International Telecommunication Union

Cybersecurity guide for developing countries

PREFACE

Information and communication technologies (ICT) make it possible to provide the inhabitants of developing countries with basic e-services for health, education, commerce and governance, even though they may lack access to physical infrastructure such as hospitals, schools and public administration.

Thanks to the rapid advances in ICT development, doctors and patients may be linked up electronically, citizens are able to communicate with government online, and businesses using the internet can sell their goods and services to distant customers. New ICT applications are helping to solve some of the problems of access to basic services, and are smoothing the road for developing countries to join the information society.

However, to take full advantage of the benefits promised by the information society, all of the stakeholders will need to work together to address problems such as how to prevent the destruction of information and tampering with data, how to authenticate electronic transactions and how best to tackle the global threat of cybercrime. National borders are of little protection against attacks such as identity theft, spam, phishing and malware (Trojan horses, worms, viruses), which can strike at people's computers from across the globe.

For the benefits of cybersecurity to become a reality, the public and private sectors of every country must have a common understanding of the challenges. The international community must pursue efforts to bridge the knowledge gap between different countries, but also within each individual country.

This reference guide has been designed to increase awareness within the developing countries of the major problems in the area of cybersecurity today, but also to promote sharing of best practices, describe solutions used in other countries and provide some orientation in this vast domain.

At a time when solutions are being elaborated to exploit the many benefits that telecommunications and ICT offer for social and economic development, I trust that this book will help to meet a real need among users, policy-makers and decision-makers, regulators and service providers, particularly in developing countries.

Hamadoun I. Touré

Director
Telecommunication Development Bureau

FOREWORD

The World Telecommunication Development Conference instructed ITU's Telecommunication Development Bureau (BDT) to use the "E-strategies and e-services/applications" programme to design tools for facilitating the exchange of information on best practices, technology and general policy issues. This cybersecurity guide for developing countries has been prepared to that end, and to meet the stated goal of the programme to "enhance security and build confidence in the use of public networks for e-service/applications".

The guide is intended to give developing countries a tool allowing them to better understand some of the issues relating to IT security, and provide them with examples of solutions that other countries have put in place in order to deal with these problems. It also refers to other publications giving further, specific information on cybersecurity. The guide is not intended as an exhaustive document or report on the subject, but rather as a summary of the principal problems currently encountered in countries wishing to take advantage of the benefits of the information society.

The content of the guide has been selected to meet the needs of developing and, in particular, least-developed countries, in terms of the use of information and communication technologies for the provision of basic services in different sectors, while remaining committed to developing local potential and increasing awareness among all of the stakeholders.

In order to avoid any duplication in the treatment of these subjects, the work already accomplished within the framework of ITU-T Study Group 17 was duly taken into account in elaborating the content of this publication, as were the other existing studies and publications in this area.

The Cybersecurity Guide was prepared by Madame Solange Ghernaouti-Hélie, Professor at the University of Lausanne, who, as an ITU expert, worked closely together with the project supervisor, Mr Alexander Ntoko, Head of the E-strategies Unit of BDT.

EXECUTIVE SUMMARY

Social issues, the economy, public policy, human issues: whichever way one looks at it, and whatever one calls it (IT security, telecom security), cybersecurity touches on the security of the digital and cultural wealth of people, organizations and countries. The challenges involved are complex, and meeting them requires that there be the political will to devise and implement a strategy for the development of digital infrastructures and services which includes a coherent, effective, verifiable and manageable cybersecurity strategy.

Obtaining a level of information security that is sufficient to meet technology and information risks is essential for the proper functioning of governments and organizations. The widespread use of digital technologies goes hand-in-hand with increased dependency on those technologies and interdependency of critical infrastructures. This creates a non-negligible vulnerability in the functioning of institutions, potentially endangering them and even undermining the sovereignty of the State.

The goal of cybersecurity is to help protect organizations' assets and resources in organizational, human, financial, technical and information terms, allowing them to pursue their mission. The ultimate objective is to ensure that no lasting harm is done to them. This consists of reducing the likelihood that a threat materializes; limiting the resulting damage or malfunction; and ensuring that, following a security incident, normal operations can be restored within an acceptable time-frame and at an acceptable cost.

The cybersecurity process involves the whole of society, in that every individual is concerned by its implementation. It can be made more relevant by developing a cyber code of conduct for appropriate use of ICTs and promulgating a genuine security policy that stipulates the standards that cybersecurity users (entities, partners and providers) will be expected to meet.

To set up a cybersecurity process, it is important to identify correctly the assets and resources that need to be protected, so as to accurately define the scope of security needed for effective protection. This requires a global approach to security, one that is multidisciplinary and comprehensive. Cybersecurity does not sit well with a freewheeling world that places a premium on permissiveness. What is required is a set of core principles of ethical behaviour, responsibility and transparency, embodied in an appropriate legal framework and a pragmatic body of procedures and rules. These must be enforced locally, of course; but they must also be applied across the international community and be compatible with the existing international directives.

To avoid creating opportunities for crime to grow, the existing telecommunication infrastructures must include suitable security measures of a technical as well as a legal nature. Attacks via cyberspace can take many forms: the clandestine hijacking of a system, denial of service, destruction or theft of sensitive data, hackers breaking into the network, cracking of software protection, phreaking (which includes sabotage, hijacking of telephone exchanges and more). The costs are invariably borne by the victims, i.e. the organizations and individuals who have been targeted.

Considered as a system, telecommunication (both infrastructures and services) represents a security challenge that is largely analogous to the challenge of IT resources. The same technical, organizational and human constraints must be observed in attempting to meet that challenge. Protecting information while it is in transit is necessary; but this is far from sufficient in itself, for the degree of vulnerability increases, if anything, once information enters the processing and storage phase. Cybersecurity must therefore be viewed from a overarching perspective. Purely technical security solutions cannot compensate for the absence of coherent, rigorous management of security needs, measures, procedures and tools. A disorganized stampede to get security tools will hinder use, weigh down operations and impair the performance of IT systems. Proper IT security is a management issue, and the associated tools and services are linked to operational system administration. For example, encrypting data for the purpose of protecting them during transmission is a pointless task if they are subsequently stored in

a non-secure manner. Likewise, installing a firewall will be of little use if connections are permitted to bypass this system.

If activities based on information processing are to grow and narrow the digital divide, this will require:

- reliable and secure information infrastructures (with guaranteed accessibility, availability, dependability and continuity of services)
- policies to create trust
- an appropriate legal framework
- judiciary and police authorities conversant with new technologies and able to cooperate with their counterparts in other countries
- information risk and security management tools;
- security tools that will foster trust in the applications and services offered (commercial and financial transactions, e-health, e-government, e-voting, etc.) and in procedures safeguarding human rights, especially personal data privacy.

Good stewardship of digital information assets, the distribution of non-tangible goods, the exploitation of content and the bridging of the digital divide are all examples of economic and social problems that cannot be addressed by looking only at the technological side of IT security. A response that takes into account the human, legal, economic and technological dimensions of the security needs of the digital infrastructure and of users can help to foster confidence and lead to economic growth that will benefit all of society.

HOW TO READ THIS GUIDE

The Cybersecurity Guide provides an introduction to this important topic, stressing what has changed with the advent of digital data, the virtualization of information and the widespread use of telecommunication networks. The stakes, in terms of the growth of societies, are presented in order to introduce the notion of a security imperative in the world of IT and telecommunication (cybersecurity).

Part I focuses on cybersecurity needs and outlines some elements of solutions. The concept of the security of the communication infrastructure is analysed in the light of the observed vulnerabilities and ambient lack of security of information and communication technologies. Drawing on the lessons learned from an examination of best practices, the daily reality of security on the internet, and the experience acquired by the international community, the specific cybersecurity needs of developing countries are then identified.

The management, policy, economic, social, legal and technology dimensions of cybersecurity are analysed. Generic recommendations are formulated regarding access to telecommunication infrastructures, with a view to controlling risks – whether of criminal origin or not – and fostering confidence in e-services, an important motor of economic development.

Part II looks at the problem of controlling cybercrime. It considers the elements that encourage criminal activity in order to show the limitations of current approaches to security and the struggle against cybercrime, as well as the complexity and scale of the problem facing us.

The various infractions and crimes that can be perpetrated via the internet are presented, with an emphasis on the economic crime viewpoint. Observed criminal behaviour is analysed, as is the profile of criminal hackers, and general descriptions of attacks and malware are given. Some guidelines are identified for preparing to meet the cybercrime threat.

Part III reviews some essential basics about the world of telecommunication and proposes a functional approach and a critical overview of infrastructure security tools.

Part IV describes a comprehensive approach to cybersecurity that takes account of the various legal aspects of the modern technologies, and outlines possible objectives in terms of putting in place security solutions for the communication infrastructure.

At the end of the Cybersecurity Guide the reader will find a glossary of security terms and an array of relevant references and other documents.

ACKNOWLEDGMENTS

The Telecommunication Development Bureau of ITU wishes express its gratitude to Solange Ghernaouti-Hélie and thank her colleagues for their support, in particular Mohamed Ali Sfaxi, Igli Tashi, Sarra Ben Lagha, Hend Madhour and Arnaud Dufour (internet strategy consultant).

This handbook builds on information and studies provided by a variety of organizations, in particular the computer security organizations "Clusif" (*Club de la sécurité informatique français*) and "Cert" (Computer Emergency and Response Team). They deserve our sincere gratitude.

The preparation of this handbook would not have been possible without the excellent cooperation of the members of ITU's E-Strategy Unit, and in particular Alexander Ntoko. We also wish to express our appreciation to Renée Zbinden Mocellin (ITU Publication Composition Service) and her team for their work in producing the Cybersecurity Guide.

TABLE OF CONTENTS

PART I

CYBERSECURITY – CONTEXT CHALLENGES, SOLUTIONS

Section I.1 – Cyberspace and the information society

I.1.1 Digitization

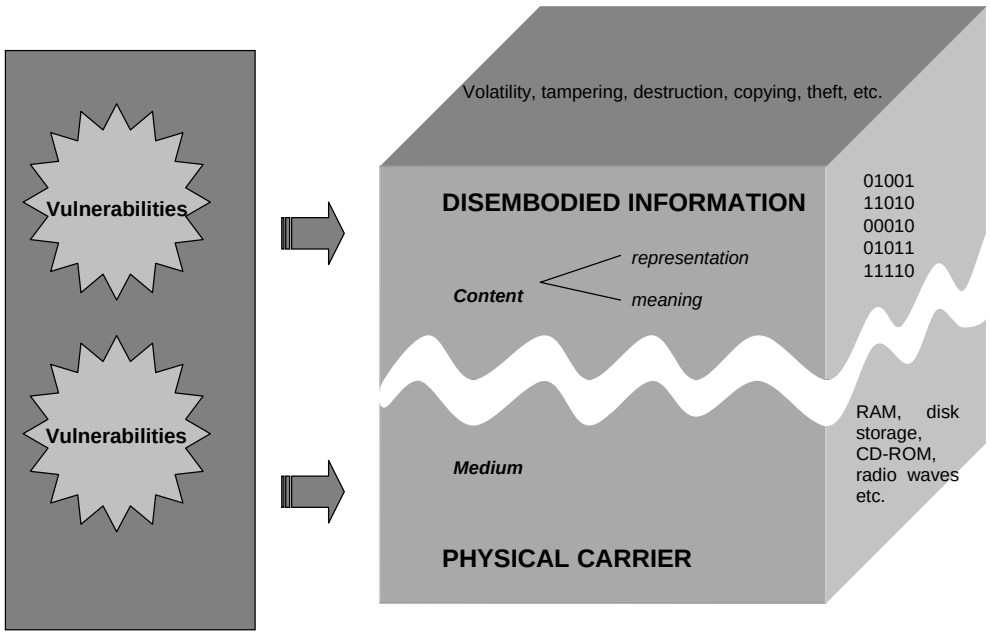
Information technologies are transforming the way we think about and do almost everything in our lives. They are bringing about important structural changes, by allowing us to model *objects* of all kinds in the form of information, and hence manipulate them electronically.

I.1.1.1 Digital information

Digitization creates a digital image of something real (a virtual version of the object). All information, whatever its nature – whether voice, data, or image – can be digitized and represented in some standardized manner.

Digitized information becomes disembodied, that is, it is no longer tied to the medium in which it is represented and stored. The information itself (content) adds value, because it costs a lot less to share and store than to produce (Figure I.1). In addition, data can be localized and processed in several places at once. The possibility of perfect duplication *ad infinitum* hollows out the notion of "original" data, with potentially troubling implications for the concept of copyright protection.

Figure I.1 – Virtualization and digital information



I.1.1.2 Digital technology

Digital technology, by standardizing data production, processing and transfer, has made it possible to construct a continuous digital information chain. In combination with data compression techniques, this digital convergence creates opportunities for synergies between IT, telecommunications and audiovisual media, as illustrated by the phenomenon of the internet. So the real technology revolution was brought about by the digitization of information, and its consequences go far beyond the world of telecommunication.

This new dimension of information processing affects all areas of human endeavour and work. Both the determination of value and modes of production, from product design to distribution, have evolved

in recent years. This has led to the reorganization of value chains among the different players in the economy.

I.1.1.3 Infrastructure and content

Controlling the digital information chain, i.e. the infrastructure and the content, has become the major challenge of the 21st century. The new market, open to all, is characterized by the unprecedented mobilization of all players in a global economy: telecommunication operators, cable operators, hardware and software manufacturers, television broadcasters, etc.

The new economic challenge for today's organization is that created by unrestrained competition and the reorganization of roles and activities.

When Gutenberg printed his first book, he had no way of imaging the industrial repercussions that his invention would have; in the event, they represented the first step on the road to industrial automation. Something similar happened at the end of the 1960s, when universities and military users, each motivated by their own, ostensibly conflicting objectives, started to set up a communication network that would become the internet. Like their predecessors of the 15th century, they acted without being fully aware of the consequences of their creation. Today, cyberspace heralds the transition of societies to the information age.

I.1.2 The information revolution

The information revolution profoundly alters the way information is processed and stored. It changes the way organizations, and indeed society as a whole, function. It is not the only technical innovation to have taken place in recent years, but it stands out because of its impact on the processing of information, and hence of knowledge. Because the information revolution affects the mechanisms by which knowledge is created and shared, it can be viewed as the wellspring of future innovation, from which the developing countries should not be excluded.

The evolution of information and telecommunication technologies leads to a genuine revolution in how we think about economic, social and cultural exchanges. It also gives us a new model of information technology based on the network, in which the security of the flow of information needs to be ensured if new applications are to be developed that will make organizations still more effective. No form of economic activity can exist without exchanges and interaction between the participants; no exchange of information is possible without some basic security guarantees; and no service can be planned without taking into account the quality of service. However, we must also bear in mind that the success of a communication depends on the ability of the parties involved to deal with the technical constraints and manage the customs that any exchange of information involves.

I.1.2.1 Innovation and development

Organizations and countries need to focus on innovation capacities and rapid adaptability, backed up by a powerful and secure information system, if they wish to survive and assert themselves as long-term players in the new competitive environment.

New areas of activity are being opened up by the diversification of telecommunication and the possibilities created by extended information technology, the benefits of which should accrue to the developing countries, too.

The technological and economic improvements made possible by the deployment of reliable IT infrastructures holds great promise for ordinary people. At the same time, however, they introduce an unprecedented degree of technological and management complexity. The associated significant risks must be kept under control, to avoid vitiating the very notion of progress. With technological risk, e.g. a failure of information processing and communication systems, brought about by a malfunction of accidental or malicious origin, comes an information risk, liable to undermine an organization's ability to make use of information.

An important point to bear in mind is that, while access to information technology is widespread and growing, a far from negligible part of the population remains excluded from the information

revolution. The reasons for this are complex, and include cultural and financial factors, as well as, in some cases, basic difficulties such as illiteracy. More than in any other domain, training and education are crucial to democratizing information technology and combating info-exclusion. The communication interfaces will also need to be thought anew so as to serve the population better and respect the diversity of cultural contexts. Computers should be adapted to the human setting in which they must be integrated, rather than dictating a new communication order.

I.1.2.2 Supporting the information revolution

Information and communication technologies, like all technology, emerge and operate in a particular historical and geographical context, generally reflecting a balance within the society. The responsibility of the people involved is to support the information revolution with the tools, procedures, laws and ethics needed to deal with security and meet the expectations and needs of society.

Currently, the utilization of communication media and the freedom to send and receive messages are covered by a host of partial regulations from ITU, UNESCO, the United Nations, OECD, the Council of Europe, and others. Developments in information and communication technologies and the way people use them have outpaced the regulations that govern them. There is therefore a need for an appropriate legal framework to be put in place to address such issues as: the aterritorial nature of networks such as the internet, the problems of responsibility, and the protection of privacy and of property rights. Technological evolution needs to be paralleled by an evolution of the social, political and legal order. This cursory consideration already gives an idea of the importance of the challenges created by the information age, the crucial role of telecommunication in meeting them, and the importance of dealing with security issues before they become a hindrance to development.

The transition to the information age reveals the importance of information technology and makes it clear that the technology needs to be mastered. Considering the new dimensions that IT creates, in technical and socio-economic terms, it is clear that the security of IT and telecommunication systems and infrastructures has become a fundamental need. It highlights the strategic and critical nature of what is at stake in planning and implementing cybersecurity, for countries, for organizations, and for individuals.

In view of the financial, material and human resources that countries have invested in creating their information and telecommunication infrastructure, it is essential for them to ensure that the infrastructure is secure, well-managed and controlled.

Section I.2 – Cybersecurity

I.2.1 The security context of the communication infrastructure

There is increasing awareness of the importance of mastering operational IT risks, with the growing utilization of new technologies, the existence of a global IT infrastructure, and the emergence of new risks.

The transformation of societies into an *information* society, made possible by the integration of new technologies in every sphere of activity and every type of infrastructure, increases the dependence of individuals, organizations and countries on information systems and networks. This is a major source of risk, which must be treated as a security risk.

The developing countries are faced with the problem of needing to join the information society without ignoring the risks of becoming dependent on technologies and technology providers, and

avoiding the danger that the digital divide gives rise to a security divide or even a heightened dependency on entities that control their needs and the means of IT security[1].

The telecommunication infrastructures and the services and activities that they make possible have to be conceived, designed, set up and managed with security in mind. Security is the cornerstone of any activity; it should be viewed as a service that makes it possible to create other services and generate value (e.g. e-government, e-health, e-learning). It is not a matter of technology alone[2]. Until now, however, the basic communication tools that have been made available have not come with the resources that are both necessary and sufficient to provide or to guarantee a minimum level of security.

