a security attack to the implementation of the first active measures, such as bringing redundant systems online, is the basis for loss severity reduction. Accordingly, policies and supporting procedures that are the subject of training, that are well written and clearly documented, communicated and enforced, can prepare an institution to respond to security threats in a timely and controlled manner. Policies should also foresee practicing security breach procedures in advance of a real attack. When experiencing a security attack or breach, policies will have determined what actions to take, what data to gather and preserve, and how to protect data, systems and networks from further damage. Documenting plans, conducting training and testing procedures in advance will allow users and administrators to coordinate their activities efficiently when responding to an intrusion.

Computer security incident response teams (CSIRTs), sometimes also called computer emergency response teams (CERTs), can be extremely valuable organizations when a security attack is imminent or under way. A CERT performs, coordinates and supports the response to security incidents that involve sites within a defined group of users, sites, networks or organizations.[84] In doing so they will monitor trends in information security breaches, cooperate with security experts to identify solutions to security problems, post alerts, and disseminate information to the public. CERTs may also analyse the security features and performance of various hardware and software products, publish research on information security issues and cooperate with other government or business entities in developing and delivering information security training. Many developing and developed countries have one or several CERT or CSIRT teams hosted by a variety of institutions, ranging from universities to businesses and government. In order for CSIRTs be successful, it is "…paramount that coordination and cooperation occurs among governments, law enforcement, commercial organizations, the research community, and practitioners who have experience in responding to IT security incidents" (Killcrece, 2004).[85] The need for regional and global coordination between CSIRTs is of prime importance as well. This is discussed in part F of this chapter.

4. Risk transfer – insurance

Insurance for information security risks is often called cyber-risk insurance. The objective of insurance is to provide financial stability for individuals, organizations and businesses by providing a risk transfer mechanism in exchange for a premium payment (UNCTAD, 2002). By presenting financial compensation when a loss occurs, insurance helps individuals and organizations continue their activities. Even when no loss occurs, insurance reduces uncertainty

and allows people and firms to focus on their objectives. In this sense, insurance and cyber insurance can provide improved security for investors, in particular those with high exposure to information security risks. However, some studies (Böhme, 2005) have questioned the fundamental insurability of information security risks and therefore the development of cyber insurance products. The near monolithic dominance of a few technological platforms could lead to a high correlation of losses from some of the threats previously discussed. To compensate, insurance premiums would surcharge, with a corresponding shrinkage in demand and a potential increase in adverse selection problems.

Using cyber-risk insurance may improve the adoption of risk management concepts and processes, as insurers will necessarily request clients to comply with any one or several regulatory or self-regulatory standards. Requirements for insurance may actually force companies to increase internal network security, and there have been suggestions that the insurance industry will eventually drive security reforms in the information technology industry (ITU, 2002; Schneier, 2000). The insurance industry can also play an important role in improving information security by working with Governments to increase public and corporate awareness of information security risks and promoting best practices.

Cyber-risk insurance cover is available primarily as a stand-alone policy for first- and third-party coverage. Policies can cover both internal and external threats. They may cover attacks aimed specifically at the policyholder or those that affect the Internet in its entirety. Examples of cyber-risk insurance policies are covers for web content liability, professional liability, network security third-party liability, intangible or information property loss, loss of e-revenue or cyber-terrorism. In practice, the total cyber-risk insurance market has probably not reached the $1 billion mark (i.e. less than 0.05 per cent of global premiums). One possible reason may be that the insurance industry lacks sufficient data to quantify security risks. As a result, insurers may set premiums higher in order to compensate for unknown risk. Such high-cost premiums may be beyond reach for small and medium-sized companies, and as a consequence many of them will retain risk and self-insure. Compounding the problem of a lack of data is the fact that the actual nature of security flaws and threats evolves and changes daily, and future risks are difficult to know. Businesses may also be reluctant to report security failure incidents, as they may result in a loss of reputation and business (Kesan, Majuca and Yurcik, 2004; ICLR 2004).

Another explanation may be that certain exclusions that severely decrease potential clients' perception of the value of cyber insurance covers. These may include, for example, disgruntled employee exclusion, which by any token is a major security risk factor. Territory exclusions may be included, with the result that claims from losses due to wrongful acts in particular parts of the world will not be reimbursed - a fairly awkward proposition given the global nature of the Internet. Abusing available material may also be excluded. These are security attacks that are performed using passwords, authorizations or other employee identification stolen in the physical world.

5. Risk retention

Risk retention is often treated as the final component in a risk management process.[86] After all means and tools have been exhausted to avoid, reduce and transfer information security risks, a certain ultimate risk component inevitably remains and falls on the individual, firm or organization. Organizations will sometimes practice risk retention only because many risks may not be assessable in advance. Beyond this "unplanned" component, formal risk retention is planned and conscious and is sometimes referred to as "self-insurance". While the notion may be simple, in practice risk retention requires setting up a risk financing mechanism. Depending on the size, importance, competencies and regulative environment of the risk taker, the financing mechanism may be managed internally or by a financial service provider. It may range from a pay-as-you-go policy to systematically setting aside funds, creating a captive insurance company, setting up insurance pools with similar institutions or establishing a finite risk insurance scheme. Whatever the solution, it needs to be put in place for two basic reasons.

The first is that some financial losses from information security incidents are inevitable, and their size may affect, at the very least, short-term cash flows. Financial problems may in turn lead to non-performance towards clients or stakeholders that provokes supplementary liability. The second is that without the surety of a risk retention mechanism, the resulting financial uncertainty may inhibit or distract entities to the point where they may forego opportunities that are in their best interest. Thus, a firm striving to maximize its value or an institution aiming to excel at

meeting its objectives may under-perform without organized and financed risk retention.

If an entity is confident that future losses will be fairly constant and predictable, and if it makes financial sense in the light of insurance premium prices, the entity may choose to retain more and insure less. However, such choices may be the privilege of large companies and organizations that, during a given financial year, accumulate enough loss events that are statistically representative of the general averages of occurrence and severity for a particular information security risk. This would enable them to forecast with confidence and surety the financial implications of security threats and set aside funds to compensate the impending damage.

F. International and national policy developments and issues

Today, Governments are faced with the certainty of information security threats and various disincentives for using and investing in information security, as well as the notion that information infrastructures are becoming part of national and global critical infrastructures. In response, Governments may engage policies to remedy security problems and seek benefits from enabling a safer, and thus wider, use of information technologies.

Awareness building and education, standard setting, promoting self-regulation, using risk management methodologies, and legislating to deter cybercrime have become important areas of activity for Governments and their institutions. Such efforts find their corresponding expression in international policy forums, where concerns have been voiced and guidelines formulated to tackle the increasingly important issue of information security as we move towards a global information economy and society. This section will review several recent policy processes and events at the international level. It will then highlight several issues of importance for national policy.