Networked IT systems are resources that can be accessed remotely; as such, they are potential targets for a cyberattack. Systems are exposed to a heightened risk of intrusion, and opportunities multiply for attacks to be launched and crimes to be committed. While systems are the targets of attacks, the prize that the attackers pursue is the information being processed (Figure I.2). Attacks can affect the ability to process, store and share information capital, and they can inflict damage on intangible and symbolic goods, production processes, and the decision-making processes of the organization. Cybersystems introduce an operational risk in the operation of the organizations that own them.

Dealing with the complex, multifaceted cybersecurity problems raised by telecommunication networks and open systems can thus be relatively difficult, and the potential repercussions and impact on the operation of organizations and countries can be devastating. Factors that are crucial to the success of economies may depend on the ability to provide security for information, processes, systems and infrastructure.

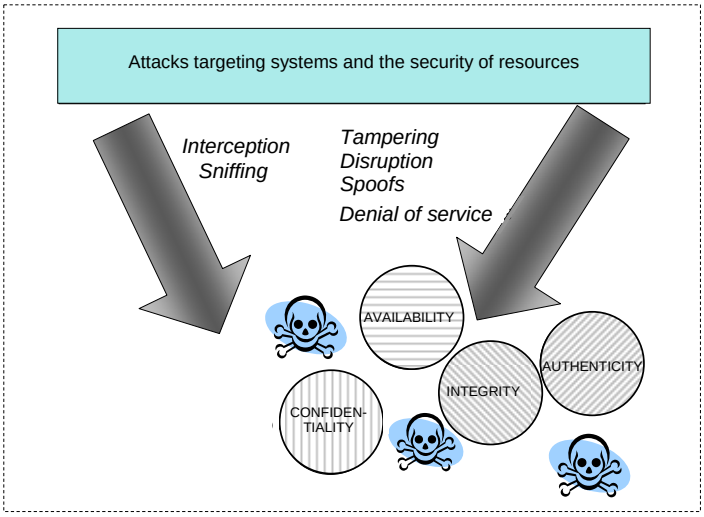
Widespread system interconnection, increasing linkage between infrastructures, growing dependence on digital technologies, and the growth of threats and risks, make it necessary for individuals, organizations and countries to take steps, adopt procedures and acquire tools to improve the way that technological and cyber-risks are managed. The challenges of the struggle to contain the technological risks are those of the 21st century itself. They call for a comprehensive global approach to security that will include the developing countries.

---

1 S. Ghernaouti-Hélie: "From digital divide to digital unsecurity: challenges to develop and deploy an unified e-security framework in a multidimensional context", in *International Cooperation and the Information Society*, section of the Swiss development policy directory, IUED publications. Geneva, November 2003.

2 A. Ntoko: "Mandate and activities in cybersecurity – ITU-D". WSIS thematic meeting on cybersecurity. ITU, Geneva 28 June-1 July 2005.

Figure I.2 – Attacks targeting systems and the security of resources



It is not enough to set up points of access to the telecommunication networks. It is necessary to deploy IT infrastructures and cyberservices that are reliable, maintainable, robust and secure, while respecting basic human rights and the rights of States. The need to protect systems and valuable information has to coexist and be made compatible with the parallel protection of the rights and privacy of individuals.

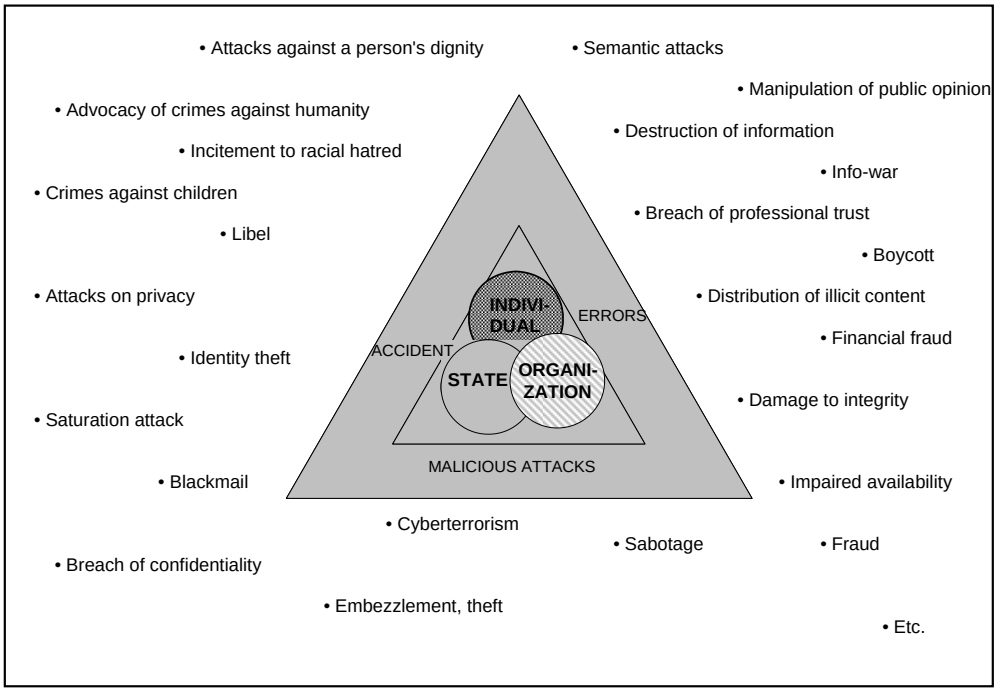
Developing countries need to enter the information society without exposing themselves to excessive risk, building on the experience acquired in the developed countries and avoiding the danger that a new factor for their exclusion arises in the form of cybersecurity.

I.2.2 What is at stake with cybersecurity

Social issues, the economy, public policy, human issues: whichever way one looks at it, and whatever one calls it (IT security, telecom security), cybersecurity touches on the security of the digital and cultural wealth of people, organizations and countries (Figure I.3). The challenges involved are complex, and meeting them requires that there be the political will to devise and implement an overall strategy for the development of digital infrastructures and services which includes a coherent, effective, verifiable and manageable cybersecurity strategy. The cybersecurity strategy must be part of a multidisciplinary approach, with solutions in place at the educational, legal, management and technical level. A strong response to the human, legal, economic and technological dimensions of digital infrastructure security needs can build confidence and generate welcome economic growth benefiting all of society.

Mastery of digital information wealth, distributing intangible goods, adding value to content, and bridging the digital divide are all problems of an economic and social nature, which call for something more than a one-dimensional, strictly technological approach to cybersecurity.

Figure I.3 – The levels of cybersecurity: individuals, organizations and countries



If activities based on information processing are to grow and thus help to narrow the digital divide, this will require:

- reliable and secure information infrastructures (with guaranteed accessibility, availability, dependability and continuity of services);
- policies to create trust;
- an appropriate legal framework;
- judiciary and police authorities conversant with new technologies and able to cooperate with their counterparts in other countries;
- information risk and security management tools;
- security implementation tools that will foster confidence in the applications and services provided (e-business, e-finance, e-health, e-government, e-voting, etc.) and in the procedures set up to protect human rights, in particular regarding privacy.

The goal of cybersecurity is to help protect the organization's assets and resources in organizational, human, financial, technical and information terms, allowing it to pursue its mission.

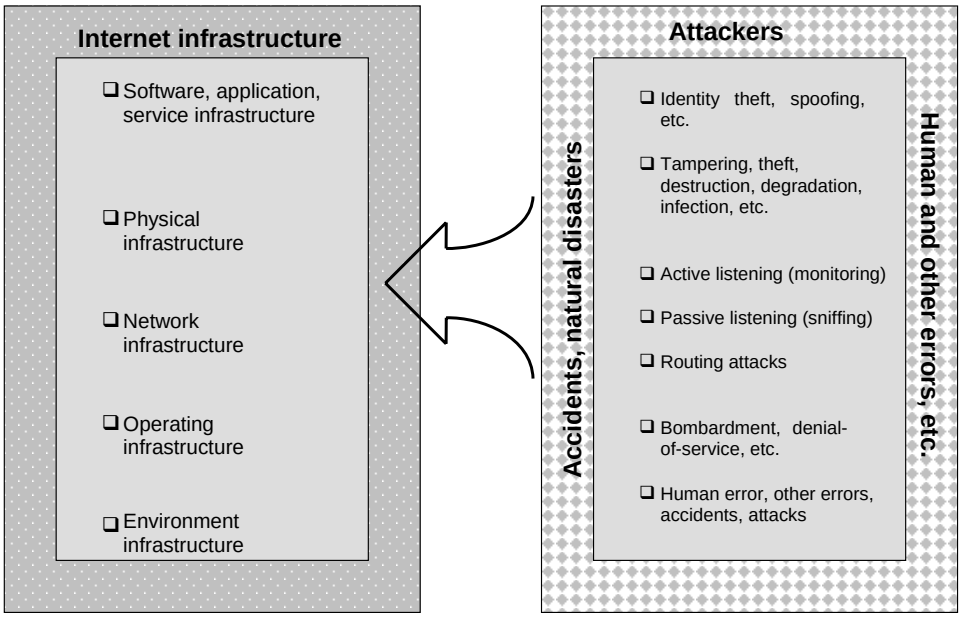
The ultimate objective is to ensure that no lasting harm is done to the organization. This consists of reducing the likelihood that a threat materializes; limiting the resulting damage or malfunction; and ensuring that, following a security incident, normal operations can be restored within an acceptable time-frame and at an acceptable cost.

The cybersecurity process involves the whole of society, in that every individual is concerned by its implementation. It can be made more relevant by developing a cyber code of conduct and promulgating a genuine security policy that stipulates the standards that cybersecurity users, entities, partners and providers will be expected to meet.

I.2.3 The security deficit

The security deficit in information and communication technologies is a reflection of the nature of IT and of cyberspace. The fact that users move in a virtual world, acting remotely and relatively anonymously, compounds the difficulties of designing, implementing, managing and controlling this technology; when one adds failures, malfunctions, errors, mistakes, inconsistencies and even natural disasters into the equation, the result, not surprisingly, is an aura of insecurity that taints the IT infrastructure (see Figure I.4).

Figure I.4 – The internet infrastructure and the many origins of problems



In this context, there are many ways in which a malicious attacker may exploit vulnerabilities[3].

The proliferation of such attacks – including identity theft, system spoofing, intrusion, resource hijacking, infection, deterioration, destruction, tampering, breach of confidentiality, denial of service, theft, extortion, etc. – illustrates the limitations of current security strategies, but also, paradoxically, shows that the infrastructures have a certain robustness.

Whatever the motivations of individual computer criminals may be, the results always include a far from trivial economic impact. Cybercrime is fast turning into an international hydra-headed monster.

Security solutions do exist, but they are never absolute, and generally represent no more than a response to a particular problem in a specific context. The result is that the security problem is displaced, and the responsibility for security shifts; furthermore, the solutions in their turn need to be secured, and managed in a protected manner.

They represent, at best, a tentative attempt to deal with the dynamic reality facing them: fluid technology, shifting targets, evolving hacker skills, and mutating threats and risks. There can thus be

3 Cybercrime, cyberattacks and cyberoffences are discussed in depth in Part II.

no guarantee that a particular approach to security will provide lasting protection, nor, as a corollary, that the return on the investment it represents can be assured.

Security strategy is often limited to setting up mechanisms to reduce the risks to which the organization's information assets are exposed, usually by means of a purely technological approach. A better strategy would be one that takes into account all the dimensions of the problem and addresses the security needs of individuals, in particular as regards the protection of privacy and basic rights. Cybersecurity should cover everyone, extending protection to data of a personal nature.

Security solutions are already available. In many cases they are purely technological in nature, addressing a particular problem in a specific context. But, like all technology, they are fallible and can be circumvented. In most cases they merely displace the security problem and shift responsibility to another part of the system they are supposed to protect. Furthermore, they are themselves in need of protection and secure management. They can never provide absolute or final protection, due to the evolutionary nature of the security context, itself a result of the dynamic environment (evolving needs, risks, technologies, hacker skills, etc.). There is thus a problem because existing solutions are short-lived at best. Another problem is that the proliferation of heterogeneous solutions may harm the overall coherence of the security strategy. Clearly, technology alone will not suffice; it must be integrated in a management approach.

Overall coherence of the security strategy is complicated by the wide range of different entities and individuals involved (engineers, developers, auditors, systems engineers, legal experts, investigators, clients, suppliers, users, etc.) and by the broad array of interests, visions, environments, and languages. A unified, systemic grasp of security risks and measures is needed, and a recognition of the respective responsibilities of all involved, if it is hoped to achieve the level of security that is required to confidently conduct activities using information and communication technologies, and contribute to building confidence in the digital economy.

I.2.4 Lessons to be drawn

I.2.4.1 Take charge of security

At the start of the 21st century, most major organizations – and many smaller ones – have generally accepted the importance of facing up to the challenges of IT security. Security strategy is no longer conceived as merely a hotchpotch of security tools. Instead, it is widely – and correctly – viewed as an ongoing process.

The goal of security governance is to ensure that the most suitable security measures are used at each place and time. This concept is based on the following simple questions:

- Who does what, how and when?
- Who are the players who develop the rules, define and validate them, implement them and exercise control over them?

I.2.4.2 Identify and manage the risks

The security strategy for digital infrastructures must be guided by an analysis of the risks associated with information processing, telecommunication and cyberspace, as part of the risk management process. The IT security risks (also referred to as computer risks, information risks or technology risks) need to be identified along with all the other risks facing the organization (strategic, social, environmental, etc.).

IT risks are operational risks, which need to be mastered. At the heart of risk management is an analysis of security needs, which makes it possible to define a security strategy and security policy. A number of questions need to be asked at this stage:

- Who will be in charge of the risk analysis and risk management?
- What is the best way to conduct the analysis?
- What tools and methods are available?

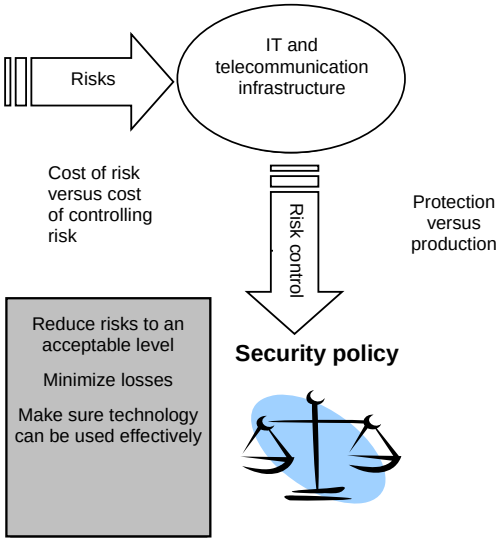
– How reliable are they?
– How much emphasis will there be on results? What are the costs?
– Would it be better to outsource this function ?
– Etc.

Risk may be defined as a danger that can be anticipated to some extent. It is quantified by the likelihood of damage and the resulting harm. Risk expresses the probability of an asset or value being lost due to a vulnerability connected with some hazard or danger.

In deciding on the desired level of protection and the types of security measures to put in place, it is necessary to balance the magnitude of the risk (in financial terms) against what it would cost to reduce it (see Figure I.5). As a minimum, the assets to be protected must be identified, along with the rationale for protecting them, depending on actual constraints and the available organizational, financial, human and technical resources. The measures taken must be effective, and must reflect a balance between performance and cost-effectiveness.

For an organization, mastering IT risks means elaborating a strategy, defining a security policy and deciding on its tactical and operational implementation.

Figure I.5 – Trade-offs in controlling risk: a policy decision



I.2.4.3 Define a security policy

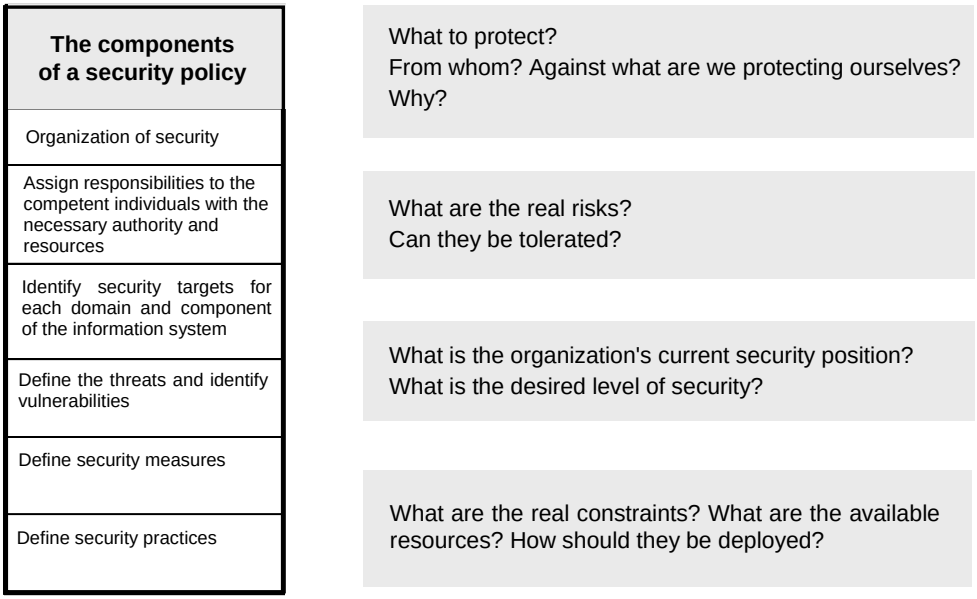
The security policy translates what is understood about the risks and their impact into security measures for implementation. It facilitates both prevention and remedial action in response to security problems, and helps to reduce the risks and their impact.

While it is impossible to eliminate risk entirely, and difficult to anticipate all the emerging threats, it is important to reduce the vulnerability of environments and resources that are to be protected, as it certainly lies at the origin of many of the security problems.

The security policy should specify, among other things, the resources, structure, procedures, and plans for defence and mitigation to ensure that operational, technological and information risks can be controlled.

ISO 17799 proposes a code of practice for security management. It can be considered as a reference for defining a security policy; as a checklist for analysing risk; as a security audit tool, whether for purposes of certification or not; or as a communication hub for security. The standard can be interpreted, and implemented, in various ways. Its value resides in the fact that it addresses the organizational, human, legal and technological aspects of security at each of the different stages of design, implementation and maintenance of security. The 2005 version of the standard (ISO/IEC 17799:2005)[4] emphasizes risk evaluation and analysis, management of assets and resources, and incident management. This is indicative of the importance that is attached to the management dimension of security.