1. International policy

A number of international organizations and processes are considering information security issues. Their work goes against any prejudgment of sameness and reflects a wide diversity of concerns and approaches. A certain distillation of these notions has been achieved in UN General Assembly resolutions 55/63 and 56/121, highlighted in part B.3 of this chapter. The General Assembly also took up the cybercrime issue in resolution 56/261, where in paragraph 5 it recommends action at national and international levels against high-technology and computer-related crime.[87] General Assembly resolutions 57/239 and 58/199 expand on these issues and speak of the creation of a global culture of cybersecurity and the need for the protection of critical information systems.[88] The UN Economic and Social Council (ECOSOC) has taken up this issue as well and has reviewed UN-wide activities in this area.[89] ECOSOC has provided guidance on cybercrime issues on several occasions. In its resolution 1999/23, it mandated research on national and international policy for the prevention and control of computer-related crime, and in resolution 2001/18 it took up the issue of the use of computer and telecommunication systems for international and national drug trafficking.[90] The issue of the use of ICT and criminal activities has been dealt with in detail in the report of the International Narcotics Control Board for 2001.[91]

More recently, the World Summit on the Information Society (WSIS), a high-level UN initiative on the development of the information society, has specifically addressed information security issues in its Declaration of Principles and Plan of Action. Article 5 of the Declaration notes that building trust is the focus of information security and a prerequisite for the development of the information society. The Declaration affirms the need for building a global culture of cybersecurity, supported by increased international cooperation and taking into account the level of social and economic development of individual countries. The Plan of Action, in part C.5, details these notions and recommends addressing them through international cooperation, public-private sector partnerships, and activities focused on education and awareness building. Particular issues were singled out, such as privacy, spam, cybercrime law, development of best practice guidelines, establishment of response teams and the effects of information security on trade and commerce.[92]

In general, it may be fair to say that policy reactions to information security issues often initially address legal implications and act to adjust legislation to deal with cybercrime. As the issue matures, international policy discussions and cooperation will increasingly engage in technical issues, such as standards or specific technologies, and move on to more holistic notions of

risk management and security cultures. Evidence of such processes is already surfacing today.

Council of Europe

The Council of Europe has been actively pursuing the information security theme since 1996. In 2001 its Committee of Ministers adopted the Convention on Cybercrime, an international treaty creating a cross-border "criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international cooperation."[93]

European Union

The European Union has addressed the issue from a legal perspective (for example through its electronic signatures directive and its data protection legislation). Under its eEurope 2005 action plan, the EU has also undertaken activities in fields such as network and information security and secure communications for e-government. The European Network and Information Security Agency (ENISA) was formally established in 2004 with the objective of supporting the development of a culture of network and information security.[94] ENISA will provide expertise on security-related issues in hardware and software products, security standards, interoperability, and risk assessment.[95]

OECD

The Organization for Economic Co-operation and Development (OECD) produced a primary set of information security recommendations in 1992 and reviewed them in 1997.[97] Given the vast increase in the global use of ICT resources, the OECD responded by re-establishing the guidelines in their present format and substance. The "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" were formally adopted as a Recommendation of the OECD Council on 25 July 2002.[97] One obvious difference between the present guidelines and the 1992 version is the inclusion of networks. More importantly, the guidelines propose an overarching theme of promoting a culture of security and focus on nine core principles that can be seen to suggest and support a risk management approach to information security issues. This is most apparent in the principles dealing with risk assessment, risk response, security design and security management. However, the recommendations go beyond risk issues and point to the human principles of ethics and democracy that can be foundational for understanding information security and its applications in modern society. The principles also address the role of the individual and comment on the need for awareness and skill development and the notion of responsibility. On a final note, the principles explain that information security is a continuous process where the reassessment of risks and the ongoing evolution of security systems is a permanent feature.

In launching the revised principles, the OECD Council made a number of policy recommendations to member countries that urged consultation, coordination and cooperation in dealing with information security issues, at both national and international levels. The Council further recommended the broadest dissemination of the Guidelines throughout public, private, government and civic organizations, and individual users, in member and non-member countries as well. A review schedule of five years has been established in order to address evolving concerns and to provide a forum for international cooperation and exchange of experience. The Guidelines were followed up by an implementation plan suggesting that Governments need to work the information security culture into their international cooperation policies and activities in order to achieve a global effect.[98] Legal cooperation to combat cybercrime was an immediate task. Supporting the establishment, work and cooperation of Computer Emergency Response Teams (CERTs) and developing closer cooperation between government and business was necessary as well. Outreach activities focusing on awareness-raising, education and exchange of experience were also highlighted as beneficiaries of government support. The plan also recognized that Governments are often owners and operators of information systems and networks, and that this presents an opportunity to lead by example and contribute to the development of best practice in information security.

In an effort to gauge implementation, the OECD conducted a survey (2004) on the implementation of the information security Guidelines. Member Governments gave the highest degree of attention to the development of a national policy framework and a legal environment, and to the implementation of the Guideline's principles, in particular those related to awareness building and response capacity. Strengthening cooperation and collaboration and fostering an exchange of practical experiences and best practices among participants, as well as with non-member economies, were declared priorities for future work.

APEC

Asia-Pacific Economic Cooperation (APEC) is a forum for facilitating economic growth, trade and investment in the Asia-Pacific region by cooperating on the basis of non-binding commitments, equality and open dialogue.[99] The APEC Telecommunications and Information Working Group is mandated to develop ICT policies and cooperation strategies on general issues, such as the transformation of the Asia-Pacific region into an information society and reducing the digital divide, as well the specific topics of protecting information and communications infrastructure and cybersecurity. The Fifth APEC Ministerial Meeting on Telecommunications and Information Industry, held in May 2002 in Shanghai, issued a specific statement on information security[100] and a programme of action,[101] which were followed up with the establishment of a cybersecurity strategy. The strategy recommends activities in six specific areas: legal issues and cooperation, information sharing, security and technical guidelines, public awareness, training and education, and wireless security. Promoting cooperation among local, national or regional CERTs was highlighted, and training activities have commenced through a project and a series of seminars on anti-cybercrime legislation and capacity building.

G8

The Group of Eight evolves informal agreements on current issues, such as the effects of globalization or information security.[102] The first G8 multilateral meeting devoted to the protection of critical information infrastructures took place in March 2003.[103] This expert meeting was followed up by the G8 member States' Ministers of Justice and Home Affairs, together with the European Commissioner in charge of Justice and Home Affairs, who met in May 2003, in Paris, to engage in a policy discussion on more general security issues, such as terrorism and organized crime. The deliberations made particular reference to the protection of critical information infrastructures and, more specifically, to the use of biometric security technologies.