Figure I.6 – To manage security, first define a security policy



The effectiveness of a security policy should not be measured by the size of its budget; rather, it depends on the risk-management policy, and on the quality of the risk analysis (Figure I.6). Among the factors that determine the risk are the area of activity of an organization, its size, its image, system sensitivity, the system environment and associated threats, and the degree to which the organization depends on its information system.

The quality of IT security depends primarily on the identification and evaluation of the value of the information assets, operational deployment of appropriate security measures based on a well-conceived security policy, and effective management.

I.2.4.4 Deploy the solutions

Various types of measures need to be instituted to make the IT and telecommunication infrastructure more secure. These include:

– build awareness; educate and train all stakeholders for cybersecurity;

4 The table of contents of the standard is given in Annex B to this guide.

- create units that can function as the national early-warning and crisis-response centre, pool the resources necessary to do so effectively and share them across several countries, for a region;
- institute surveillance and checks (analogous to road checks);
- build expertise in a cyberpolice team that can contribute to a cooperative international effort for the investigation and prosecution of computer-related crime;
- develop technological solutions for identity management, access control, the use of secure hardware and software platforms, back-up infrastructures, encryption protocols and operational management.

I.2.5 The management perspective

I.2.5.1 Dynamic management[5]

Approaching security through a dynamic and continuous management process positions the organization to deal with the dynamic nature of the risk and the evolving needs, by continuously adapting and improving its solutions. The quality of the security management will determine the level of security provided. The cybersecurity policy should be defined at the level of top management. There are as many security strategies, policies, measures, procedures and solutions as there are organizations with security needs that need to be met at any particular time.

For an example of the dynamic context within which security management must operate, consider the process of detecting and patching security vulnerabilities. This is done by means of periodic issues of security patches. Information newsletters, more or less customized, make it possible to stay informed about vulnerabilities that have been detected and how to patch them up. If a minimum level of security is to be maintained, the security administrator or system administrator will have to install the security patches as they are issued. However, knowledge of dangerous system vulnerabilities is useful not just to the security administrator, but also to hackers, who may attempt to exploit them before the patches have been applied. It is therefore imperative to allocate sufficient resources to implement a dynamic management that continuously updates the security solutions and thus maintains a consistent level of security.

Published alerts and patches allow the administrator to control the update process (by choosing whether to install those patches or not); it is also possible to do so in automatic mode, effectively delegating the responsibility for regular and systematic patch installation to the software publisher.

This raises the question of responsibility. For example, what are the legal consequences of a software update that has been declined, when problems arise from the exploitation of an uncorrected vulnerability? Since numerous attacks do just that, the question of who decides, and the responsibility of the system administrator, is a very pertinent one.

The dynamic dimension of security represents a crucial challenge not only for the providers of security tools and software publishers, but also for system administrators and security administrators, who rarely have the time needed to incorporate all of the patches and updates that are available.

As computer managers, security administrators and system administrators possess full access to the organization's IT resources, not only is it necessary to apply strict surveillance and control procedures for their activity (proportionate to the risks to which they potentially expose the systems under their control), but these staff must also display irreproachable personal integrity.

I.2.5.2 Outsourcing and dependence

Service providers who offer anti-virus and anti-spam filters effectively take over a part of the security management for their customers. This trend is starting to change the distribution of roles and responsibilities in security matters. Security will increasingly be shifted onto the service provider or

---

5 The following two sections are adapted from an article entitled "*Sécurité informatique, la piège de la dépendance*", A. Dufour, G. Ghernaouti-Hélie, *Revue Information et Système*, 2006.

technical provider. This shift does not, of course, resolve the problem of security, it merely transfers it to the service provider, who becomes responsible not only for the availability and performance of the service, but also for the management and maintenance of a certain level of security.

Publishers of anti-virus software typically offer an automatic update service. The addition of this new dimension of service makes software rental increasingly attractive, as the responsibility for maintenance is transferred to the publisher for a lengthy period. It also fuels a broader trend towards outsourcing of applications and a concomitant business model.

The question of outsourcing or delegating all or part of the security mission is not a purely technical one. It is of a strategic and legal nature, and raises the fundamental issue of dependence on suppliers.

A security outsourcing strategy may include the definition of policy, its implementation, access management, firewall administration, remote maintenance of systems and networks, third-party application maintenance, back-up management, and so on. The choice of a contractor must be accompanied by a quality-control process, and may take into account such things as the contractor's experience, in-house expertise, technologies used, response time, support service, contractual arrangements (e.g. guaranteed results), or sharing of the legal responsibilities.

I.2.5.3 Preventive and remedial action[6]

Security prevention is, by definition, proactive. It involves the human, legal, organizational, economic (ratio between implementation cost/level of security/services offered) and technological dimensions. Until now, IT environment security has concerned itself largely with the technical dimension. This way of understanding information systems security, primarily from a technical point of view, neglecting the human dimension, is a real problem in controlling the technology risk associated with criminal acts. This is because criminality is primarily a human issue, and not a technical one. A purely technical response is therefore inappropriate for controlling what is essentially a human risk.

The approach to addressing IT criminality is typically one of reaction and prosecution. It thus comes after the event, i.e. following the occurrence of an incident which by definition has highlighted a gap in the protective measures. It is necessary not only to prevent and deter cyberattacks by developing investigative/criminal mechanisms, but also to identify in the security policy those measures that are needed to respond to attacks and prosecute the attackers. For this, back-up and continuity plans must be designed and put into place, incorporating the constraints related to the investigation and prosecution of cybercrime within the different work processes and objectives, with specific time-scales.

I.2.6 The political dimension

I.2.6.1 Responsibility of the State

The State possesses considerable responsibility for making digital security a reality. This is particularly true for the definition of an appropriate legal framework, one that is unified and practical. The State should not merely promote and encourage research and development in security but also promote a security culture and demand compliance with minimum security standards (security should be built into products and services), while strengthening law enforcement in respect of cybercrime. This raises the question of the underlying financial model and public-private partnership for national and international action plans.

At the strategic level it is necessary to ensure prevention, reporting, information sharing and alert management. It is also necessary to raise awareness of best practices in risk management and security. Another important requirement is for coordination and harmonization of legal systems. Assistance to promote law enforcement and security, the elaboration of proposed cooperative ventures (formal/informal, multilateral/bilateral, active/passive, national/international) must also be defined.

---

6 This section is adapted from the book *Sécurité informatique et réseaux* by S. Ghernaouti-Hélie, Dunod 2006.

At the same time, it is essential to provide education, information and training in information processing and communication technologies, not merely security and deterrent measures. Building awareness of security issues should not be limited to the promotion of a particular security culture and cyber code of conduct. The security culture must be underpinned, upstream, by an IT culture.

The different players must be given the means to learn to manage the technological, operational and information risks that threaten them in connection with the use of new technologies. In this context, the State must also encourage reporting of instances of cybercrime and ensure that there is trust between the various players of the economic world and the legal and law-enforcement authorities.

Those authorities, but also the civil-defence authorities, emergency services, armed forces and security forces, have a tactical and operational role to play as well, in the struggle against cybercrime, in order to protect, prosecute and repair. Surveillance, detection and information centres for IT and criminal risks must be made operational in order to provide prevention, necessary for the control of those risks.

It is up to each State to define a development policy for the information society reflecting its own particular values, and to provide the resources necessary to make it a reality. This includes the means for protection and the struggle against cybercrime.

To contain cybercrime in a global, centralized and coordinated manner, a response is needed at the political, economic, legal and technological level, a single response that can be adopted by all of the players in the digital chain as fellow partners in security.

I.2.6.2 State sovereignty

The desire for simplicity and effectiveness in security is at odds with the complexity of needs and environments, and makes the outsourcing of services and system and information security to specialized providers more attractive. This tendency creates a high, or total, degree of dependence. This is a major security risk. States must beware of becoming dependent for the strategic, tactical and operational management of their security on external entities that are beyond their control.

Governments have a role to play in imposing the following:

- build in security capability (security by default) that is user friendly, intuitive, transparent and verifiable;
- keep individuals and organizations from putting themselves into dangerous situations (avoid lax configuration, risky behaviour, over-dependence, etc.);
- compliance with security standards;
- mitigation of vulnerabilities in technologies and security solutions.

I.2.7 The economic dimension

The point of security is not to make money, but to avoid losing it. While it may appear relatively straightforward to estimate what security costs (associated budgets, cost of security products, training, etc.), assessing the profitability of security is more difficult. Taking a subjective approach, one might suppose that security measures intrinsically possess a "passive" form of effectiveness that prevents certain potential losses.

Nonetheless, it is difficult to weigh the cost of security and the costs associated with losses due to accidents, errors or malicious acts. The cost of security is a function of the needs of the organization, and depends on the assets to be protected and the cost of damage resulting from insufficient security. There is thus no ready answer to the following questions:

- How can the organization's risk exposure be evaluated, especially the serial risks that are due to the interconnection of infrastructures between organizations?
- How can the indirect costs of a lack of security be estimated, such as those associated with damage to image or espionage?
- What can security yield for the organization that implements it?
- What is the economic value of security?

– What is the return on investment of security?

The economic value of security must be conceived in the broadest social sense, taking into account the impact of new technologies on individuals, organizations and nations. It cannot be reduced to the costs of installation and maintenance.

I.2.8 The social dimension

It is important to make all participants in the internet aware of the importance of getting security right, and what the basic steps are that will strengthen the level of security if they are clearly formulated, defined and implemented intelligently.

Information campaigns and civic education for a responsible information society, covering the challenges, the risks and the preventive and deterrent security measures, are needed in order to educate all cybercitizens to buy into the security process.

The emphasis should be on the duty of security, individual responsibility and deterrent measures, as well as the potential implications under criminal law of a failure to respect security obligations. More generally, it is also necessary to provide education and training in information and communication technologies, and not merely security and deterrent measures. The awareness of security issues should not be limited to the promotion of a certain security culture. The security culture must be embedded within an IT culture, perhaps in the form of the computer user's licence recommended by the CIGREF (*Club Informatique des Grandes Entreprises Françaises*), an association of major French corporations for IT issues[7].

The internet should be made into a commons open to all, so that all cybercitizens can potentially benefit from the infrastructures and services at their disposal, without taking excessive security risks. A code of security ethics needs to be developed, accepted and respected by all players in cyberspace.

I.2.9 The legal dimension

I.2.9.1 Critical success factor

Some bodies of national law and international conventions legally bind organizations to put into place security measures. As a result, the managers of the organization, and, by virtue of the delegation of authority, their security administrators, have an obligation with respect to security measures (but not an obligation in terms of results). A legal entity that is guilty of a security lapse leading to an infraction may have a responsibility of a criminal, civil or administrative nature. Whether or not such responsibility is established will of course have no bearing on the criminal responsibility of the individuals who are guilty of the infraction.

Appropriate legislation on data processing makes it possible to strengthen the economic partners' confidence in the national infrastructure, contributing to the economic development of the country. Thus, by helping to create a favourable context for data exchange based on compliance with the law, they act as a factor for the adoption of information and communication-based services by the general public. Legislation and security may be viewed as two levers of the national economy. Cybersecurity conceived in terms of confidence and quality lays the foundations for the development of a sound service economy.

I.2.9.2 Strengthening legislation and enforcement

At the present time, cybercrime is not well controlled, as becomes clear if one examines the annual statistics produced by the Computer Security Institute (CSI)[8] or the Computer Emergency and

7 www.cigref.fr

8 www.gocsi.com

Response Team (CERT)[9]. Thus, it may be seen how security measures put in place by organizations tend to provide protection for a given environment, in a particular context, but are helpless to prevent criminal activity via the internet. The reasons for this state of affairs have to do, in particular, with the following:

- the nature of cybercrime (automation, intelligent malware, remote activation);
- the ease and impunity with which hackers can usurp legitimate user identities, thereby thwarting the ability of the legal system to identify the authors of a criminal act;
- the need to resolve competence issues before conducting an investigation;
- lack of human and material resources within the services responsible for anti-cybercrime work;
- the transnational nature of cybercrime, which necessitates frequent calls for international assistance and judiciary cooperation, imposing time delays that are at odds with the speed of the attackers and the demand for immediate resumption of operation of IT systems that have been attacked;
- the absence of appropriate categories, in some jurisdictions;
- the inadequate definition and transient nature of most IT-related evidence.

For all of these reasons, the legal system remains ineffective in the context of the internet. Furthermore, just as there are tax shelters, so there are legal safe havens. The proliferation of computer-related crime is not necessarily a sign that there are not enough laws. Existing laws already cover many of the activities of IT criminals and hackers.

What's illegal offline, is also illegal online

New legislation, born of the need to define a suitable legal framework adapted to the use of new technologies, is needed to complement many of the existing laws, which, of course, also apply in cyberspace.

It is not enough to strengthen legislation, if the means to apply it are not there. A law is of little use if law enforcement is not up to the task of gathering and analysing evidence and identifying and prosecuting the perpetrators of criminal acts. If hackers are confident that they will escape punishment, that is proof that the law is ineffective.

I.2.9.3 Combating cybercrime while respecting digital privacy: a tricky compromise

The means needed to combat the growing international scourge of cybercrime require a legal framework that has been harmonized at the international level and can be applied effectively, along with the means for true international cooperation at the level of the police and justice authorities.

National governments have important responsibilities in ensuring cybersecurity. This is particularly true for the definition of the suitable legal framework, i.e. one that is uniform and applicable, for the promotion of a security culture that will respect individuals' right to digital privacy while strengthening efforts to combat cybercrime.

The struggle against cybercrime must have as its principal objective the protection of individuals, organizations and countries, bearing in mind the fundamental principles of democracy.

The tools used to combat cybercrime are potentially inimical to human rights, and may undermine the privacy of personal information. Security requires surveillance, verification and profiling. Checks and balances are essential if abuses of power and of position are to be prevented, the temptation of totalitarian methods resisted, and respect of basic rights guaranteed, including the right to cyberprivacy and the protection of confidential personal information.

9 www.cert.org

In addition to the European directive of 1995, other laws for the protection of personal information have been on the books in various countries for a number of years:

Germany:	Law of 21 January 1977
Argentina:	Law on the protection of personal information, 1996
Austria:	Law of 18 October 1978
Australia:	Law on privacy, 1978
Belgium:	Law of 8 December 1992
Canada:	Law on the protection of private information, 1982
Denmark:	Law of 8 June 1978
Spain:	Law of 29 October 1992
United States:	Law on the protection individual freedoms, 1974; Law on databases of private information, 1988
Finland:	Law of 30 April 1987
France:	Law on information technology and liberty of 6 January 1978, amended in 2004
Greece:	Law of 26 March 1997
Hungary:	Law on the protection of personal information and the communication of public information, 1992
Ireland:	Law of 13 July 1988
Iceland:	Law on the recording of personal information, 1981
Israel:	Law on the protection of privacy, 1981, 1985, 1996; Law on the protection of information in the administration, 1986
Italy:	Law of 31 December 1996
Japan:	Law on the protection of computerized personal information, 1988
Luxembourg:	Law of 31 March 1979
Norway:	Law on personal data records, 1978
New Zealand:	Law on official information, 1982
Netherlands:	Law of 28 December 1988
Poland:	Law on the protection of personal information, 1997
Portugal:	Law of 29 April 1991
Czech Republic:	Law on the protection of personal information in computerized systems, 1995
United Kingdom:	Law of 12 July 1988
Russia:	Federal law on information, informatization and the protection of information
Slovenia:	Law on the protection of information, 1990
Sweden:	11 May 1973
Switzerland:	Federal law on the protection of information, 1992
Taiwan:	Law on the protection of information, 1995

I.2.9.4 International cybercrime legislation

The first international convention set up to address the international character of cybercrime was the Council of Europe "Convention on Cybercrime"[10] adopted in Brussels on 23 November 2001, which entered into force in July 2004 (following its ratification by five of the signatory countries, at least three of which had to be from the Council of Europe). The convention contains the following points.

– Substantive criminal law:
  - offences against the confidentiality, integrity and availability of computer data and systems;
  - computer-related offences;

[10] www.conventions.coe.int/Treaty/FR/Treaties/Html/185.htm

- offences related to infringements of copyright and related rights.

– Procedural law:
  - expedited preservation of computer and traffic data and rapid disclosure of the latter to the competent authorities;
  - preservation and maintenance of the integrity of computer data for a period of time as long as necessary to enable the competent authorities to seek its disclosure;
  - production order;
  - search and seizure of stored computer data;
  - real-time collection of computer data;
  - the adequate protection of human rights and liberties.

– Each State has to adopt the necessary legislative and other measures to establish jurisdiction over the following offences, without prejudice to its domestic law:
  - when committed intentionally, the access to the whole or any part of a computer system without right;
  - when committed intentionally, the interception without right of non-public transmissions of data to, from or within a computer system;
  - when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right;
  - when committed intentionally, the serious hindering without right of the functioning of a system;
  - the production, sale, procurement for use, import, distribution or otherwise making available of a device designed or adapted for the purpose of committing any of those offences;
  - when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic;
  - when committed intentionally and without right, the causing of a loss of property to another person by any input, alteration, deletion or suppression of computer data, or any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person;
  - establish as criminal offences the aiding or abetting of any of those offences, and any attempt to commit any of those offences.

– Each of the signatories has to establish jurisdiction over any offence committed:
  - in its territory;
  - on board a ship flying the flag of that country;
  - by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

– Rules on international cooperation relating to:
  - extradition;
  - mutual assistance for purposes of investigation;
  - procedures for criminal acts related to computer systems and data;
  - collection of electronic evidence of a criminal act.

– Creation of a mutual assistance network
  - available on a 24/7 basis;
  - with a national point of contact;
  - with immediate assistance with offences.

The political will to deal with cybercrime exists at the international level. The problem is not always the absence of laws or guidelines, such as those promulgated by the Organisation for Economic Co-operation and Development (OECD) with its "OECD Guidelines for the Security of Information

Systems and Networks – Towards a Culture of Security – 2002[11]" (Figure I.7). Rather, it is the difficulty and complexity of the task, and the resources necessary to meet the objectives of the struggle to combat not only cybercrime but also organized crime, that result in the internet being exploited for malicious purposes.

Figure I.7 – OECD principles for information security (July 2002)

Awareness	All participants are responsible for the security of information systems and networks
Responsibility	All involved have a share in the security of systems and information networks
Response	Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents
Ethics	Participants should respect the legitimate interests of others
Democracy	The security of information systems and networks should be compatible with essential values of a democratic society
Risk assessment	Participants should conduct risk assessments
Security design and implementation	Participants should incorporate security as an essential element of information systems and networks
Security management	Participants should adopt a comprehensive approach to security management
Reassessment	Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures

I.2.10 Cybersecurity basics

Security solutions must contribute to satisfying basic security criteria such as availability, integrity and confidentiality (the AIC criteria). Other criteria that are often cited in this context are authentication (which makes it possible to verify the identity of an entity), non-repudiation and imputability (which make it possible to verify that actions or events have taken place) (see Figure I.8).