The G8 meetings stressed the importance and interdependence of critical information infrastructures, as well as the need to increase international cooperation to ensure their protection against potential terrorist attacks. The meetings resulted in a set of 11 internationally agreed principles for protecting critical information infrastructures that would serve as a foundation for further work in this area.[104] The principles noted that effective protection requires "…communication, coordination, and cooperation nationally and internationally among all stakeholders – industry, academia, the private sector, and government entities, including infrastructure protection and law enforcement agencies." They also define information security in terms of a process approximating a risk management approach, rather than an amalgamation of technologies. From the perspective of direct government involvement, the principles point to the need for countries to have early warning and crisis communications networks and bodies, as well as to the role of Governments in supporting awareness building and training. Biometric technologies and their use in travel procedures and documents received special mention and have progressed up the G8 agenda to the highest level in the form of the Secure and Facilitated International Travel Initiative.[105]

Professional initiatives

Practitioners of information security will certainly support international developments while developing less formal mechanisms for international cooperation. The main advantage of such bodies is their unhindered capacity for rapid reaction. Noted disadvantages are a possible lack of transparency of operations and the lack of legal enforcement of their agreements (ITU, 2002). Most will have government or government-funded institutions as their members, so the designation of "non-governmental" may not strictly apply. The Forum of Incident Response and Security Teams (FIRST) was established in 1989. The FIRST membership consists of computer emergency response teams from educational, commercial, vendor, government and military organizations.[106] FIRST describes its purpose as assisting an information technology community in preventing and handling security-related incidents by fostering cooperation and coordination in incident prevention, enabling rapid reaction to incidents and promoting a culture of information sharing among its community. The Computer Emergency Response Team Coordination Center (CERT/CC) was created by the United States Defense Advanced Research Projects Agency in November 1988 after the Morris worm struck. It is a multilateral initiative and coordination centre dealing with Internet security problems. CERT/CC is run by the United States government-funded Software Engineering Institute (SEI) at Carnegie Mellon

University. The Asia-Pacific Computer Emergency Response Team (APCERT) is a coalition of CERTs from 13 economies across the Asia-Pacific region.[107] APCERT has gained the formal support of Governments in the region and has been invited to participate and contribute at the intergovernmental forums of APEC. Latin American countries and CERTs are involved through the Inter-American Committee against Terrorism, which is hosting an initiative for the establishment of a framework for regional coordination among CSIRTs. The framework was adopted in June 2004.[108]

2. National policy

Governments have been intimately involved in defining, engineering and using information security technology from the earliest days. The requirements of diplomatic services and military organizations drove security technology development until the middle of the twentieth century. The change in the role of government from innovator to standard-bearer has only occurred recently and, as explained in part D, has been caused by the broad take-up of computer and Internet technology by firms, organizations and individuals. The decentralized nature of Internet computer networks and the development of intelligent applications that run on its periphery have led to an almost complete loss of direct control over technology users or the network itself.[109]

Governments will need to set policies while appreciating the notion that information security has become a part of the national critical infrastructure. The level of acceptance will vary from developed to developing and least developed countries, but there will rarely be outright rejection. Economic activities are becoming increasingly and strategically dependent on information technology, and therefore the importance of information security has become indisputable. Public sector functions, such as transport and utilities, as well as civil administration, are increasingly using technology to maintain or improve their quality of service and enrich their offerings.

In part B.4, the chapter discussed the problem of incentives. Governments will need to analyse how investment in information security is related to actually achieved security. Should the conclusion be that there is a general under-investment due to problems stemming from a tragedy of the commons or first-mover advantage and network externalities, incentives may need to be adjusted through a combination of fiscal and regulatory policies.

Government policy and practice are often faced with tough decisions: sound policies may enhance security, while misconceived regulation may be detrimental (Sadowsky et al, 2003). Regulating and legislating is often seen as the natural course of action, and indeed adjustments to incorporate the notion of cybercrime in national legislation have for many Governments been a first practical and determined step in the right direction. This is discussed in chapter 6. However, just because some regulation is good does not mean that more is better, and Governments will need to balance regulating with encouraging innovation. Several regulatory initiatives were discussed in part E.2 of this chapter.

More broadly, in order to develop a national security policy, Governments may conduct a national information risk analysis, not dissimilar to what a firm or an organization would do. Awareness, education and capacity building for information security, within both administrative and other public bodies, schools, universities and training centers, as well as among the general public, can and should be a strategic activity. The promotion of information sharing on critical issues for information security through the establishment and support of national CERTs has become an established activity judging by the broad memberships of organizations such as FIRST or APCERT. The only part of the risk analysis process that may be given less prominence at a government policy level may be any prescription on particular types of applications and technologies, beyond the formulation of minimal standards and requirements. Technological neutrality may eventually be adjusted, with a preference for security technologies that support public standards or that have endured public scrutiny and testing.

While all developed and many developing countries have implemented policies supporting various types of information security activities, it may be doubly important to bring such activities into officialdom by embracing them within a broader national e-strategy framework. This will facilitate the involvement of all stakeholders in information society development. It will also support the notion of evolving information security into a risk management exercise, as the activities of risk assessment and avoidance will generate data and inputs on which to base actual policy actions targeting concrete problems and issues.

G. Concluding remarks

The widespread and growing use of information technology implies shared responsibilities among developed and developing countries, as well as among individuals, firms and Governments, for the threats and weaknesses it presents. The position of developing countries is not conceptually different from that of developed countries. As is indicated in chapter 6 on cybercrime, here too the common wisdom applies to all.

The objective of having in place an appropriate level of information security at all levels is complicated by a number of factors, several of which may be considered as the domain of government policy. Unlike other issues where government involvement is questioned, information security policy and practice are not fundamentally disputed, perhaps because of their strong links and history with national security. Another reason may be the strong realization that information technology, and therefore security, has become part of a nation's critical infrastructure – much like physical security, certain utilities or an assured minimum standard of welfare.

Government policy

Trade, financial transactions, government administration and education are examples of activities that are increasingly dependent on technology infrastructures and therefore on information security. Globalization enables – or indeed compels – firms, organizations and individuals to explore opportunities for better business, to compete and to cooperate. Government policy needs to reflect these realities and is increasingly requested to provide leadership and foresight. The productive and intensive use of ICTs requires a high level of trust in the technologies and among its users. In this sense, the application of risk management to information security and the environment of trust it creates and supports is a foundational element for information economy development, and it follows that developing countries would need to support this notion within their e-strategy or digital development policies and practice.

Impact on the ICT service sector

Governments can investigate and assess the intensity and modes of use of security technologies and may regulate minimum general standards or specific guidelines for a particular sector or group, such as financial services or government suppliers. Voluntary self-regulation can also affect demand, as consumers request certification of a standard of quality of services before buying. Meeting increasing regulatory demands may provide additional incentives for the development of information security services in developed and developing countries as well – in particular in those countries that are active in business process outsourcing services. When judging business prospects, ICT and information security services firms may find focusing on trends in ICT purchases important but insufficient. Even though spending on information security is still a subset of the information technology market, security firms will need to monitor international and national regulatory developments and adjust their commercial expectations accordingly. In this sense, the information security industry is both a global and a local business. However, information security services may not be perfectly tradable from an international perspective as local provision may necessarily require locally relevant knowledge and production cost structures. Accordingly, an increasing demand for information security services may present an opportunity for local and national ICT service sector development, in particular in developing countries.

Risk management

Underlying these notions is a shift away from technology-centric treatment of information security and towards a risk management approach. Instead of reaching for a technical fix, risk management requires consideration of the problem and its context. Threats are evaluated, but so are the assets subject to compromise. Incentives and disincentives are analysed, and security policies, human resource development and legal instruments can be used to change their weight and influence on the intensity of applied security measures. The purpose of such an exercise would be to adjust the level of applied information security in order to bring it closer to a perceived or theoretical optimum. However, policy makers in developing countries may benefit from a better historical, social and economic understanding of the progress of information security technologies as, at second glance, many recent issues may not be fundamentally or technically novel. Given comparatively limited resources, developing countries need to make better strategic choices, and they may achieve this by using a risk management framework instead of a technology-centric and reactive approach.

Standards and regulations

The importance of standards and regulations is highlighted by the opportunities presented when firms in developed countries outsource particular business activities. Increasingly stringent regulation aims to, among other things, designate liabilities and fault in case of security compromises. The substantive engagement of the international community in providing security guidelines and addressing particular issues that may need policy consideration and action may offset the difficulties presented by such increased regulatory requirements. Opportunities for global sharing of security information and experience are increasingly accessible, and non-governmental forums are engaging in cooperation with established multilateral institutions.

The way ahead

In closing, it should be noted that developing countries may need to address several issues more specifically. The scope for building awareness may be larger than in developed countries, and government policy may reflect this by extending activities and support to all educational and training institutions. Furthermore, as developing countries have less infrastructure and fewer ICT assets to protect, incentives for applying information security may be significantly different given that the majority of the world's information resources and technologies are owned or managed by entities from developed countries. However, if information security is of global strategic concern, it can only be improved at an equally global level. This suggests that international technical and policy cooperation with developing countries should be encouraged and supported, in particular by the most technologically advanced countries, as there is only mutual benefit to be had. Export and outsourcing opportunities will in the future, if not already, depend on satisfying security regulations in the export destinations. Accordingly, undemanding regulation does not do any ICT exporter a favour – the regulations that apply are those of the importer, and exporting firms may need information and guidance on how to achieve compliance. Establishing an information security policy, preferably within the framework of an overall e-strategy where one exists, based on a risk management approach and regulating an appropriate set of incentives for its use, can provide important support for the development of information security practice.

Annex I

A simplified mathematical illustration of the Diffie-Hellman key exchange

This example owes much to the wisdom of simplification presented in Khan (2000). The actual mathematics use much larger numbers. The purpose of the key exchange process is to allow Alice and Bob to each, on their own and in secrecy, establish the identical secret key without revealing any information about it. Mathematically minded readers are encouraged to explore the process through a referential text such as Schneier (1996).

Step 1

Alice and Bob decide to use the one-way modular function

$$Y^X \text{ (Mod P}$$

where "mod P" (or modulo P) means calculate the whole number remainder of Y^X divided by P. For example, if $Y^X = 6^2 = 36$, and P = 7, Y^X(mod P) would be the remainder of 36..7, or 36 minus 35 (which is 7 x 5), which equals 1. However, if someone gave away the result, i.e. 1, and asked to have the equation reversed to find out Y^X and therefore X, even with knowing that P = 7, it would be time consuming to do this. If Y and P are sufficiently large, the exercise becomes unfeasible.

Step 2

In step 2 Alice and Bob will agree on the values for Y and P. Let us assume they have chosen Y = 7 and P = 13. These numbers are not secret.

Step 3

In step 3, Alice and Bob will choose each, in secret, their own values for "X", which are now referred to as A and B

Alice chooses A = 5. Bob chooses B = 8.

Step 4

In step 4, Alice and Bob will apply the pre-agreed modular function to their choice of "X".

$Y^X(\text{mod P}) = Y^A(\text{mod P})$
$7^5(\text{mod 13}) = 16{,}807(\text{mod 13}) = 11$
We will call 11 "***a***".

$Y^X(\text{mod P}) = Y^B(\text{mod P})$
$7^8 (\text{mod 13}) = 5{,}764{,}801(\text{mod 13}) = 3$
We will call 3 "***b***".

Step 5

In step 5 Alice and Bob will swap ***a*** and ***b***. They can do this over a public communications network without any worry. Eve the eavesdropper may intercept ***a*** and ***b***, but will find it very difficult, if not unfeasible, to reverse the calculation to get A and B. Therefore, Alice and Bob can use an unsecured Internet connection or telephone line for swapping ***a*** and ***b***.

Step 6

In step 6, Alice and Bob will use each other's ***b*** and ***a*** instead of the original Y they had agreed upon.

b^A (mod P)
$3^5(\text{mod 13}) = 243(\text{mod 13}) = \mathbf{9}$

a^B (mod P)
$11^8(\text{mod 13}) = 214{,}358{,}881(\text{mod 13}) = \mathbf{9}$

The reason being that $(Y^B(\text{mod P}))^A = (Y^A(\text{mod P}))^B$; $Y^{BA}(\text{mod P}) = Y^{BA}(\text{mod P})$ or $b^A = a^B$.

Step 7

In the final step 7, having agreed the secret key is **9**, Alice and Bob will establish an encrypted communication based on this key.

References

Adams C and Lloyd S (2003). *Understanding PKI: Concepts, standards and deployment considerations*, Addison-Wesley Professional, Second edition.

Anderson R (2001). Why information security is hard - An economic perspective, paper presented at the 17th Annual Computer Security Applications Conference, 10-14 December, New Orleans, Louisiana.
http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf

Anderson R (2002). Security in open versus closed systems - The dance of Boltzman, Coase and Moore, paper presented at the Conference on Open Source Software: Economics, Law and Policy, 20-21 June 2002, Institut d'Economie Industrielle, Toulouse, France.
http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/toulouse.pdf

APEC (2002). Shanghai Declaration, Program of Action, Statement on the Security of Information and Communications Infrastructures, Fifth APEC Ministerial Meeting on Telecommunications and Information Industry, TELMIN5/1.
http://203.127.220.112/content/apec/ministerial_statements/sectoral_ministerial/telecommunications/2002.downloadlinks.0001.LinkURL.Download.ver5.1.9

Atkins D, Graff M, Lenstra AK and Leyland PC (1995). The magic words are squeamish ossifrage, *Advances in Cryptology - Asiacrypt '94*, Springer-Verlag, 263-277.
http://www.mit.edu:8001/people/warlord/rsa129.ps

Belrose J S (2001). A radioscientist's reaction to Marconi's first transatlantic wireless experiment, Antennas & Propagation Society International Symposium, Boston, 8-13 July 2001.