I.2.10.1 Availability

To ensure the availability of services, systems and data, the components of the infrastructure systems must be appropriately sized and possess the necessary redundancy; in addition, operational management of resources and services must be provided.

Availability is measured over the period of time during which the service provided is operational. The potential volume of work that can be handled during the period of availability of the service determines the capacity of the resource (a server or network, for example). The availability of a resource is closely linked to its accessibility.

I.2.10.2 Integrity

Preserving the integrity of data, processing or services means protecting them against accidental and intentional modification, tampering and destruction. This is needed to ensure they remain correct and reliable.

[11] www.oecd.org/dataoecd/16/22/15582260.pdf – See Annex F to this Guide.

To prevent tampering, a way is needed of certifying that they have not been modified during storage or transfer.

Data integrity can only be guaranteed if data are protected from active tapping techniques that can be used to modify the intercepted information. This type of protection can be provided with such security mechanisms such as

– strictly enforced access control;
– data encryption;
– protection against viruses, worms and Trojan horses.

Figure I.8 – Cybersecurity basics

The system must…	Security objectives	Security tools
... be capable of being used	• availability • sustainability • continuity • confidence	• dimensioning • redundancy • operation and back-up procedures
... operate correctly	• operating security • reliability • durability • continuity • correctness	• design • performance • ergonomics • quality of service • operational maintenance
... provide access for authorized entities (while denying unauthorized access)	• confidentiality (secrecy) • integrity (no changes)	• access control • authentication • error control • consistency check • encryption
... verify actions	• non-repudiation • authenticity (beyond doubt) • non-contestation	• certification • logging, traceability • electronic signature • proof mechanisms

I.2.10.3 Confidentiality

Confidentiality is the safeguarding of secrecy of information, information flows, transactions, services or actions performed in cyberspace. It guarantees the protection of resources against unauthorized disclosure.

Confidentiality can be implemented by means of access control and encryption.

Encryption helps to protect the confidentiality of information during transmission or storage, by turning it into a form that is unintelligible to anyone who does not possess the means to decrypt it.

I.2.10.4 Identification and authentication

The purpose of authentication is to remove any uncertainty about the identity of a resource. It presupposes that all entities (hardware, software and persons) are correctly identified and that certain characteristics can serve as proof of identification for them. In particular, logic-based access control systems to IT resources require that the identification and authentication of entities be managed.

Identification and authentication procedures are implemented in order to help achieve the following:

- data confidentiality and integrity (access to resources is restricted to identified authorized users, and resources are protected against change by all except those who are so authorized);
- non-repudiation and imputability (actions can be traced to an identified and authenticated entity), traceability of messages and transactions (transmissions can be traced to an identified and authenticated entity), proof of destination (the message can be proven to be addressed to an identified and authenticated entity).

I.2.10.5 Non-repudiation

In some circumstances, it is necessary to verify that an event or transaction has taken place. Non-repudiation is associated with the concepts of accountability, imputability, traceability and, in some cases, auditability.

Establishing responsibility presupposes the existence of mechanisms for authenticating individuals and attributing their actions. The possibility of recording information to make it possible to trace the performance of an action becomes important when there is a need to reconstitute the sequence of events, particularly when performing computer investigations to find a system address used to send data, for example. The information needed to conduct subsequent analysis, for system auditing purposes, needs to be saved (information logging). This is called system auditability.

I.2.10.6 Physical security

The spaces within which workstations, servers, IT areas and services (air-conditioning, electrical supply panels, etc.) are located need to be physically protected against unauthorized access and accidents (fire, water damage, etc.). Physical security is the most fundamental and ubiquitous type of IT system control.

I.2.10.7 Security solutions

In view of the daily reality of security-related problems for most infrastructures, the proliferation of proposed solutions, and a flourishing security market, a number of questions are in order:

- Are the proposed security solutions adapted to requirements?
- Are they correctly installed and managed?
- Can they be used in, or adapted to, a dynamically evolving environment?
- Can they moderate the inordinate concentration of power in the position of system administrator?
- How can they be used to address security problems which have their origins in negligence, human error, design flaws, installation problems or mismanagement of technology and security solutions?
- etc.

PART II

CONTROLLING CYBERCRIME

Section II.1 – Cybercrime

II.1.1 Computer-related crime and cybercrime

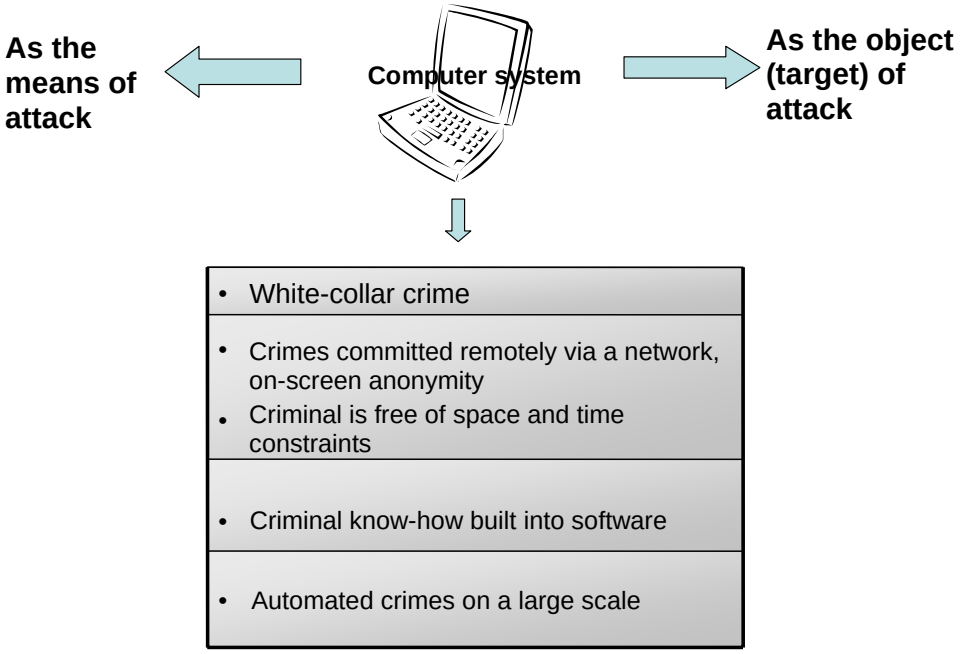
The vulnerabilities of digital technologies and inadequate control of them combine to create an environment of insecurity. Criminals naturally take advantage of this state of affairs. Every technology can potentially be exploited by criminals for illegal purposes; the internet is no exception, as the criminal presence in cyberspace amply demonstrates.

In 1983, OECD defined computer-related crime as any illegal, unethical or unauthorized behaviour involving the transmission or automatic processing of data.

A computer-related crime is one where the computer system is the object of the crime, the means of committing the crime, or both; it is a crime connected with digital technology, a subset of white-collar crime. Cybercrime is a form of computer-related crime committed using internet technology; it covers all crimes committed in cyberspace.

In the virtual world, crime can be automated, creating the potential for a large-scale cyberepidemic, capable of being launched remotely via a network (freeing the criminal from constraints of time and space), with the possibility of delayed action (Figure II.1).

Figure II.1 – The nature of computer-related crime



Internet technology facilitates a wide range of infractions: theft, information sabotage, copyright infractions, breach of professional trust, digital privacy, intellectual property, distribution of illegal content, anti-competitive attacks, industrial espionage, trademark infringements, disinformation, denial of service, various forms of fraud, etc.

Notable events that contributed to the growing awareness of the threat of cybercrime – in addition to the Y2K bug, which drew attention to the vulnerability of software and society's dependence on

computers – include denial-of-service attacks such as those launched against Yahoo (on 10 February 2000) and the attack by the notorious "I love you" virus (4 May 2000). Since then, media coverage of the virus attacks (such as the "Code red" virus in July 2001 or "Nimda" in September 2001) and denial-of-service attacks (such as that launched against the DNS network on 21 October 2002), among many other examples, has increased the general public's awareness of the reality of threats that operate through the internet. The news media continue to devote considerable space to covering problems related to computers.

II.1.2 Factors that make the internet attractive for criminal elements

II.1.2.1 Virtualization and the virtual world

The uncoupling of transactions from physical media (virtualization), communication tools involving encryption, steganography and anonymity: these are factors which criminals in different countries exploit in order to collaborate while dispensing with physical meetings, operating in a flexible, secure manner and with complete impunity. They can form teams, plan crimes and carry them out, whether in the traditional manner or using new technologies. The global reach of the internet allows criminals to act globally, on a large scale and very rapidly.

These powerful possibilities created by the digital world and telecommunication come on top of the inherent problems associated with the design, implementation, management and control of information technology, with its crashes, malfunctions, errors and human mistakes, and even natural disasters, as well as the interdependence of infrastructures, all of which imply by definition a certain level of insecurity in digital infrastructures.

The potential for malicious exploitation of vulnerabilities is thus very broad, translating in practice into:

> identity theft, spoofs, unauthorized access, fraudulent use of resources, infection, sabotage, destruction, tampering, breach of confidentiality, data theft, blackmail, extortion, protection rackets, denial of service, etc.

This clearly shows the inadequate control of computer-related risks of criminal origin to which organizations are exposed, and the limits of current security strategies.

Cyberspace, which allows users to operate remotely via a network, hidden behind a screen, creates ideal conditions for criminal activity. Indeed, some individuals may in fact stray across the boundary into criminal activity without ever being fully conscious of the criminal nature of their acts.

II.1.2.2 Networking of resources

The wide-scale networking of computer and information resources makes them attractive targets for economic crime using new technologies. The various forms of computer attack that exist have in common the relatively low level of risk for the criminal, set against a potential for harm and damage that greatly exceeds the resources necessary to launch an attack. Electronic identity theft, easy anonymity and the possibilities for taking control of computers make it easy to carry out illegal acts without exposing oneself to any great risk.

II.1.2.3 Proliferation of hacks and vulnerabilities

The widespread availability of "hacks", which exploit system vulnerabilities, and libraries of attacks and software that build on criminal know-how, make the task of carrying out a computer attack easier. This, combined with the possibility of virtual action, encourages computer experts with criminal tendencies and criminals with computer skills to turn their expertise to a malicious use. In some cases, cyberspace eases the transition to a criminal act almost unawares.

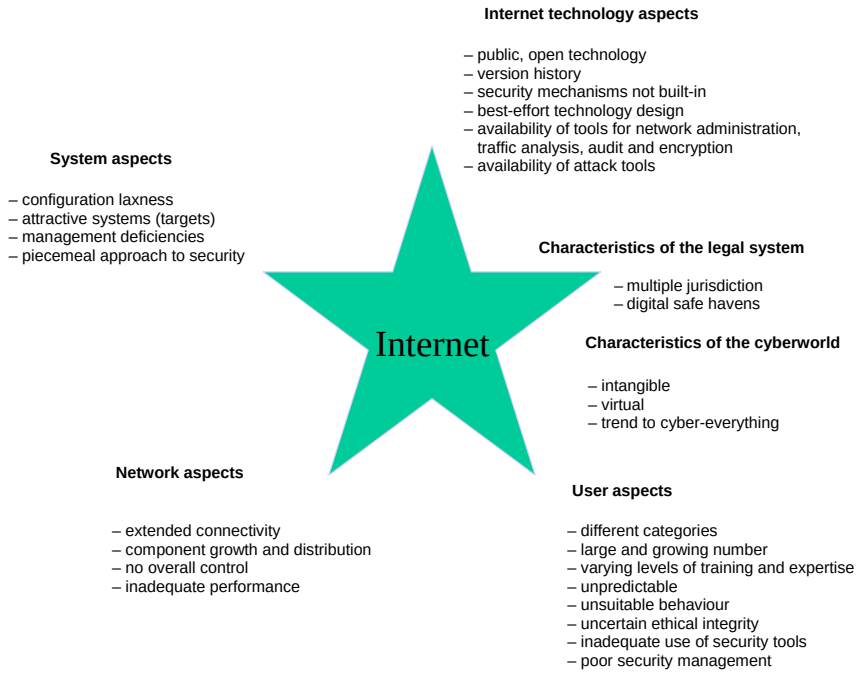
II.1.2.4 Faults and vulnerabilities

Criminals exploit organizational and technical faults and vulnerabilities of the internet, the absence of a harmonized legal framework between countries, and the lack of effective coordination between

national law-enforcement agencies. This may involve traditional forms of criminality (traditional crimes committed with new technologies: money-laundering, blackmail, extortion, etc.) or new types of crime based on digital technologies: system intrusion, theft of processor time, theft of source codes, databases, etc. The environment, in all of those cases, is exceptionally conducive: minimum risks, wide coverage, lucrative profits.

Figure II.2 summarizes the sources of the vulnerabilities of the internet infrastructure.

Figure II.2 – Principal characteristics of the internet exploited for criminal purposes



II.1.2.5 Unmasking cybercriminals

Computer-related crime is sophisticated, and is usually committed across national borders, frequently with a time delay. The traces it leaves in the systems are intangible and difficult to gather and save. They take the form of digital information stored on all sorts of media: working memory, storage peripherals, hard discs, external discs and USB sticks, electronic components, etc. The problem is how to capture the wide variety of evidence turned up in a digital search. The following questions illustrate the extent to which the concept of digital evidence remains elusive:

- How to identify the relevant data?
- How to trace them?
- How to store them?
- What are the judicial rules of evidence?
- How to recover files that have been deleted?
- How to prove the origin of a message?

- How to establish the identity of a person on the basis of only a digital trace, in view of the difficulties of reliably linking digital information with its physical author (virtualization) and the proliferation of identity theft?
- How to establish the conclusiveness of digital evidence in establishing the truth before a court (concept of digital evidence), knowing that the storage media from which the evidence has been recovered are not infallible (date-time information being treated differently from one computer system to another, and subject to tampering)?
- etc.

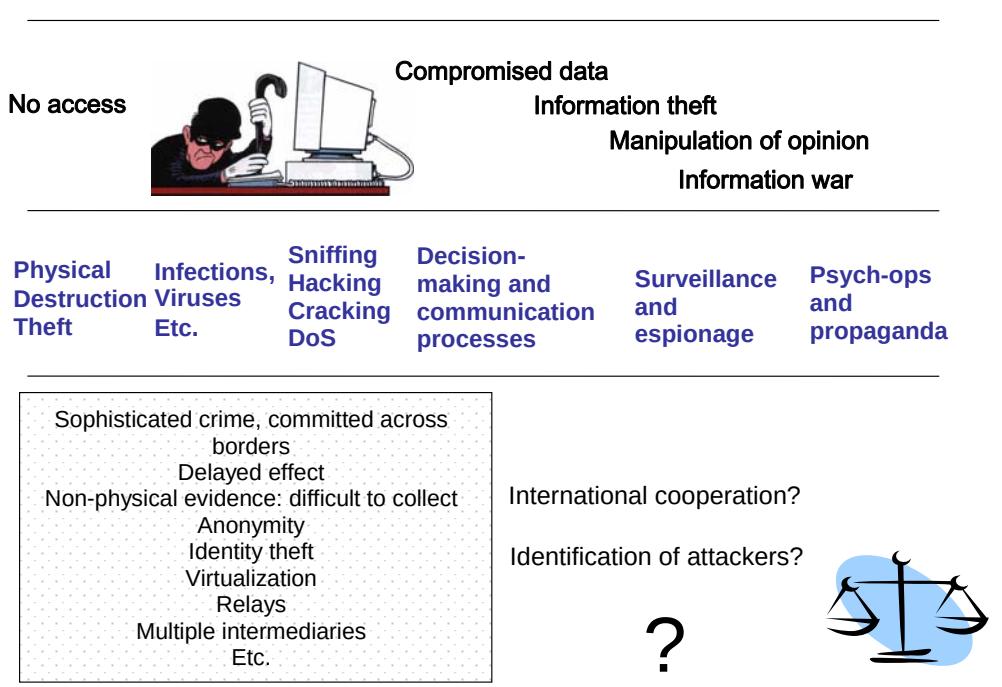
Digital evidence is even more difficult to obtain when it is scattered across systems located in different countries. In such cases, success depends entirely on the effectiveness of international cooperation between legal authorities and the speed with which action is taken. Effective use of such evidence to identify individuals depends on the speed with which requests are treated: if treatment is slow, identification is next to impossible.

Figure II.3 shows the different types of problems caused by malicious acts such as physical destruction or theft of equipment, preventing access to systems and data, infection of resources, compromised decision-making or communication processes through denial-of-service attacks (or as the result of espionage or intrusion into the systems), information theft and tampering (manipulation of opinion, info-war). It also outlines the main characteristics of cybercrime that make it difficulty to identify the criminals.

Furthermore, in most countries there is a significant mismatch between the skills of the criminals who commit high-technology crimes and the resources available to the law-enforcement and justice authorities to prosecute them. The use of computer technologies by those authorities, whether at the national or international level, remains weak and varies greatly from one country to another.

In most cases, the police and judicial authorities rely on conventional investigation methods used for ordinary crime to prosecute cybercriminals so as to identify and arrest them.

Figure II.3 – Difficulties in identifying an attacker



II.1.2.6 Aterritoriality, digital safe havens

Criminals take advantage of the aterritorial nature of the internet and the lack, in some countries, of legislation outlawing computer-related crime, as well as the multitude of jurisdictions covering the internet.

In a similar manner to tax havens, digital safe havens allow criminals to host servers, distribute illegal content or perform illegal actions without fear of retribution. Installing such servers on the territory of weak countries creates a haven for cross-border operations.

The lack of international regulation and control and the ineffective nature of international cooperation in legal investigations and prosecutions allows the internet to act as a protective buffer for criminals.

Currently, no effective approach, legal or technical, has been adopted for dealing with all the different types of crime observed on the internet, such as:

- the highly organized parallel industry of large-scale software, film and music piracy, which has taken on unprecedented dimensions in cyberspace;
- copyright violations, betrayal of professional trust, violation of digital privacy and intellectual property;
- property offences, theft, damage to or destruction of property, and interference in someone else's property (concept of electronic trespassing);
- distribution of legal content;
- attacks against competitors, industrial espionage, trademark infringements, disinformation, and denial-of-service attacks against competitors.

II.1.3 Traditional crime and cybercrime

Cybercrime is the natural extension of ordinary criminal activity. Today, criminal acts are committed across cyberspace, using non-conventional means in a manner that is complementary to ordinary crime.