Böhme R (2005). Cyber-Insurance Revisited, paper presented at the 2005 Workshop on the Economics of Information Security.
http://infosecon.net/workshop/pdf/15.pdf

Cashell B, Jackson WD, Jickling M and Webel B (2004). The Economic Impact of Cyber-Attacks, Congressional Research Service, Report for the Congress, The Library of Congress, Order Code RL32331.
http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

Cilek P, Janko W, Koch K, Mild A and Taudes A (2001). The evaluation of IT-investments in public sector organisations, Proceedings of the 8th European Conference on IT Evaluation, Oxford, UK.
http://wwwai.wu-wien.ac.at/~koch/forschung/bpr/ecite01.pdf

Diffie W (1988). The first ten years of public-key cryptography, Proceedings of the IEEE, Vol. 76, No. 5.
http://cr.yp.to/bib/1988/diffie.pdf

Diffie W (2003). Risky business: Keeping security a secret, ZDNet.
http://news.zdnet.com/2100-9595_22-980938.html

Diffie W and Hellman ME (1976). New directions in cryptography, Institute of Electrical and Electronics Engineers, Transactions on Information Theory.
http://crypto.csail.mit.edu/classes/6.857/papers/diffie-hellman.pdf

ECOSOC (2002). Effective measures to prevent and control computer-related crime: Report of the Secretary-General, E/CN.15/2002/8.
http://www.unodc.org/pdf/crime/commissions/11comm/8e.pdf

Ford W and Baum MS (2000). *Secure electronic commerce*, Prentice Hall PTR, Second edition.

G8 (2003). G8 Principles for Protecting Critical Information Infrastructures.
http://www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf

Good J, Michie D and Timms G (1945, declassified in 2000). General Report on Tunny, National Archives of the United Kingdom, HW 25/4 and HW 25/5.
http://www.alanturing.net/turing_archive/archive/index/tunnyreportindex.html

Gutmann P (2002). PKI: It's not dead, just resting, IEEE Computer Society, August edition.
http://www.cs.auckland.ac.nz/~pgut001/pubs/notdead.pdf

ICLR (2004). Cyber-incident risk in Canada and the role of insurance, Institute for Catastrophic Loss Reduction, Research paper series - No.38.
http://www.iclr.org/pdf/Cyber-Incident%20Risk%20Final%20Report_April%202004.pdf

ITU (2002). International coordination to increase the security of critical network infrastructures, International Telecommunication Union, CNI/04.
http://www.itu.int/osg/spu/ni/security/docs/cni.04.pdf

Kesan JP, Majuca RP and Yurcik WJ (2004). The economic case for cyberinsurance, University of Illinois College of Law, Law and Economics Working Papers.
http://law.bepress.com/cgi/viewcontent.cgi?article=1001&context=uiuclwps

Khan D (1996). The codebreakers : The comprehensive history of secret communication from ancient times to the Internet, Scribner, Revised edition.

Killcrece G (2004). Steps for Creating National CSIRTs, Software Engineering Institute, Carnegie Mellon University.
http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

Menezes A, van Oorschot P and Vanstone S (1997). Handbook of Applied Cryptography, CRC Press.
htp://www.cacr.math.uwaterloo.ca/hac/

Nathan PX and Erwin MW (2004). On the rules of engagement for information warfare, Symbiot, Inc.
http://www.whurley.com/pdfs/iwROE.pdf

OECD (2002). OECD Guidelines for the security of information systems and networks, OECD Publications.
http://www.oecd.org/dataoecd/16/22/15582260.pdf

OECD (2003). Implementation plan for the OECD guidelines for the security of information systems and networks: Towards a culture of security, OECD Publications, DSTI/ICCP/REG(2003)5/REV1.
hhtp://www.oecd.org/dataoecd/23/11/31670189.pdf

Outreville JF (1997). Theory and Practice of Insurance, Springer, first edition.

Perens B (1998). Why security-through-obscurity won't work, Slashdot.
http://slashdot.org/features/980720/0819202.shtml

Rivest R, Shamir A and Adleman LM (1977), (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21,2, 1978.
First published in 1977 as MIT Memo MIT/LCS/TM-82.
http://theory.lcs.mit.edu/~rivest/rsapaper.pdf

Sadowsky G, Dempsey JX, Greenberg A, Mack B and Schwartz A (2003). Information Technology Security Handbook, The International Bank for Reconstruction and Development, Washington, DC.
http://www.infodev-security.net/handbook/

Schneier B (1996). Applied cryptography, Wiley Publishing, Inc., Indianapolis, Second edition.

Schneier B (2000). Secrets and lies: Digital security in a networked world, Wiley Publishing, Inc., Indianapolis.

Siegel CA, Sagalow TR and Serritella P (2002). Cyber-risk management: Technical and insurance controls for enterprise-level security, CRC Press.
http://www.aignetadvantage.com/content/netad/CyberRisk_Article_043002.pdf

Singh S (2000). The code book: The science of secrecy from ancient Egypt to quantum cryptography, Anchor Books, New York.

Surendran K (2005). Information security: Nurturing a security conscious workforce, Knowledge Platform White Paper.
http://www.knowledgeplatform.com/presentation/information_security.html

Sveiby KE (2004). Methods for Measuring Intangible Assets, Sveiby Knowledge Associates.
http://www.sveiby.com/articles/IntangibleMethods.htm

UNCTAD (2001). E-Commerce and Development Report 2001, United Nations Publications.
http://r0.unctad.org/ecommerce/docs/edr01_en.htm

UNCTAD (2002). E-Commerce and Development Report 2002, United Nations Publications.
http://r0.unctad.org/ecommerce/ecommerce_en/edr02_en.htm

UNCTAD (2003). E-Commerce and Development Report 2003, United Nations Publications.
http://r0.unctad.org/ecommerce/ecommerce_en/edr03_en.htm

UNCTAD (2004). E-Commerce and Development Report 2004, United Nations Publications.
http://r0.unctad.org/ecommerce/ecommerce_en/edr04_en.htm

United States General Accounting Office (2004). Information security, Technologies to secure federal systems, GAO-04-467.

Varian H R (2000). Managing Online Security Risks. The New York Times. 1 June.
http://www.nytimes.com/library/financial/columns/060100econ-scene.html

Vaughan E, Vaughan TM (2002), Fundamentals of Risk and Insurance, Wiley, New Jersey, 9th edition.

Wheeler DA (2003). Secure Programming for Linux and Unix HOWTO.
http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html

Williamson LC (2001). A discussion of the importance of key length in symmetric ad asymmetric cryptography, SANS Institute, GIAC Practical Repository.
http://www.giac.org/certified_professionals/practicals/gsec/0848.php

Wilson RMS, Stenson J and Oppenheim C (2000). Valuation of Information Assets, The Business School of Loughborough University, Research Series Paper 2000:2.
http://www.lboro.ac.uk/departments/bs/research/2000-2.pdf

Zwicky EDtt, Cooper S and Bren Chapman D (2000). Building Internet firewalls, O'Reilly, Second edition.
http://www.oreilly.com/catalog/fire2/
http://www.hn.edu.cn/book/NetWork/NetworkingBookshelf_2ndEd/fire/index.htm.

Notes

1. This definition has been attributed to George McDaniel and his text IBM Dictionary of Computing (1994). See http://www.sei.cmu.edu/str/indexes/glossary/information-security.html.
2. UNCTAD (2003) presented an initial discussion of information security issues in its first chapter. It noted that, while technology can help reduce information security risks, the key to a secure online environment is not technical, but a combination of market efficiency, industry initiatives, political will and an appropriate legal environment.
3. See part F.1 for more details on international policy cooperation.
4. We will often permanently monitor our trust level during the exchange as we continue to judge the sincerity and intent of the other conversant by reading, sometimes unconsciously, body language or speech mannerisms.
5. The privacy of spoken discussion can range from an interview for public or news media or an exchange of views at a conference, to a business meeting among negotiating teams or an intimate consultation with a medical expert.
6. See http://www.unhchr.ch/udhr/lang/eng.htm .
7. See http://www.un.org/Depts/dhl/resguide/r55.htm and http://www.un.org/Depts/dhl/resguide/r56.htm .
8. See http://www.nta-monitor.com/fact-set.htm .
9. Zombie computers are computers that have had malicious software installed, without the knowledge of their users. This software allows malicious hackers to use them to launch massive and coordinated attacks against websites or a firm's computer infrastructure.
10. The tragedy of the commons is a metaphor used to illustrate the conflict between individual and community interests that can often result in the overexploitation of a public good or service.
11. For an example of the limited liability of a common software license, see http://www.microsoft.com/windowsxp/home/eula.mspx.
12. Freedonia, Information Security, Study #1761, February 2004; Silicon.com, IDC: Companies must spend more on security, 28 April 2004, http://software.silicon.com/security/0,39024655,39120310,00.htm .
13. Estimates are from Cashell (2004) citing reports from Computer Economics Inc. and Mi2g. The quoted figures do not include damage caused by spam.
14. *Computerworld*, "The new information security market puts the old in the rearview", 6 December 2002, http://www.computerworld.com/ .
15. A VPN is a private communications network superimposed over a public network (e.g. the Internet). VPNs use cryptographic tools to provide confidentiality and authentication and to prevent message alteration, thus achieving a desired level of privacy over an unsecured network.
16. The firms were chosen by observing the competitors' listings for each, on the Yahoo Finance and Hoover's company information websites. As such, they are only examples illustrating the breadth, scope and diversity of the security information sector.
17. See http://www.europki.org/, http://www.dartmouth.edu/~pkilab/ and http://middleware.internet2.edu/pkilabs/.
18. See http://www.ossim.net/, http://www.openca.org/ , http://cacert.org and http://smartsign.sourceforge.net/ .
19. See http://news.com.com/2102-7350-3-5624251.html
20. Monoalpahbetic means that the equivalent "code" letter or symbol does not change throughout the message.
21. While there are many definitions for infrastructure, here we will be using the term to distinguish it from point-to-point systems set up privately by entities that have an established level of mutual trust. In this sense, drawing a dedicated wire between two localities is not infrastructure.

22. Tesla, Edison and others had explored wireless telegraphy in the 1860s. Marconi started experimenting with radio signals in 1894. By 1896 he could send and receive signals over distances of several kilometers and was awarded a patent that same year. In 1902 Marconi claimed to have radio-telegraphed the letter "S" in Morse code across the Atlantic Ocean from England to Newfoundland, an event that kick-started the race in global wireless communications. Given the relative lack of sophistication of the equipment used, doubts have been expressed over what was actually transmitted and the possibility of misinterpreting noise for a signal (Belrose, 2001).

23. Polyalphabetic cyphers were proposed by the Florentine architect Alberti and developed into a practicable system in the sixteenth century by the French diplomat and cryptologist Vigenère.

24. Bletchley Park (BP) was the site of a secret British military intelligence operation during and just before World War II. The site was named after the mansion in the grounds of which it was established.

25. Many cryptographic rotor machines were used until the 1980s. Besides the Enigma and Lorenz machines, the original Hebern machine from 1918 (United States), the Fialka (Soviet Union), the HX-63 and NEMA (Switzerland), the Hagelin M-209, SIGABA and KL7/Adonis (United States) and the Typex (United Kingdom) are well known.

26. Standards have been commissioned and designed more recently by other organizations and entities, for example the Gosudarstvennyi Standard GOST 28147-89 (Soviet Union – see http://ietfreport.isoc.org/ids-wg-smime.html), NESSIE - New European Schemes for Signatures, Integrity and Encryption (European Commission, see https://www.cosic.esat.kuleuven.ac.be/nessie/) or CRYPTREC - Cryptography Research and Evaluation Committee (Japan, see http://www.ipa.go.jp/security/enc/CRYPTREC/).

27. See http://csrc.nist.gov/cryptval/des.htm .

28. See http://www.mediacrypt.com/ .

29. See http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf .

30. Recent studies confirm this notion, and the European Commission's "*Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*" (2001) can be singled out as being particularly comprehensive. See http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_en.pdf or http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf .

31. See http://crypto.csail.mit.edu/classes/6.857/papers/diffie-hellman.pdf . See also http://patft.uspto.gov/netahtml/srchnum.htm and search for patent number 4,200,770. There have been suggestions that a comprehensive public key system was developed by Cocks, Ellis, and Williamson before 1975 while working for the British Government Communications Headquarters. See http://www.nytimes.com/library/cyber/week/122497encrypt.html#1 and http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=3&displayPage=31 .

32. See Rivest, Shamir and Adleman (1977)

33. The more precise definition of a prime number is a positive integer (1, 2, 3, 4, ...) whose only positive integer divisors are 1 and itself.