The internet not only provides ideal conditions for new illegal projects and activities, but also makes possible variations on fraud and other crimes by means of computer.

The internet makes it easy to find and exploit new means of making money. This empowering feature is, naturally, not lost on the criminal world. By embracing IT, criminals hope to increase their winnings while minimizing their exposure to risk.

II.1.4 Cybercrime, economic crime and money-laundering

Economic crime via the internet is not limited to organized crime. Modern information and communication technologies allow isolated individuals to engage in economic crime, either working alone or in concert with groups of various sizes formed for the purpose.

Criminals can organize themselves around the exchange of information, thanks to the use of IT. Networks can bring together individuals and expertise to organize a virtual criminal gang.

Given the high degree of economic expertise and skills that economic crime requires, it is an obvious candidate for "improvement" by means of modern IT.

The internet contributes to the acquisition of information and the knowledge of markets, laws, technology, etc. that are needed to commit economic crimes. It can also be used to prospect for victims.

Economic crime is influenced by new technologies, which become part of the criminals' repertoire and place information at the heart of their strategies and decision-making processes.

New technologies can facilitate theft of all kinds, tampering, information sabotage and fraud. Blackmail, extortion, protection rackets and ransom demands have all made move leap to the internet.

Information resources in effect become potential hostages of the cybercriminals. Blackmailers have shifted their operations to cyberspace, and anyone may suddenly find themselves the victim of attempted blackmail, disinformation or propaganda attempts. Furthermore, the explosion in identity theft since 2003 shows that the benefits of anonymity that the internet affords, and the use of false identities to avoid prosecution or criminal and terrorist responsibility, have not been lost on criminals. Identity theft, readily performed via the internet, is a factor in illicit activities.

Like all criminals who exploit the existing technical infrastructures, money-launderers increasingly use the internet in order to take money that is generated by criminal activities such as drug trafficking, arms smuggling, corruption, prostitution, child abuse, tax fraud, etc. and move it into the domain of legality.

Although it is greatly under-reported and frequently invisible, money-laundering via the internet is increasingly popular. The internet is an ideal vehicle, thanks to its virtual nature (anonymity, cyberspace, speed of transfer) and its freedom of territorial constraints (cross-border nature, conflicting competence and jurisdictions), which money-laundering agents have learned to exploit. The internet makes it possible to channel monies of criminal origin into legitimate economic circuits using money transfers, investment and capitalization.

Online investment, gambling and commerce, such as the sale of imaginary goods and services for real money, make it possible to generate seemingly legitimate revenues that are difficult to monitor and almost impossible to prosecute. E-banking, real-estate transactions via the net, the use of virtual front companies and electronic cash can all be used to launder the proceeds of crime. Ordinary users may unknowingly support money-laundering when they use certain virtual services. Commercial organizations may also unwittingly become involved, with all the – potentially disastrous– implications that entails, in legal and commercial terms. This is a major source of risk for companies.

Currently there are few effective means of controlling the phenomenon of IT-enabled money-laundering.

II.1.5 Cybercrime – an extension of ordinary crime

Cybercrime most commonly takes the form of ordinary crime, largely invisible, yet highly potent on account of the networking of resources and individuals. Not only companies, but also their IT and information assets, can become attractive targets for criminal organizations in search of profit. This is a strategic threat, as the money resides in information systems, in corporations, in pension funds etc., and not merely in banks.

By opening the corporate gates to the internet, via web servers, portals and e-mail, companies expose themselves to the risk of criminal attention and give criminals a potential foothold. While the internet is a powerful communication tool, it is also a chaotic, complex, dynamic and hostile environment which can be used to undermine the organization and serve as a vehicle for crime. The internet should be treated with caution, as a high-crime zone. Given the importance that organizations attach to their internet presence, they are, in all likelihood, contributing to the expansion of criminality to the internet.

Today, national security faces challenges in the form of IT-related criminal threats. Internet technologies are at the heart of the notion of infowar, whose objectives are primarily economic; it can have a huge impact on the conduct of business operations. The internet not only makes it possible to manipulate information; it is also an ideal rumour-mill that can fuel campaigns intended to spread disinformation or uncertainty. It also facilitates espionage and other intelligence-gathering activities, given the ease with which information travelling across the internet can be intercepted.

II.1.6 Cybercrime and terrorism

Cybercrime can take on a terrorist dimension when the systems targeted are part of a critical infrastructure. The vulnerability of the essential infrastructures of a country (energy, water, transportation, food logistics, telecommunication, banking and finance, medical services, government functions, etc.) is increased as the use of internet technologies takes root.

Particular emphasis needs to be placed on the electrical power generation and distribution systems, which are essential to the operation of most infrastructures. One of the key objectives of cyberterrorists appears to be the control of critical infrastructure elements, as shown by the increase in the number of scans (probing for vulnerabilities that can be used to penetrate the system at a future date) targeting the computers of infrastructure operators.

There is no agreed definition of what constitutes cyberterrorism at the present time. The simplest would no doubt be to consider it as terrorism applied to cyberspace. In its turn, terrorism is generally understood to mean the systematic use of violence to achieve political aims.

It is entirely legitimate to ask whether the breakdown of the internet, or a portion of it, as a result of malicious acts, might not sow terror within the community of web users, some groups of economic players, and the general public.

Or, in the main, we may be dealing with instances of economic terrorism, aimed at damaging organizations that use the internet for their activities.

The term cyberterrorism, which has come into vogue since the September 11 attacks, should be used with discretion. It should not be forgotten that the very first widely publicized distributed denial-of-service (DDOS) attacks, on 10 May 2000, were the work of a fifteen year-old who went by the nick-name of "Mafia Boy". The youth was identified and apprehended several months later. Although the reasons for his actions remain unknown, it is highly unlikely that they were political in nature.

Had the same attack been carried out after the events of September 11, it might have been immediately classified as cyberterrorism.

In the absence of specific information, such as a note from the attackers or their identity, it is difficult to attribute an attack to cyberterrorism.

The term cyberterrorism covers a fairly vague catalogue of new threats, and it is difficult to speculate what the motivation or aims of an unknown attacker or group of attackers might be. When the only thing known is the target of the attack, it is very dubious to extrapolate to the thinking that may have motivated a hacker, terrorist, mercenary, activist, ordinary criminal or prankster.

The type of computer-related attack cannot be used to state the motivation or aims of the attackers with any certainty. This is one of the difficulties in the fight against computer-related crime, as additional information is needed to determine what the criminal intention was.

Whether it is through a process of economic destabilization, by threatening critical infrastructures, spreading ideology or manipulating information, cyberterrorism constitutes a new threat that must be taken very seriously. Apart from its threat to the information systems and the cyberworld, symbolized by the internet, it can endanger human life by creating an indirect menace to life and limb.

II.1.7 Hackers

Understanding a hacker's motivation and level of technical skill can help to assess how serious an attack is, and assist in devising a counter-strategy. In order to secure an information system, one needs to know against whom it needs to be protected. At the present time there are two principal groups of hackers: the professionals who make money from their work, and the amateurs, who tend to be persons with a pronounced need for recognition (Figure II.4).

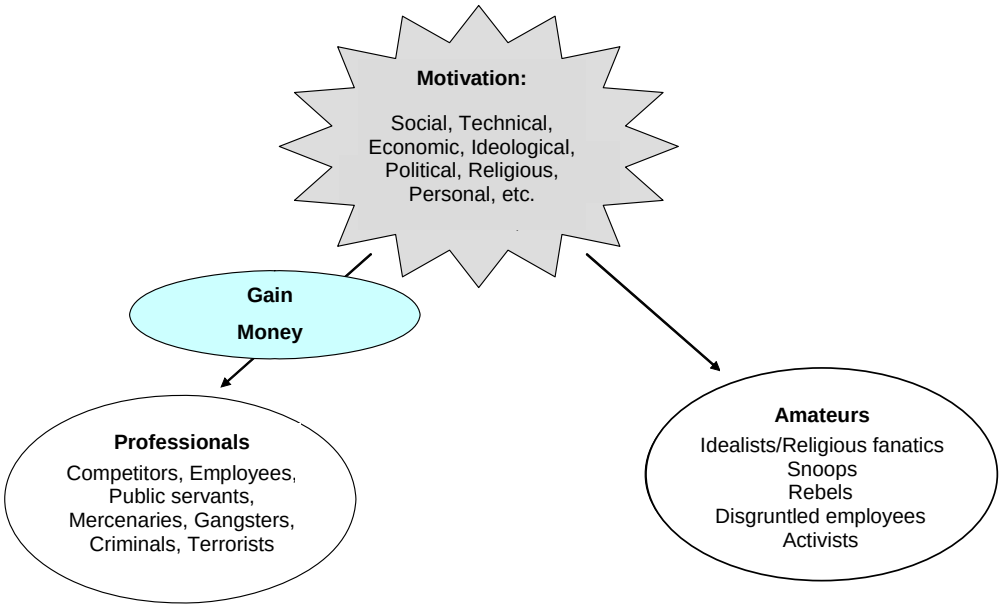
Professional hackers generally fall into one or more of these categories:

- direct competitors of the organization targeted;
- civil servants;
- mercenaries (hackers in the pay of an organization in the private or the public sector);
- other criminal elements.

Amateur hackers may include:

- technicians, the descendants of the original "hackers", computer buffs who were motivated primarily by the desire to display their mastery of the technologies involved;
- snoops;
- pranksters, also called "script-kiddies" or "kidiots", who frequently enjoy a great amount of publicity when they are caught, although the fact that they tend to be the ones most frequently unmasked should not lead us to imagine that they are the only representatives of the category of hackers;
- psychologically disturbed individuals;
- activists working for an ideological or religious cause (frequently more professional than amateur).

Figure II.4 – Two main groups of hacker



The underlying motivation of these individuals may have to do with social, technical, political, financial or government-related factors.

Social factors are typically the need for peer recognition, often linked to membership of a gang or group. These hackers want to demonstrate their importance in the group, by living up to the group's values. Their acts are analogous to those of urban graffiti taggers, and are based on a very simplistic view of a social hierarchy. This is frequently the case among pranksters, who engage in hacking because it gives them a feeling of superiority and control over institutions that they perceive to be domineering in ordinary life.

Technical motivation is rare, and has the primary objective of exploring the limits of a technology, demonstrating those limits and vulnerabilities, and understanding the strengths.

Political motivation focuses on events that will attract media interest so as to draw attention to a serious problem, in order to build public awareness leading to its resolution. The dividing line between this and terrorism may be a fine one, at least in terms of the theory. It is not uncommon for a socially-motivated individual to hide behind a political goal.

Financial motivation can be a strong factor, and underlies a large number of illegal actions. The lure of easy money draws white-collar criminals (fraudsters, embezzlers, criminal competitors, etc.) to ply their trade on the internet.

Finally, the last group in our list involves governments. This form of hacking includes infowar and espionage, and is perpetrated by government services working for the State.

Malefactors of all kinds have rapidly adapted to the computer age, adding hacking to the tools of their trade. They bring a frightening resourcefulness to bear on new ways of misusing this technology.

II.1.8 Nuisances and malware

II.1.8.1 Spam

Spam is the bulk sending of unsolicited e-mail for commercial or publicity purposes, the object being to entice web users to order a product or service.

Spam remains a potent nuisance, despite the enormous technical and financial resources that service providers have committed to the search for a way of blocking it, despite the announced intention of public authorities to combat it, and despite the conviction of particularly blatant spammers in the past. In September 2003, spam made up 54 per cent of all e-mail traffic. In 2005, the number of spam messages sent in the United States exceeded 12 billion, i.e. 38.7 per cent of all traffic, according to IDC.

At its worst, spam comes to resemble an e-mail bombing attack, with overloaded mail servers, full user mailboxes, and the attendant inconveniences. Users may fall victim through the practice known as list linking, whereby their address is added to spammers' lists without their consent. The only alternative to attempting to unsubscribe from the lists, which can be an arduous task, is to change one's e-mail address. While this measure is effective, it is also highly disruptive, as it requires the user to notify all possible correspondents of the change.

The exorbitant number of unsolicited, inappropriate, and sometimes shocking messages may be perceived as an intrusion into the user's private sphere, like junk mail. In addition, however, spam is also increasingly being used as a vehicle for malicious programs (malware), which is an exponential increase in its harmfulness.

II.1.8.2 Malware

The principal monitors of IT security (including the Computer Emergency Response Team (CERT)[12], the United States Federal Bureau of Investigation (FBI), and the French *Clusif*) have observed in their annual reports on cybercrime that the number of malicious and nuisance programs running on computers without their owners' knowledge is increasing.

This includes the following kinds of software:

- downloaders, which are used to download and install data and programs remotely;
- keyloggers, which monitor what keystrokes the user enters at the computer; there are also hardware keyloggers, invisible at the software level, which record such data;
- zombies, or "bots" (short for "robots"), are programs that allow the system to be controlled remotely for the purpose of building a hidden army of computers. Every day, 25-50 new bots are discovered. They are used for spamming purposes, phishing attacks, or for the distribution of adware. In October 2005, the Netherlands police arrested three men suspected of running a network of 100 000 bot computers to launch denial-of-service attacks and target the PayPal and eBay accounts of their victims[13];
- adware (advertising software), used to customize business transactions;
- spyware, which, as the name indicates, clandestinely records information. According to the software publisher Webroot, there are over 100 000 different types of spyware on the internet, and over 300 000 sites that host them. A typical PC with an internet connection has an average of 28 spyware programs installed, unbeknownst to the user. More than 80 per cent of company computers have one or more spyware programs. These programs are involved in 70 per cent of all attacks.

---

12 <www.cert.org> – See statistical information for 1998-2005, at <www.cert.org/stats/cert_stats.html>

13 Source: Clusif Report, *Panorama de la cybercriminalité, 2005*: www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k5-fr.pdf

In addition to these forms of malware, there are viruses and related products (worms, Trojan horses, logic bombs).

A virus consists of malicious code that is installed in a system without the user's knowledge and has the capability of replicating itself (in the case of polymorphous viruses, the replication is not exact, but rather a mutation). It attacks the host environment and contaminates others with which it comes into contact. Viruses can be distinguished on the basis of their signature, behaviour, how they replicate and spread, the types of malfunctions they induce, etc.

The purpose of a computer virus, like that of its biological analogue, is to reproduce and propagate itself. It does so by moving from computer to computer, attaching copies of itself to programs and, most commonly, e-mail. This usually occurs in connection with some user action. The damage that a virus causes to the integrity of the contaminated information resources may range from mild annoyances to major destruction, with an impact on system availability and confidentiality.

The generic term "virus" is used to designate any harmful computer program (causing infection, destruction, misappropriation of resources, etc.) capable of reproducing and propagating itself.

In 2005, an estimated 50 000 new virus were in circulation[14]. For example, the virus HTML_NETSKY.P, as described by the World Virus Tracking Centre, has infected 855 244 machines around the world since April 2004. The cost, for companies that were infected, was in the order of USD 42 million, according to the Computer Security Institute. The site <F-secure.com> estimates at four thousand the number of viruses in circulation every day.

Worms are bits of computer code that also travel through the net, often on their own without any action by the user. Typically, they are designed to tie up system resources (memory and bandwidth), thereby undermining system availability, or enabling remote control of the infected system.

The malware known as Trojan horses is often hidden inside ordinary programs or help files and then infiltrated into systems, where they attempt to take control in order to steal processor time, tamper with or destroy data or programs, cause crashes, conduct snooping or other forms of malicious activity, or merely lie dormant pending a future attack.

Logic bombs are viruses that are activated on a particular event (such as birthdays) to attack the host system.

None of these should be confused with computer "bugs", which are programming errors, or, more generally, design flaws that show up as functional problems.

The normal way for viruses to propagate and execute is to await inadvertent activation by the user, for example by starting an infected program. In the past, most viruses have been propagated via e-mail attachments, and are commonly activated by clicking on the file icon.

Many malicious programs are disguised as helpful add-ons for navigation, connection, customization of services etc., when in fact they are designed to carry out surveillance (information theft, password theft, traffic surveillance), use computer resources or perpetrate attacks. They are also used to disseminate and control tools used for distributed denial-of-service attacks. Thousands of these programs are in circulation, the objective being financial gain.

Denial-of-service (DOS) and distributed denial-of-service (DDOS) attacks are aimed at crippling system resources. Typically they operate by overloading a server with requests for the ordinary services it is designed to provide routinely, thus preventing it from delivering the service to regular users (whence the term denial-of-service). Because these requests resemble ordinary requests, such an attack is very difficult to counter (it is the sheer volume of requests that overwhelms the system). For added effectiveness, they can be launched simultaneously from many different points or systems; this is what constitutes a distributed DOS attack.

The means by which malware of various sorts is propagated include free or demonstration software and pornographic websites or games, e-mail, but also spam and discussion groups.

---

14 Source: IPA/ISEC Computer virus incident report.

Whatever the means used to infiltrate malware – it may even include, for example in the case of adware (but never spyware), a step of explicit or tacit approval by the user – once installed, they are turned to illicit use. Most commonly, they are executed without the consent of the user. Clandestinely, they collect and transmit data (for example, on surfing habits, of interest for targeted advertising). They can act as drones for illegal activities like spam and phishing attacks, effectively working for the controller's financial gain. Detecting and uninstalling such software is not always straightforward. Frequently, users lack the skills and tools necessary to control these risks.

The term phishing – a metaphor for angling, where the fisherman reels in his catch after attracting it with bait and hooking it – refers to an attack using mail programs to trick or coax web users into revealing sensitive information that can be then exploited for criminal purposes (e.g. fraud or embezzlement). The *Journal du net*[15] of 26 January 2005 recorded over five thousand phishing sites that were active on the web in just one month (September 2005), targeting 110 different brands.

In general, phishing attacks are conducted using e-mail messages that are forged to appear as though they come from a genuine institution with which the user may have dealings (e.g. the post office, a bank, a dealer, online auction site), but attackers may also use a telephone call, instant messaging (IM) or cellphone text messages, or even approach the victim in person.

II.1.8.3 Trends

Today, viruses no longer have as their principal objective gratuitous large-scale data destruction. They tend to be designed for a much more intelligent purpose: making money. Thanks to this new pragmatic focus and their inherent characteristics, they can be used for fraud. Thus, viruses have become highly lucrative tools for organized criminals engaged in financial crime.

For spam and related nuisances, the French *Club de la sécurité des systèmes d'information français* (Clusif)[16] reported that AOL filtered 500 billion spam messages in 2003, and the most prolific spammer in the world, as revealed in December 2003 by the anti-spam organization Spamhaus[17], is thought to have despatched 70 million e-mail messages in a single day!