34. See http://mathworld.wolfram.com/RSANumber.html .

35. See http://www.rsasecurity.com/rsalabs/node.asp?id=2093 .

36. A discovery of a method for factoring large prime numbers would break certain asymmetric systems, regardless of their key length.

37. For a discussion on why asymmetric keys need to be longer than symmetric keys, see Williams (2000).

38. "Broken" would mean that a method has been found to reverse the hash value back into the message in less time than it would take a theoretical brute-force computational attack. A hash function would also be considered broken if it could be demonstrated that two different messages would produce an identical hash value. The reported attacks on SHA-1 are described as working on a subset of SHA-1 keys and under specific circumstances. Therefore, SHA-1 and derivative technologies are still considered to be secure at the time of writing. See http://www.schneier.com/blog/archives/2005/02/sha1_broken.html and http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html .

39. Unlike telephony, where a dedicated connection is established and reserved for those speaking, data travels on the Internet in a multitude of independent data packets. The sender's computer will take a file and divide it into many packets and each will receive an indication of origin, destination and reassembly instructions. These will travel through the Internet and sometimes will use different routes to reach the recipient computer, where they will be reassembled and presented in an application such as a browser. If the packets are encrypted to disallow access to a third party intercepting and lodging copies of the data packets, this creates a virtual private network (VPN) within, or on top of,

the Internet. Unlike telephony, this does not require any change in the Internet communications protocols and standards, nor does it require sequestering bandwidth or infrastructure. VPNs are powered by applications that sit on the computers of those communicating without affecting the underlying Internet.

40. See http://www.nullify.org/docs/elgamal.pdf .

41. For more details, see and http://www.itl.nist.gov/fipspubs/fip186.htm .

42. The original discussions on elliptic curve cryptography were presented in Koblitz (1987) "Elliptic curve cryptosystems" in Mathematics of Computation 48; and Miller (1985) "Use of elliptic curves in cryptography" in CRYPTO 85.

43. For a list of Certicom patents on elliptic curve cryptography, see their letter to the Standards for Efficient Cryptography Group (SECG) at http://www.secg.org/download/aid-398/certicom_patent_letter_SECG.pdf and SECG's commentary on patent issues at http://www.secg.org/?action=secg,about_patents .

44. See Certicom, *Code & Cipher,* Vol.2, No.1, http://www.certicom.com/download/aid-391/codeandcipher2-1.pdf .

45. See http://www.imlogic.com/news/press_107.asp .

46. See http://news.bbc.co.uk/2/hi/technology/4354109.stm .

47. See http://www.vnunet.com/news/1160924 .

48. This definition is often attributed to the American Risk and Insurance Association. Outreville (1997) provides an excellent overview of various definitions of risk.

49. Hedonic demand theory is a method of estimating demand or prices and can be used to assess information technology investments in non-profit or public organizations. An obvious effect of new information technology would be a change in the pattern of use of human resources from lower value to higher value functions, with a corresponding change in the overall wage-per-function structure of the organization. By classifying employee types and functions and assuming wages weightings for each employee type-function combination, "before" and "after" new technologies scenarios can be compared and the difference understood as the creation of an intangible technology asset.

50. For more details see http://www.willis.com/Services/Risk%20Management%20Operational/Operational.aspx .

51. See "Managing Reputation - an Holistic Approach" in AON Dimensions: Corporate Governance Special at http://www.aon.com/about/publications/pdf/dimensions/dimensions_1002.pdf .

52. A more conventional definition is that catastrophic risks are infrequent events that cause severe loss, injury or property damage and affect a large population of exposures.

53. For more details consult CyberSource, 6th Annual Online Fraud Report, at http://www.cybersource.com/fraudreport.

54. See http://www.verisign.com/static/030910.pdf .

55. See the full report of the APWG at http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf .

56. For more detail and various analyses of the power crisis in California, see http://business.baylor.edu/Tom_Kelly/Califonrial%20Power.htm as well as the CNN brief at http://www.cnn.com/SPECIALS/2001/power.crisis/backgrounder.html .

57. For reports and examples see: http://www.itweek.co.uk/news/1162306 , http://www.itweek.co.uk/news/1160555 and http://www.winneronline.com/articles/april2004/distributed-denial-of-service-attacks-no-joke.htm .

58. For examples of vulnerability tracking and reports, see http://secunia.com/ , http://www.frsirt.com/ , http://www.us-cert.gov/ or http://www.niscc.gov.uk/niscc/index-en.html . It is sometimes ironically noted that software vulnerabilities, exploits and bugs are in fact "undocumented features".

59. If we define PKI from the perspective of what it does, we can say that it is an infrastructure that creates public key certificates, provides a certificate repository, provides for certificate revocation, maintains a key back-up and recovery facility, provides support for non-repudiation of digital signatures, automatically updates key pairs and certificates, provides management of key histories, provides support for cross-certification with other PKIs, and ensures that client software properly supports the public key functionalities in a secure, consistent and trustworthy manner. UNCTAD (2001) provides an overview of the functioning of PKI in its chapter 6, on managing payment and credit risks online. For a more detailed description, see http://www.entrust.com/resources/docs/pki.htm .

60. An approachable overview of various PKI architectures and their suitability for use by the New Zealand Government can be found at: http://e.govt.nz/docs/see-pki-paper-4/chapter3.html .

61. For a critical commentary on PKI technologies and implementations, see http://www.schneier.com/paper-pki-ft.txt or http://infosecuritymag.techtarget.com/articles/october01/columns_logoff.shtml .

62. For an interesting discussion on the argument for and against FOSS and proprietary software from a security perspective, see http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/open-source-security.html .

63. For an example of opposing views on the issue, one can consult the papers "Is Linux more secure than Windows?" at http://www.microsoft.com/windowsserversystem/facts/analyses/vulnerable.mspx and "Windows v Linux security: The real facts" at http://www.theregister.co.uk/2004/10/22/linux_v_windows_security/ .

64. Some examples are the 1996 WIPO Copyright Treaty (Article 11), the European Copyright Directive (Article 6(1)) or the Unites States Digital Millennium Copyright Act (Section 1201). In general, legislation is formulated to deter the circumvention of so-called digital rights technologies that content owners use with the aim of reducing the scope of use. Examples of this would be that a legally downloaded music file will only play on specified computers or will be copied a limited number of times.

65. The ITU website has a comprehensive explanation of its standards at http://www.itu.int/rec/recommendation.asp?type=products&lang=e&parent=T-REC-X .

66. Examples of other types of self-regulation, often called "control frameworks", would be COBIT (http://www.isaca.org/template.cfm?Section=COBIT6 , FFIEC (http://www.ffiec.gov/ and NIST SP 800 (http://csrc.nist.gov/publications/nistpubs/ . Their application may enable firms and organizations to achieve regulatory compliance.

67. For more information see http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf .

68. For more information, see http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf .

69. The original signatories were the United States, Canada, France and Germany.

70. To form GAISP, the ISSA merged its predecessor, the Generally Accepted System Security Principles, with a related initiative, the Commonly Accepted Security Practices and Recommendations. For more details, see the GAISP Project Overview at http://www.issa.org/gaisp/_pdfs/overview.pdf .

71. For example, the United States Federal Information Security Management Act affects all federal Government resources, and thus the range of improvements in everyday practice is surveyed across all federal agencies, rather than just those that have volunteered or have had success, and in this way provides a healthy level of transparency of governance. See http://reform.house.gov/GovReform/News/DocumentSingle.aspx?DocumentID=22247 .

72. UNCTAD (2003) includes an extensive discussion of the outsourcing phenomenon in its chapter 5: Business process outsourcing service for economic development.

73. There are other relevant regulations in the United States that should be reviewed by ICT service providers and exporters of outsourcing services. These would include the Gramm-Leach-Bliley Act, whose main purpose was to repealed the Glass-Steagall Act in order to open up competition among banks, securities companies and insurance companies and which has impacted financial institutions though added responsibilities for the protection of customers' non-public personal information, and the Health Insurance Portability and Accountability Act, which aims to increase the transfer of health care information from one insurer or provider to the next and which required the development of privacy regulations to protect the confidentiality of individually identifiable health care information. For more details, see http://www.ftc.gov/privacy/glbact/glbsub1.htm and http://www.legalarchiver.org/hipaa.htm .

74. Paragraph 4 of the full text of the framework available at http://www.bis.org/publ/bcbs107.pdf .

75. See paragraph 644 of the full text of the framework available at http://www.bis.org/publ/bcbs107.pdf .

76. For a detailed discussion of information security implications of Basel II see Bruce Moulton, "Basel II: Operational Risk and Information Security" at http://ses.symantec.com/Industry/Regulations/article.cfm?articleid=3270&EID=0

77. See United States Bill H.R.2458 on the management and promotion of electronic government services, SEC. 301. Information Security, § 3544. Federal agency responsibilities, at http://csrc.nist.gov/policies/FISMA-final.pdf .

78. See http://www.sarbanes-oxley-forum.com/modules.php?name=Surveys&op=results&pollID=1 . If anything, the survey should have a positive bias, as only business with intent to implement SOx would visit the forum and vote at the poll.

79. For more details, see http://www.sas70.com/about.htm .

80. For more details, see http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci963032,00.html

81. For more details, see http://www.csoonline.com/analyst/report3172.html or http://magazine.digitalidworld.com/Sep04/Page46.pdf .

82. Regular patching and virus database updates are among the simplest of such measures.

83. See Surendran K (2005).

84. See the Internet Engineering Task Force best practice paper on CRIST at http://www.ietf.org/rfc/rfc2350.txt .

85. Killcrece (2004) provides a useful description of the necessary steps in creating a national CSIRT.

86. From a process point of view, risk retention may precede the risk-transfer/insurance phase. Many firms may first explore what they can retain and then seek insurance cover for risks they cannot keep.

87. See General Assembly resolution 56/261 (A/RES/56/261) http://daccessdds.un.org/doc/UNDOC/GEN/N01/497/54/PDF/N0149754.pdf .

88. See http://www.un.org/Depts/dhl/resguide/r57.htm and http://www.un.orgDepts/dhl/resguide/r58.htm .

89. See ECOSOC (2002).

90. See ECOSOC resolution 1999/23 (E/1999/INF/2/Add.2) at http://www.un.org/documents/ecosoc/docs/1999/e1999-inf2-add2.pdf , and resolution 2001/18 on the implementation of the computer and telecommunication system for international and national drug control (40th plenary meeting, 24 July 2001) at http://www.un.org/docs/ecosoc/documents.asp?id=144 .

91. See chapter 1 of the INCB annual report for 2001, "Globalization and new technologies: challenges to drug law enforcement in the twenty-first century", at http://www.incb.org/incb/annual_report_2001.html.

92. See http://www.itu.int/wsis/docs/geneva/official/dop.html and http://www.itu.int/wsis/docs/geneva/official/poa.html for the text of the WSIS Declaration of principles and Plan of action.

93. From the Preamble of the Convention on Cybercrime at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. As of 28 June 2005, 11 countries had ratified the Convention, and an updated list is available at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG .

94. For more details, see the dedicated ENISA website http://www.enisa.eu.int and the Regulation (EC) No 460/2004 of establishment at http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_077/l_07720040313en00010011.pdf .

95. More information on the European Commission's work on security issues can be found at their dedicated website http://europa.eu.int/information_society/eeurope/2005/all_about/security/index_en.htm and in the document "Proposal for a regulation of the European Parliament and of the Council establishing the European Network and Information Security Agency " (2003) (COM(2003) 63 final).

96. For the original 1992 text of the OECD Guidelines for the Security of Information, see http://www.oecd.org/document/19/0,2340,fr_2649_201185_1815059_1_1_1_1,00.html .

97. The full text of the OECD Guidelines on information security is available at: http://www.oecd.org/dataoecd/16/22/15582260.pdf .

98. The full text of the OECD implementation plan for the OECD guidelines for the security of information systems and networks: Towards a culture of security (2003) is available at: http://www.oecd.org/dataoecd/23/11/31670189.pdf .

99. See http://www.apec.org/apec/about_apec.html .

100. See http://webapps.apec.org/content/apec/ministerial_statements/sectoral_ministerial/telecommunications/2002.downloadlinks.0001.LinkURL.Download.ver5.1.9 .

101. See http://www.apectelwg.org/admin/document/documents/telmin5sub021.htm .

102. See http://www.g8.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1078995913300 .

103. See http://www.g8.utoronto.ca/summit/2003evian/press_statement_march24_2003.html .

104. The conclusions are available at http://www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf .

105. See http://www.fco.gov.uk/Files/kfile/Art%2013%20SAFTI,0.pdf . During the expert consultations in 2003, establishing standards for biometric technologies was considered of particular importance in order to achieve interoperability and ensure their technical reliability and fast progress in implementation.

106. A list of members is available at http://www.first.org/about/organization/teams/index.html .

107. A list of members is available at http://www.apcert.org/member.html .

108. See "Adoption of a comprehensive inter-American strategy to combat threats to cybersecurity: A multidimensional and multidisciplinary approach to creating a culture of cybersecurity", at http://www.cicte.oas.org/Docs/CyberSecurityConference/Cyber%20Strategy-English.doc for the

109. Telephone and radio technologies have not have the same effect as the Internet because in both cases the infrastructures have a high level of centralized control and centralized intelligence. From a security perspective, this allows direct control and solutions and facilitates implementing information security processes and technologies – something the Internet does not do.