Clusif also reported how, in May 2003, the so-called Buffalo spammer was sentenced in the United States to pay USD 16.4 million to the internet service provider Earthlink, for sending 820 million unsolicited messages. According to Ferris Research, in 2003 spam cost the business world USD 2.5 billion in Europe and USD 8.9 billion in the USA. When added to the USD 500 million that service providers have invested to block spam, the full magnitude of this problem of e-mail abuse becomes clear. It is obviously an issue that can no longer be ignored.

In addition to the direct costs resulting from fraud, one has to consider the costs related to service interruption, leading to disruption of operations, loss of sales, collateral damage, loss of image and reputation, and the cost of restoring the systems to an operational state. These represent a considerable cost for the organizations that are the targets of computer crime.

Observations show that the number of attacks is growing all the time and computer viruses have become veritable pandemics. Identity-theft operations are growing and have taken on an impressive level of sophistication, as have fraud and the various forms of swindles and blackmail that are the daily reality of cyberspace. They have become ubiquitous, affecting everyone and all sectors of activity, across barriers of geography and time.

There is not a system, hardware or software platform, or operating system that is immune, including mobile systems (laptops and mobile telephones).

---

15 www.journaldu net.com

16 www.clusif.asso.fr

17 www.spamhaus.org

II.1.9 Principal forms of internet crime

II.1.9.1 Swindles, espionage and intelligence activities, rackets and blackmail

The various common forms of organized crime (protection rackets, human trafficking, confidence schemes, theft, etc.) can benefit from using new information technologies, in particular the internet. By making it easy to communicate, the internet assists those engaged in any form of smuggling (whether it be of arms or human beings), and swindles (attacks against property, computer systems and infrastructure, data theft, copyright infringements, etc.).

Criminals use the internet in various ways. Some use another person's identity in order to make purchases on the victim's account. This is frequently done by means of credit-card fraud, for example by creating valid card numbers that do not correspond to any real account. The information is used to purchase something online, using a "disposable" address for one-time delivery. The cost will be borne by the bank system or the merchant. Card users may also be victimized, for example when their credit-card numbers have been divulged, by a pickpocket or a dishonest merchant, to a specialized gang.

Another category of swindle involves the sale of imaginary services (university diplomas, diplomatic passports for non-existent countries, auctions of non-existent products, etc.).

Espionage and intelligence work are also facilitated by the web, which makes it easy to illegally intercept information being transferred on the internet.

It should also be noted that the systematic use of secure means of communication, such as encryption, by professional terrorists can help them to operate with greater security, by reducing the amount of information that is vulnerable to interception by law-enforcement authorities.

The internet is a powerful medium that lends itself to the dissemination of ways of committing crimes and illegal acts, encouraging potential criminals.

II.1.9.2 Crimes against persons

The internet makes it possible for clandestine virtual communities to form around practices that are subject to severe legal sanction. This may involve pornography, paedophilia or so-called snuff movies (films showing scenes of violence and torture on real-life victims that can sometimes result in their death). This type of crime is commonly linked to human trafficking, which most often involves women and children. Films and photos can be shared, with greatly reduced risk of police detection. As the servers are frequently located in countries where law enforcement is absent or ineffectual, and with the use of private internet relay chat (IRC) services for very limited periods of time, peer-to-peer (P2P) exchanges greatly increase the freedom of action of criminals.

All of these illegal activities come within the province of common law. The question may be raised as to whether their industrialized, large-scale practice, made possible by the internet and by the freedom of movement of goods and persons, has transformed them into crimes against a part of humanity.

Among the crimes against persons, other examples include infractions touching on privacy, personal image, professional confidentiality, and data privacy rights. Crimes specifically against minors include the dissemination of pornographic messages that may be seen by minors.

II.1.9.3 Piracy

The ease with which digital information can be reproduced has spawned a market for illegal copies. It accounts for many tens of billions of US dollars in losses for publishers of software, music and video films.

It has also been observed that there has been a great increase in the number of scholarly and academic works resorting to plagiarism simply by copying existing documents from the web.

There is a great variety of possible intellectual property infractions: forgery of an author's work (including software), design, model, trademark, etc.

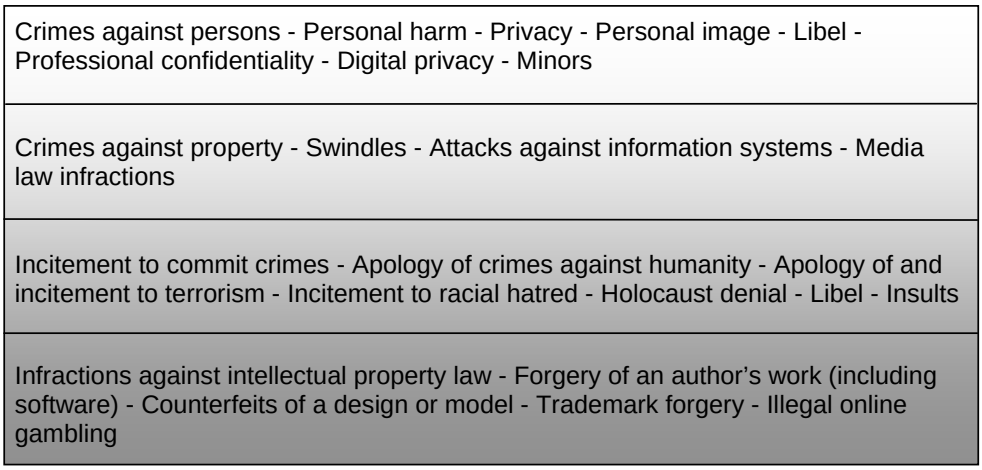
II.1.9.4 Information manipulation

Manipulation can take many forms, for example the leaking of internal documents in order to destabilize a company, sending e-mail requests for charity donations via false sites, etc.

The internet lends itself to spreading rumours and disinformation. It also facilitates infractions against the media law, criminal incitement, apology of crimes against humanity, apology of and incitement to terrorism, incitement to racial hatred, historical revisionism (negationism), character assassination, insults, etc.

Figure II.5 gives some examples of the types of crimes that are facilitated by the internet.

Figure II.5 – Examples of the types of crime facilitated by the internet



II.1.9.5 Role of public institutions

More than ever, public authorities are called upon to play their traditional role of prosecuting and preventing fraud and crime. They also need to become active in educating and building awareness among the general public. In particular, it would be useful to have reference information on protecting persons and property made available when using the internet.

It would be dangerous to let the law-enforcement authorities fall behind technologically. The cost of trying to catch up after several years of lost time goes beyond the direct financial cost, in the form of acquisition of new infrastructure; there is, above all, a social cost associated with the growing influence of organized crime structures on society, with the attendant risks of destabilization.

At the same time, an excessive police presence on the internet is not necessarily desirable, and may be in conflict with the need to protect the confidentiality of exchanges and respect individual privacy.

II.1.10 Security incidents and unreported cybercrime

It should be noted that few statistics are available on cybercrime. It is a new type of criminality, and most incidents are not reported to the police. Also, with infractions taking place across borders, whereas criminal legislation tends to be national, it is difficult to compile statistics on crimes which are defined differently from one country to another. For example, in the case of a computer system that is used to carry out a fraudulent financial transaction using a stolen user identity, it could be classified either as computer-related crime or as financial crime.

Nonetheless, the establishment in the United States, for example, of decentralized computer investigation and infrastructure threat assessment (CITA) squads, coordinated by the National Infrastructure Protection Centre (NIPC), gives some indication of the magnitude of cybercrime.

The number of security incidents reported to CERT[18] has been growing steadily since the start of the current century, as has the number of attacks reported to the legal authorities, contributing to a better understanding and accounting of computer crime. In 2003, there was a significant increase in the volume of spam, which spread beyond the internet to SMS text messages, and numerous spammers were arrested and convicted. Large-scale police operations conducted in the United States (operations E-Con in May 2003 and Cyber-Sweep in October 2003) and in Europe (Spain, Italy, France, United Kingdom, etc.) show that the authorities are reacting and adapting to the new criminal context. The arrest and conviction of several virus authors and spammers testify to the determination to deal with these new types of nuisance. However, the number of convictions remains very low given the sheer volume of spam and viruses circulating on a daily basis[19].

The rate of unreported cybercrime is difficult to estimate. It is possible that the legal authorities, the police and the general public are aware of no more than 12% of cybercrime[20]. It is difficult to obtain a realistic inventory of computer-related crime, and this is a serious obstacle to attempts to analyse the phenomenon and determine its magnitude.

The absence of official statistics is partly due to the fact that organizations:

- wish to avoid publicity about attacks;
- may be unaware that they have been the victims of cybercrime, particularly in the case of passive attacks (transparent hijacking of data, traffic, passive listening, undetected intrusion, etc.); they may also not learn of the attack until much later, when there is no longer any point in reacting;
- do not know how to deal with a crisis situation;
- lack the necessary confidence in the legal authorities and police, and in their ability to deal with this type of problem;
- prefer to handle the matter themselves.

Hacker skills, the sophistication and potency of attacks and attackers' toolkits are improving all the time, and the actual quantity of attacks continues to grow. The ever-increasing complexity resulting from this dynamic trend is difficult to handle. Without a strong political will and a sense of responsibility among all participants at the international level, as well as an effective partnership between the private and public sectors, any security measures, whether of a technical or legislative nature, will not reach beyond an inadequate and piecemeal approach to security, and thus remain ineffective in tackling computer-related crime.

II.1.11 Preparing for the cybercrime threat: a responsibility to protect

It is necessary to prepare oneself for the threat of cybercrime, which is bound to materialize sooner or later.

The protection and defence of the organization's assets needs to be organized, taking into account the risk of crime when defining the security strategy. Although it can be difficult to identify cybercriminals, and not enough is known of their methods of action and their motivation, it has been observed that criminal organizations generally behave in an opportunistic manner, and tend to be more

---

18 CERT Coordination Center, Carnegie Mellon University (http://www.cert.org)

19 The Information Technology Promotion Agency Information Security Center (IPA/ISEC) in Japan identified 85 059 known viruses in December 2003 in its Computer Virus Incident Reports, 2004: www.ipa.go.jp/security/english/virus/press/200401/virus200401-e.html

20 Vladimir Gobulev, "Computer crime typology" published on 9 January 2004 by the Computer Crime Research Center: www.crime-research.org/articles/Golubev1203/

inclined to attack the most vulnerable. Organizations can take steps to make sure they are not an attractive target for cybercrime, by ensuring that their computer infrastructure is better protected than those around it, rather than contenting themselves with remaining on the same level as their competitors, in terms of insecurity. Cybercrime risk thus becomes a lever for ensuring a high level of security.

By contrast, an organization that is viewed by criminals as a lucrative potential victim or an important symbol to be destroyed will inevitably draw targeted attacks. In the second case, the threat of destruction by terrorist acts becomes a real possibility. In such cases it is necessary to put an appropriate protection and defence strategy into place. However, conventional insurance and risk management tools are of limited effectiveness in dealing with the criminal risk, as the only way of avoiding certain risks would be to avoid connecting to the internet.

The criminal risk has a global dimension, and affects organizations at all levels (shareholders, executives, staff, production facilities, etc.). They must therefore learn to safeguard their integrity faced with the risk of crime, as they have learned to do with the risk of corruption, for example. They must remain profitable, and compensate for the opportunity cost caused by cybercrime risk and the cost of measures put in place to manage it. An economic model must be designed to find the best way of supporting the cost of protecting infrastructure and providing security for systems, networks, data and services, which is a burden on economic growth, with the help of those who have a share in the wealth created by the organization.

The realization of the fragility of the digital world and the impossibility of perfect control, not only of IT and telecommunication technologies and the infrastructure, but also of commercial security solutions, must inevitably raise the fundamental question of dependence on technologies that are beyond our control.

To what extent are we willing to be dependent on a provider, a country, or an administrator?

The first step towards controlling the cybercrime risk has to be:

- review the relationship with new technologies and providers;
- demand a security guarantee;
- institute responsibility of all participants.

Before implementing conventional security measures based on a prevention-protection-defence approach, we must first seek to protect the organization's sensitive and critical resources by reviewing their relationship to new technologies.

We must demand:

- high-quality products providing a manageable and verifiable level of security;
- that security be transparent, rather than hidden, as in the past;
- that security be the responsibility not only of users but also technical stakeholders (legal responsibility of professionals: software designers, access providers, etc.);
- that a minimum level of security be built into technology solutions (safe products).

Looking beyond the concerns of the organization, and faced with synergies and convergence in organized crime, economic crime and cybercrime, a comprehensive, multilateral and international response is needed to strengthen economic players' confidence in information technology and reduce the opportunities for crime.

This response must meet the imperatives of national security and security of organizations and individuals. It must help keep cybercrime to an acceptable level, strengthen confidence in the digital world and minimize the risk of corruption and the threat to the public authorities.

Section II.2 – Cyberattacks

II.2.1 Types of cyberattack

There are various ways of exploiting the possibilities offered by internet technologies. More often than not, they are based on the appropriation of the connection parameters or passwords of legitimate users, on deception and on exploiting the flaws and vulnerabilities of the technologies.

II.2.2 Theft of users' passwords to penetrate systems

The main methods used to obtain the connection parameters of legitimate users to gain access to systems are:

- Guessing: The password is so obvious (name of user, spouse or child, birthday, etc.) that the account is essentially unprotected.
- Deception (social engineering): The attacker poses as an administrator and asks for the password, under some technical pretext. In a surprisingly large number of cases, users will reveal their data.
- Listening to traffic: The attacker intercepts or listens to unencrypted data transmitted over the network through communication protocols (sniffing, monitoring).
- Software: A "Trojan horse" is infiltrated into a user's workstation, where it clandestinely records the parameters used to connect to remote systems.
- Accessing the password storage file.
- Cracking passwords that are sent in encrypted form.
- Spying on users by activating their multimedia peripherals to record their connection parameters.

Once in possession of the access key necessary to get into the systems (the combination of username and password), it is easy to penetrate the systems and carry out all sorts of read and write operations. The challenge for the hacker is to avoid being detected and to leave no trace of his presence in the systems accessed.

II.2.3 Denial-of-service attacks

A denial-of-service attack is typically carried out by overloading system capacity. Targeted systems, inundated with far more requests than they are equipped to cope with, crash and become unavailable. These attacks can be perpetrated by taking advantage of flaws in the operating system and exploiting certain system features, for example, buffer management (buffer overflow attack), causing serious malfunctioning which can lead to system shutdown.

E-mail bombing, which involves flooding a user's inbox with messages, is one form of a denial-of-service attack.

II.2.4 Defacement attacks

A defacement attack is carried out by replacing the victim's web page with another, where the content of the new page (e.g. pornographic, political) will depend on the hacker's motives. One variation on this type of attack involves redirecting users to a decoy website that looks exactly the same as the one they were accessing, where they are asked to disclose their credit card information, for example. This is done in phishing attacks, for example.

The content of websites can also be defaced for purposes of disinformation (to influence events, sow uncertainty, manipulate public opinion, etc.). These are semantic attacks, which subvert the meaning of the information content, and fall into the category of infowar.

II.2.5 Spoofing attacks

All TCP/IP (transmission control protocol/internet protocol) protocols can be corrupted and used to breach system security. Protocols and mechanisms that transport data through a network are equally at risk. Thus, it is possible to hijack a TCP session during a client-server working session.

TCP functions by establishing a logical connection between two correspondents and supporting the exchange of application data between the two. To connect distributed applications, TCP uses port numbers, the logical identifiers of applications. Some are fixed, reserved for particular programs, and well-known by the users; others are allocated dynamically during the connection, according to a specific algorithm. A TCP port number attack involves guessing or predicting the next port numbers to be allocated for data exchange in order to use them in the place of the legitimate user, effectively hijacking them. This makes it possible to pass through firewalls and establish a "secure" connection between two entities (the hacker and the target). Meanwhile, the legitimate remote user's access to the facility is of course blocked, but it is simple enough just to send him a message saying that the requested system is inactive.

User datagram protocol (UDP) is a level 4 (transport), connectionless protocol. It is an alternative to using TCP for the rapid transfer of a small volume of data. UDP communications are not subject to any control mechanisms, so there are no checks for identification, flow or error. As a result, anyone can use the IP address of an authorized system user in order to penetrate it. UDP session theft can take place without alerting the application servers.

Since the functioning of the various protocols is public information, it is relatively easy to misuse them, for example to generate false packets in order to overwhelm a network, in a denial-of-service attack. This illustrates the need for security in relation to the availability of networks and services.

Hackers exploit protocols and their limitations to:

- paralyse networks;
- redirect IP packets to a false destination (their own, for example);
- overload systems by deluging them with junk messages;
- prevent a sender from transmitting data;
- take control of the flow of packet transmission, impeding the circulation of network traffic and degrading its performance (reliability, dependability, etc.).

Generally, routing attacks involve confusing routers, gateways and addressees by providing them with false addressing information so that data can be misdirected.

By using certain optional IP features which serve to define the route, in other words, to specify the addresses of the intermediary systems through which the packet must pass, and by falsifying these addresses, attackers can easily redirect packets towards a destination of their choice.

Attackers know how to exploit not only operational features of communications protocols, but also the characteristics of the various operating systems and the ways they work. Thus, by overloading certain buffers (buffer overflow attack), it is possible to provoke a serious malfunction or system crash. The targets of this type of attack are, of course, those systems that provide an important service, either in data transfer (for example, routers) or in the management of names and addresses, for example nameservers. Most attacks on websites aim to shut them down by exploiting flaws in the operating system.

II.2.6 Attacks against critical infrastructure

The vulnerability of the essential infrastructures of a society (power supply, water, transportation, food logistics, telecommunication, banking and finance, medical services, government functions, etc.) is

increased as the use of internet technologies takes root and they become accessible via the "network of networks".

Particular emphasis needs to be placed on the vulnerability of electrical power generation and distribution systems, which are essential to the operation of most of the national infrastructure, and hence of vital importance. The complexity and distributed nature of the relations between the various critical infrastructures is part of their strength and, at the same time a source of vulnerability.

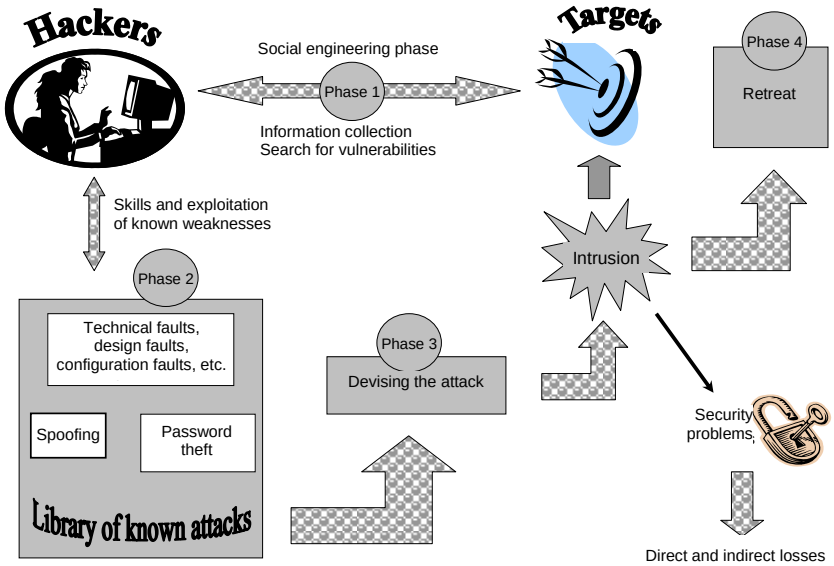
It is essential that the gateways between the networks used to operate these infrastructures and the internet be made secure, and that regional or national bodies be set up to oversee the protection of critical infrastructures. Their first task must be to coordinate the design and maintenance of plans for the protection of each of the infrastructures. Coordinated, consistent plans and security solutions are essential in case of emergencies striking several infrastructures simultaneously.

II.2.7 Phases in a cyberattack

Figure II.6 shows the different phases in a cyberattack[21].

The object of the first phase is to gather information and explore potential vulnerabilities in the target system, in order to gain the maximum information for future exploitation. This involves studying the mechanisms and levels of security used for identification, authentication, access control, encryption and surveillance, and identifying technical, organizational and human weaknesses in the environment. The attacker often attempts to coax naïve or credulous users into revealing information that can be used to design an attack (this is called social engineering).

Figure II.6 – Typical phases in a cyberattack



21 Illustration taken from *Sécurité informatique et télécoms: cours et exercices corrigés* by S. Ghernaouti-Hélie (Dunod 2006).

Hackers can also look for and exploit known - but not yet repaired (patched) – security vulnerabilities, using the available means (attack libraries, attack toolkits) to infiltrate the system. The retreat phase is intended to cover up the traces of the attack, and ensure that such traces as are left do not allow the hacker to be identified. Hackers increase their anonymity by using aliases, usurping legitimate users' identities, or covering their tracks by means of multiple intermediate (relay) systems.

PART III

TECHNOLOGICAL APPROACH

Section III.1 – Telecommunication infrastructures

III.1.1 Characteristics

By virtue of its vast geographical coverage, the telephone network has become a primary network serving a large number of users. Today, the telephone network infrastructure can be used to carry not only speech, but also data. It is thus possible, with the requisite interfaces, to connect computers over the telephone network. Also, internet network access points have proliferated in recent years, cybercafés are still on the increase and more and more countries are being equipped with a more accessible transport infrastructure offering even greater capabilities. In some places, cable networks are being deployed to support the transmission of television channels.

In addition to fixed telecommunication infrastructures, there are also what are known as "wireless" infrastructures, which allow user mobility. Wireless technologies are supported by satellite and space infrastructures and terrestrial radio systems. In recent years, mobile telephony has become a means of providing services in many developing countries.

The GSM (Global System for Mobile communication) standard has established itself on several continents for the transmission of voice and sometimes small volumes of data. However, it is the new generation of mobile networks, based on the UMTS (Universal Mobile Telecommunication System) standard, which, offering better transmission capabilities, is paving the way for more extensive use of mobile multimedia handsets. Having said this, GSM networks are evolving, to incorporate GPRS (General Packet Radio Service), which allows increased transmission speeds in order to meet the requirements of data applications over mobile networks.

The sudden arrival of technologies like GSM reflects not only a technological but also a behavioural and economic change. Mobile communications is a booming industry, within a context of fierce global competition. It has also allowed a new service, radiotelephony, to enter the telecommunication market, hitherto the exclusive province of operators, while constructing an infrastructure that can be reused for all kinds of data transfer.

Irrespective of the technology adopted for the deployment of e-services, telecommunication infrastructures in the developing countries should provide for:

- standardized digital interworking (voice, data, image) of a defined set of basic services that are easy to set up and maintain and offer the requisite geographical coverage (national and international), within the framework of a total-quality approach (a sustainable, stable and granular offering that can be altered at little technical and economic cost) and optimum security;
- technical and commercial harmonization; protection against possible cartelization, for harmonious development of infrastructures and services, with a guarantee of active regulation of abuses of dominant positions.

III.1.2 Fundamental principles

A telecommunication network is constituted by a set of information and transmission resources working together, offering communication services. These services allow remote access and sharing of interconnected information resources, interconnection of applications and people, remote execution of programs and transfer of information.

All economic activity is now critically dependent on the availability of an efficient communication infrastructure linking all sorts of equipment, applications and people, and enabling them to work together, irrespective of distance, place and the type of information flows to be transferred.

Networks are distinguished primarily on the basis of a number of criteria such as geographical coverage, topology[22], technology employed and applications supported, mode of operation, type of transmission medium (wireline/wireless), their private or public nature, etc.

Historically, the first networks were wide area networks[23] (telephone, telex, Transpac, internet, etc.). It is with the dawn of PCs (at the beginning of the 80s) that local area networks emerged[24].

Of late, these distinctions have tended to become less marked, since the networks in question are interconnected. A local area network, for example, may be connected to other LANs and thereby become a larger network. Moreover, networks are no longer dedicated to supporting a single type of application, but can be used to transmit voice, data and video images (multimedia network).

A network may be private, belonging to an organization which has exclusive usage rights, or public. In public networks, telecommunication services are made available to various individuals or institutions on the basis of particular subscription arrangements.

The main transmission technologies used to set up wide area networks are TCP/IP, frame relay and ATM (asynchronous transfer mode). On the business LAN market, the main technology is ethernet and its high-speed variants (fast ethernet, switched ethernet).

In the telecommunication field, optical transport and ATM switching technology constituted a major step in the evolution of transmission infrastructures and arteries, enabling high-speed and high-quality transmission, dynamic bandwidth allocation, variable bit rates and multi-usage.

III.1.3 Network components

III.1.3.1 Interconnection media

In order to connect computers together and in a network, transmission media are required. These may be physical media (twisted cable pairs, coaxial cables, optical fibre) or intangible media (radio, infrared waves). These different media each have specific characteristics that determine their reliability and capacity to carry varying amounts of information at different speeds.

The transmission or capacity of an interconnection medium is the quantity of information transferred during a given lapse of time. It is expressed in kilo, mega or even terabits per second (e.g. 100 Mbit/s). It is proportional to the bandwidth of the transmission medium, which corresponds to the range of frequencies of a signal that can pass through the medium without any modification.

III.1.3.2 Connection components

The type of connection or connection component to be inserted between a transmission medium and a computer in order to link the two depends on the type of medium and transmission mode used. The connection box, or network interface, solves the connectivity problems and adapts the signal transmitted or received by the computer to the signal that can be transmitted over the medium. For example, a modem (modulator/demodulator) provides an interface between a computer, which is a digital machine processing digital signals, and a transmission medium such as an analogue telephone

---

22 A network's topology is the pattern of links connecting its different elements or nodes.

23 A wide area network or WAN is a network connecting computers spread over a relatively large geographical territory (> 100 km), or even worldwide.

24 A network is termed a local area network or LAN when it connects computers in a small geographical area a few kilometres in size (~10 km). A metropolitan network or MAN is a network interconnecting local networks that may belong to different entities, having a geographical coverage of up to 100 km. New terms are being coined to identify different types of networked resources or to depict a specific application domain. Thus, for example, the following acronyms are encountered in specialized texts: HAN (home area network), a network interconnecting remotely controllable equipment in a house (oven, VCR, lighting and heating, etc.); CAN (car area network); SAN (storage area network); etc.

line, which transmits signals in continuous form[25]. In theory, any electronic component can be connected to the network insofar as it has an appropriate hardware and software connection interface.

III.1.3.3 Specialized machines and data servers

Apart from user systems serving to access a network and the computers dedicated to managing and processing applications (data hosts and servers), communication processors constitute a network's transport infrastructure. These are computers that carry out one or more functions required to manage and set up telecommunications (resource optimization and sharing, routing of data, management of addresses, names, interconnection, etc.). They include, for example, routers, multiplexers, concentrators, switches or interconnection gateways.

In order to communicate, information has to be reliably transmitted according to exchange arrangements that are satisfactory for the correspondents. The point is that systems interconnected over telecommunication networks are *a priori* different. In order to be able to dialogue, they have to use the same frame of reference for communication, in other words speak the same language and follow common exchange rules.

This is like two people of different mother tongues wishing to exchange information, who will agree on which language to use. One may make the effort to speak the other's language, or they may use a third common language.

If then a third, a fourth, a fifth person, and so on, joins the initial conversation, and these people speak other languages, it is liable to become difficult for them to exchange information if one language has to be translated into another for each pair of interlocutors. In this case, it is preferable to speak a common language that will be adopted by all the parties involved.

In the same way, networked computers have to comply with identical communication protocols and follow the same dialogue rules in order to be able to communicate. These protocols are integrated in the communication software. They serve, *inter alia*, to make sure that the data are correctly routed and ensure interworking of the remote applications and systems.

International standards or *de facto* standards are defined by bodies recognized by the whole industrial community. The International Organization for Standardization (ISO) and the International Telecommunication Union (ITU) are international standardization organizations that recommend international standards (for example the X.400 series standards).

A *de facto* standard is a standard which, while not adopted by such a body, is widely used in the market. It then becomes a reference, i.e. a *de facto* standard. For instance, all the protocols stemming from the internet community are *de facto* standards.

The standards define, *inter alia*, the type of services to be provided by communication protocols and specify how they are to be established. This makes it possible to design data solutions that can communicate with each other. Therefore, by using the same types of protocols in different (heterogeneous) machines, they are able to communicate. The universal nature of the internet hinges on the integration of protocols of the internet family in all the machines connected.

III.1.4 Telecommunication infrastructure and information highway

By telecommunication infrastructure, we mean all the transmission media on which communication services can be set up. A distinction is drawn between the transmission channels and routing technologies, on the one hand, and the telecommunication solutions and services offered to customers, on the other. It is thus possible, without owning it, to utilize an existing infrastructure as a transport facility for providing particular applications.

---

25 In order for the information at the output of a computer to be carried over such a medium, it has to be modulated. The information carried in analogue form has to be demodulated on reception and presented to the computer of destination in digital form. The same piece of equipment, the modem, modulates and demodulates the information emitted and received by a computer.

With the availability of multimedia equipment and high-performance communication infrastructures, as well as the convergence of the audiovisual, information technology and telecommunication worlds, the concept of a fully digital information chain emerges: digital continuity between all the sources and users of information, both within the transport infrastructure and at the level of the content.

The concept of information highway encompasses the widespread provision, over high-performance communication infrastructures, of a range of public or commercial services that will help improve people's lives, for example in the realm of health, education, culture, land planning, administration or the media. By virtue of the nature of some of the services offered over the internet, the latter may be considered as an information highway.

III.1.5 The internet

III.1.5.1 General characteristics

The internet started in the United States, and spread progressively by linking together neighbouring information systems and computer networks. This reticular development is still ongoing. It determines the structure of the network, which is a network of networks. There can be no overall control of all the infrastructures thus placed end to end, insofar as they are independent and belong to different organizations.

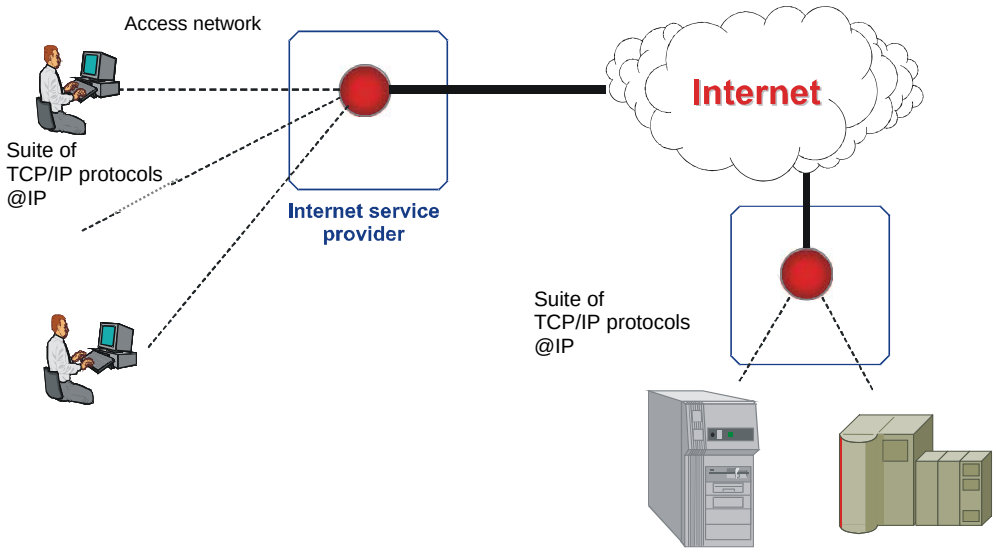
In hardware terms, the internet, like any telecommunication network, comprises information systems, connection elements and transmission media. The information systems include those which are used to access the network and allow dialogue with the end user (PC, mobile phone, pager, PDA, etc.), those that support applications (web server, database server, etc.) and those dedicated to processing within the network (routers, interconnection gateways, etc.).

Data is exchanged between computers over the transmission media by which they are physically connected. When the access point to the internet infrastructure is through a system allowing user mobility, such as for example a mobile phone, then we speak of mobile internet.

Data transfer, routing and communication between the distributed information processes and human users are achieved by communication protocols of the TCP/IP family[26]. These exchange softwares, standardized in the internet world, constitute a communication interface that enables interoperability of different types of systems. To communicate in the internet environment, a computer must be equipped with these communication protocols and have an IP address affording it a unique identity (Figure III.1).

[26] TCP/IP: Transmission control protocol/internet protocol.

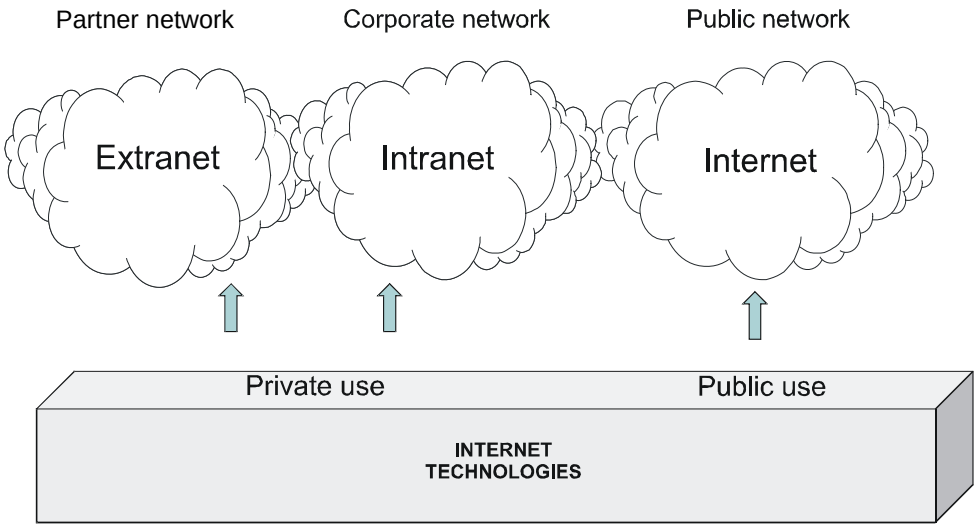
Figure III.1 – Internet access via an ISP, a suite of TCP/IP protocols and an IP address



Internet designates the whole of the communication infrastructure made available to the public in order to communicate. When an organization wishes to use this infrastructure privately and restrictively, it establishes a virtual private network (VPN). For internal needs, it may also use internet technologies to construct a private network or intranet. When the intranet is also open to a number of partners (customers, suppliers, etc.), it is called an extranet (Figure III.2).

Together with e-mail, the world wide web (or "web" for short) is the most important internet application. On the basis of web navigation, a multitude of services have been developed. It is possible to navigate throughout the web, thanks to a client software, the browser, installed in the user's workstation, allowing remote access to web servers. It can be used to search, consult or transmit information or even run programs. The notion of browsing or surfing the web stems from the fact that the documents accessible via the web application are hyperdocuments. This means that they have been designed, structured and formatted so as to be read in a non-sequential manner, using tags and links inserted when they were created. Activating a link takes the reader to another part of the document or a different document, possibly located on a remote computer. One thus surfs from site to site by activating these hyperlinks.

Figure III.2 – Internet – intranet – extranet



III.1.5.2 IP address and domain name

Access to the internet network is through access points managed and controlled by specialized enterprises called internet service providers (ISP). Each ISP is itself connected to the internet over permanent telecommunication lines which it shares among its different clients. In addition to this basic service, it generally offers an e-mail management service and can also host its clients' websites.

In order to communicate over the internet, one needs an internet address (IP address). This is a 32 bit binary sequence unambiguously identifying each machine communicating on the internet[27].

An IP address is expressed in its decimal form, comprising four decimal numbers separated by periods (full stops). For example, the address 128.10.2.30 corresponds to the binary value 10000000.00001010.00000010.00011110. Since it is impossible to memorize such number sequences, even the decimal ones, names (often mnemonic) or logical addresses are used to identify resources in the internet environment. These IP addresses and corresponding names are stored and managed in electronic directories called name servers, known in practice by the acronym DNS (domain name server).

To implement communications in an open environment, it is necessary to be able to allocate a unique identifier in a given naming domain. The parties involved in the communication have to be identifiable (addresses, systems, application processes, entities, management objects, etc.), as must the implementation tools for setting up the communication (protocols). In order to ensure unique names worldwide, there are procedures for registering names with competent authorities, whose role is to allocate an unambiguous and unique identifier to each object to be identified.

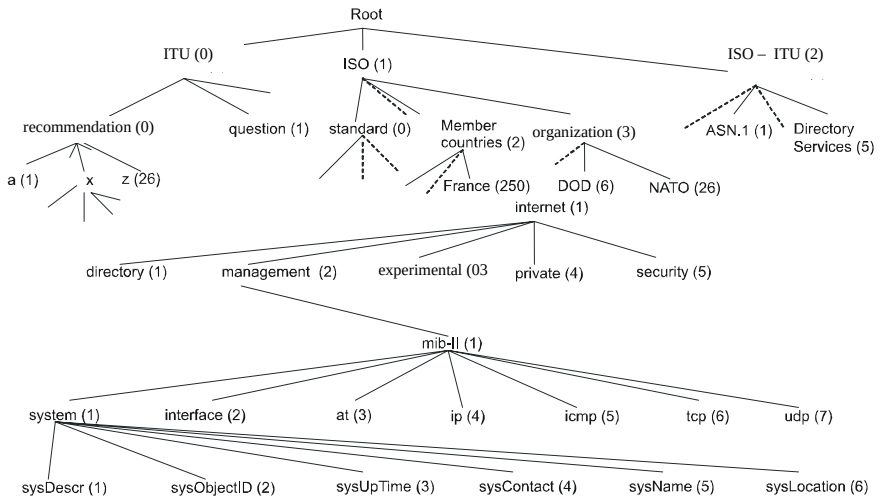
ISO standard 9834 specifies the registration authorities and organizes them in a hierarchal tree structure. The root of the tree has three branches, leading to distinct first-level nodes representing the naming domains ITU, ISO and a joint ISO-ITU committee. These are the international registration authorities. The level immediately below ISO authorizes the registration, *inter alia*, of:

---

27 An IP address is unique. It can be allocated permanently (static IP address) or not (dynamic IP address).

- various ISO standards (0 standard);
- ISO members (member-body 2), under which we will find AFNOR (208) and ANSI (310);
- organizations (organization (3)), under which are located for example the American Department of Defense (DOD) (6) (Figure III.3).

Figure III.3 – Registration authorities and tree



Generic internet domain names are registered in this logical registration structure. The relevant part of the registration tree in this case is the root node of the highest-level domain names called top-level domains (TLD). These identify primarily countries, indicated by two letters (fr, it, uk, ch, nl, de, etc.), and functional domains such as:

- .com commercial organizations;
- .edu academic institutions in North America;
- .org organizations, institutional or otherwise;
- .gov American government;
- .mil American military organizations;
- .net network operators;
- .int international entities;
- .biz for the business world;
- .info for all uses;
- .name for individuals;
- .museum for establishments in which collections of objects are kept and classified for conservation and exhibiting to the public;
- .aero for the air-transport industry;
- .coop for cooperatives;
- .pro for professions.

Within these broad domain designations, there are subdomains, corresponding to large corporations or important institutions.

The Internet Assigned Number Authority (IANA)[28] within the Internet Corporation For Assigned Names And Numbers (ICANN)[29] is responsible for allocating names and addresses and must ensure that they are all unique. This responsibility for managing names may be delegated to a subdomain which is hierarchically under its authority.

Registering a domain name consists in inserting an entry in a name directory. This is tantamount to creating a new arc in the registration tree managed by an authorized organization. There are several of these worldwide, notably for the domains .biz, .com, .info, name, .net, .org.

In the case of France, for example, the registration authority (accredited registrar directory) accredited by ICANN is AFNIC[30].

Authority for the allocation and management of addresses is entrusted to an American association – on American territory, operating under American law[31]. This association thus controls access to the internet. This poses a genuine problem of the dependence of organizations and States on a foreign supra-structure which has a vocation to be open to the rest of the world but in which non-American representation is weak.

The criterion of security in terms of availability (of infrastructures, services, data), which hinges on the accessibility to the internet network, cannot be controlled or governed by organizations. Organizations depend, for their access to the internet, on the allocation of IP addresses and domain names, hence on outside entities.

The domain name directories can be seen as databases managed by DNS servers. Some fifteen DNS root servers are coordinated by ICANN, and the vast majority of root servers are located in North America. They manage the top-level domain names and IP addresses. This includes all of the domains referred to above (.org, .com, etc.) and also the 244 domain names for the different countries (.cn – China, .ga – Gabon, .lk – Sri Lanka, .pf – French Polynesia, etc.). Local DNS servers called resolvers keep a copy of the information contained in the root servers. These resolvers, frequently associated with strategic network access points or linked to internet service providers, serve to answer user queries regarding the translation of a domain name into an IP address (Figure III.4)[32].

---

28 http://www.iana.org/.

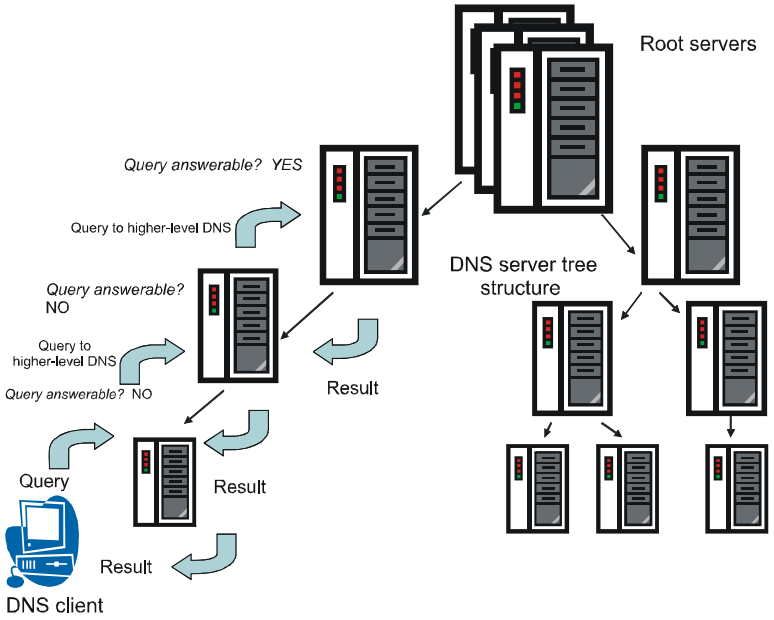
29 http://www.icann.org/index.html.

30 http://www.afnic.fr.

31 According to ICANN: "The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for internet protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) top-level domain name system management, and root server system management functions. These services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. ICANN now performs the IANA function."

32 Figure taken from: "*Sécurité informatique et télécoms: cours et exercices corrigés*"; S. Ghernaouti-Hélie; Dunod 2006.

Figure III.4 – DNS server tree structure



It is vital that the addresses, processes and systems involved in the management of names and addresses and the routing of data should be characterized by availability, integrity, reliability and security. It is the responsibility of the entities in charge of transport infrastructures to protect and effectively manage their communication environments.

III.1.5.3 IPv4 protocol

Version 4 of the internet protocol (IPv4)[33], which has existed since the beginnings of the internet network, is still widely used. The role of this protocol is to encapsulate the data to be transmitted in order to constitute IP packets that will be routed over the internet network to their destination. Each packet contains, among other things, the source IP address of the sender system and the IP address of the destination system.

Routing is carried out by handing on to each intermediate system (router) crossed, following the interpretation of the packet addresses and the routers' routing algorithm.

The IPv4 protocol does not include any function or mechanism for guaranteeing secure service. Indeed, under IPv4 there is no way of authenticating the source or the destination of a packet, nor of ensuring the confidentiality of the data transported or of the IP addresses involved in the transfer of information between two entities. In addition, since the protocol operates in connectionless mode, there is no guarantee of:

– delivery of data (possible data loss);

33 IPv4: RFC 0791 –www.ietf.org/rfc/rfc0791.txt IPv4 and main TCP/IP protocols:
TCP: RFC 0793 – www.ietf.org/rfc/rfc0793.txt – UDP: RFC 0768 – www.ietf.org/rfc/rfc0768.txt – FTP: RFC 0959 – www.ietf.org/rfc/rfc0959.txt – HTTP version 1.1: RFC 2616 – www.ietf.org/rfc/rfc2616.txt – Telnet: RFC 0854 – www.ietf.org/rfc/rfc0854.txt

– delivery of data to the right addressee;
– correct sequencing of data.

The IP protocol (layer 3 of the OSI architecture) offers an unreliable IP packet delivery service. It operates in so-called "best effort" mode, in other words it does its best in the circumstances and packet delivery is not guaranteed. In fact, no quality of service whatsoever is guaranteed and there is no error recovery. Thus, a packet can be lost, altered, duplicated, fabricated (forged) or delivered out of sequence without the sender's or recipient's knowledge. Because no prior logical relationship is set up between sender and recipient, this means that the sender sends his packets without informing the recipient and they can get lost, take different routes or arrive in the wrong order.

To counter this lack of quality of service, the transmission control protocol (TCP) is installed in end systems. TCP offers a reliable transport service in connection-oriented mode (layer 4 of the OSI architecture). However, the TCP protocol does not offer any security service in the true sense of the word.

Section III.2 – Security tools

Securing information, services, systems and networks entails ensuring availability, integrity and confidentiality of resources, as well as non-repudiation of certain actions, and the authenticity of events or resources.

Data security is only meaningful if it is applied for data and processes which we are certain to be exact (notion of quality of data and processes) so that they may be stable over time (notion of data stability and service continuity).

The main security solutions are founded on the use of encryption or environment isolation techniques, on resource redundancy, and on procedures for surveillance, control and management of incidents and for system maintenance, access control or management.

Data security in telecoms is obtained by means of a succession of barriers (protection measures) which raise the level of difficulty that potential assailants have to overcome in order to access the resources. They do not solve a security problem, but just shift it and transfer responsibility for security to other entities. Security solutions have to be protected and secured themselves if they are to offer a certain level of security (recursive nature of security).

III.2.1 Data encryption

Encryption techniques make it possible to preserve data confidentiality, check data integrity and authenticate entities.

There are two main types of data encryption system: symmetric (private-key) encryption, and asymmetric public-key encryption.

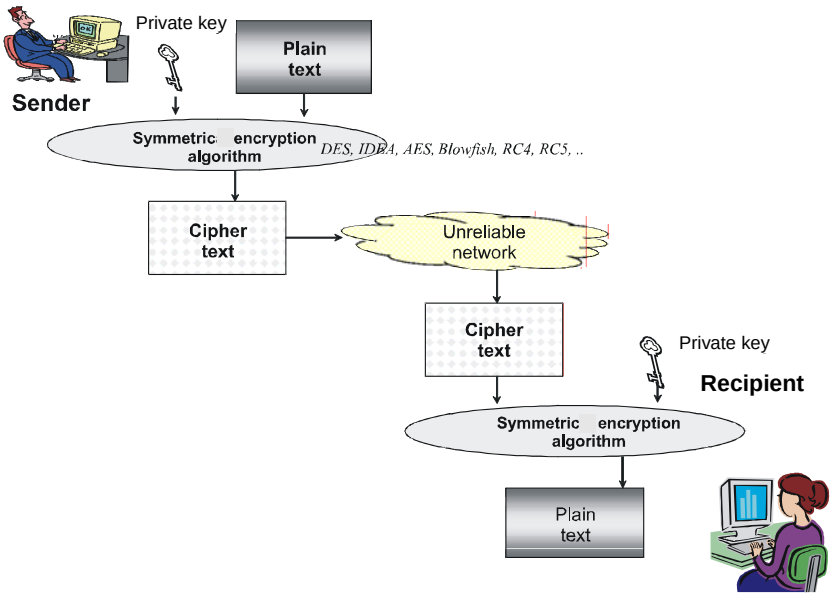
Various encryption algorithms exist. Irrespective of whether they operate in symmetric or asymmetric mode, they are founded on the use of keys. In general, how robust they are hinges on the ability to manage encryption keys in a secure manner, on the length of the key (the minimum length of the key is determined by the type of algorithm), and on the security of the physical and software platform in which the encryption algorithms are installed and run.

III.2.1.1 Symmetric encryption

In order to encrypt or decrypt a text, one needs a key and an encryption algorithm. If the same key is used for both operations (encryption and decryption), the encryption system is termed "symmetric". The sender and receiver have to possess and use the same private key to make data confidential and to be able to understand them. This poses the problem of managing the distribution of private keys (Figure III.5).

The main symmetric encryption algorithms are: DES, RC2, RC4, RC5, IDEA and AES.

Figure III.5 – Symmetric encryption



III.2.1.2 Asymmetric or public-key encryption

An asymmetric encryption system is based on the use of a unique pair of matching keys. This double-key comprises a public key and a private key. Only the public key can be known to everyone, whereas the private key must remain confidential and be kept secret.

The sender encrypts a message with the recipient's public key and the recipient decrypts the message with his private key (Figure III.6).

The main public-key encryption algorithms, named after their inventors, generally use keys of length ranging from 512 to 1 024 bits, or sometimes 2 048 bits. They are: RSA[34] (stands for R. Rivest, A. Shamir, L. Adelman), Diffie-Hellman[35], El Gamal[36].

III.2.1.3 Encryption keys

An encryption key must be kept doubly secret. Secret keys for encryption systems have to be managed in a confidential manner.

As already indicated, security of the encryption process hinges to a very large extent on the confidentiality and the length of the keys used, how robust the algorithms are and the security of the underlying hardware and software platforms.

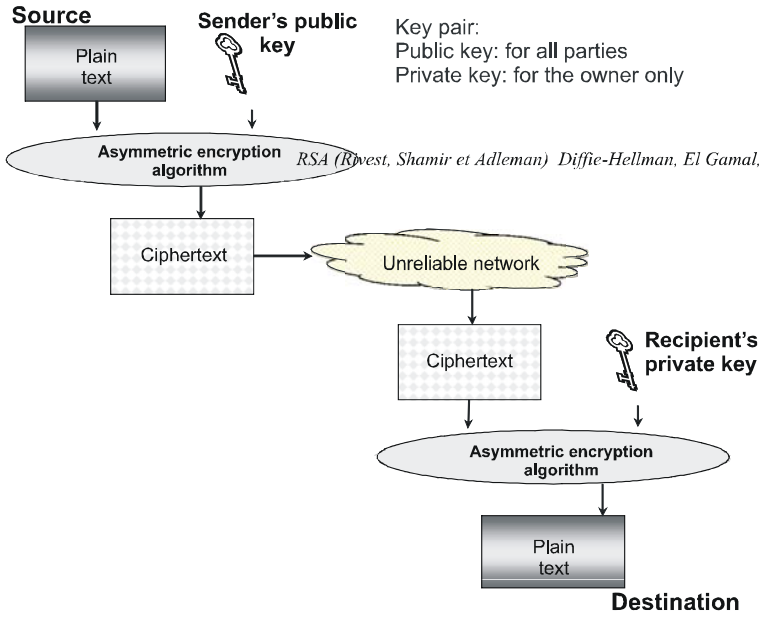
---

34 RSA: Schneier B, "Applied cryptography" 1996, 2nd edition 1996.

35 Diffie-Hellman: www.ietf.org/rfc/rfc2631.txt.

36 El Gamal: Schneier B, "Applied cryptography" 1996, 2nd edition 1996.

Figure III.6 – Asymmetric encryption



III.2.1.4 Key management system

A public key infrastructure (PKI) is used to implement asymmetric encryption systems. The main functions it supports are:

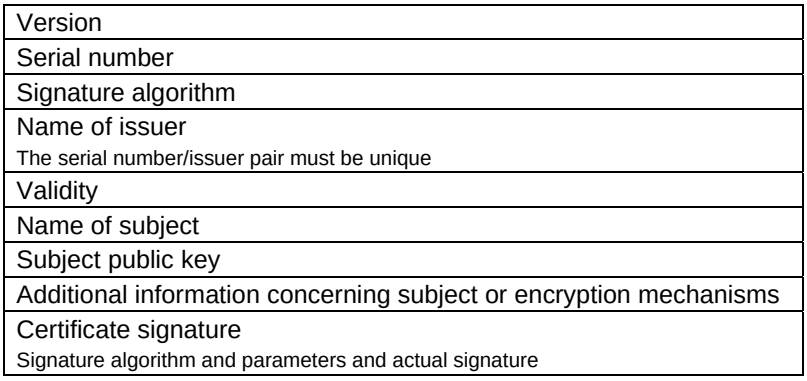
- generation of a unique key pair (private key + public key), allocation of a pair to an entity and storage of the necessary information for its management, archiving of keys, and procedures for retrieval if the user should lose the key or the judiciary authorities should request disclosure;
- management of digital certificates, and establishment, signature, issue, validation, revocation and renewal of certificates;
- dissemination of public keys to authorized requesting resources;
- certification of public keys (signature of digital certificates).

III.2.1.5 Digital certificates

A digital certificate is the digital identity card of an entity (legal or physical person) or an information resource, subject of the certificate. It contains, among other things, the identity of the subject (holder), the public key assigned to the subject and the identity of the issuing body.

The X.509 standard (directory authentification framework) offers an architectural framework for the establishment of an authentication service based on the use of digital certificates, and specifies the structure and format of a digital certificate. This standardized structure is adopted in many solutions on the market (Figure III.7).

Figure III.7 – Main elements of an X.509v3 digital certificate



To validate a certificate received, the client has to obtain the public key of the issuer of the certificate pertaining to the signature algorithm, and decrypt the signature. With this information, the client calculates the hash value and compares it with the value in the last field of the certificate. If the two values match, the certificate is authenticated. The client then ensures that the period of validity of the certificate is correct.

With access control based on digital certificates, a large number of users can be connected to a given server. Control is effected on the basis of the information contained in the client's digital certificate. The server thus trusts the validity of the certificates and the manner in which they were issued, which constitutes a loophole in system security, since it is possible to corrupt a certification server or even create a forged digital certificate. Moreover, controlling a certificate's validity is no easy matter. Revocation of certificates is an extremely laborious task, since the information has to be transmitted to all the parties and registered in the certificate revocation list (CRL). A certificate has to be revoked as soon as any change occurs in its content (e.g. when information in the certificate becomes obsolete, the user's private key has been corrupted, the user leaves the company, etc.). Systematic consultation of the corresponding database slows down access control and diminishes the availability of the servers, including for authorized users.

III.2.1.6 Trusted third party

Whatever name it may go by – trusted third party (TTP), registration authority, certification authority, or certificate authority – the main function of the body setting up a public key infrastructure is to issue certificates vouching for the public key assigned to an entity (identify certificate).

A client files a registration request (certification request) to a certification authority (web-based registration service). The registration server may ask for proof of the client's identity according to the identification and authentication procedures put in place by the authority. After validation of the information, the certification server generates encryption keys and produces a digital certificate in the client's name, signs the certificate with its private key (certification of the digital certificate) and sends the certificate to the client. The client will use the authority's public key to verify that the certificate has indeed been issued by the authority in question.

A certification authority is a trusted third party which issues digital certificates and serves to verify the validity of certain information.

III.2.1.7 Drawbacks and limitations of public key infrastructures

The fact that there are several certification authorities poses problems in terms of their mutual recognition, their interoperability, the compatibility of certificates and their scope of validity.

Nevertheless, it is not desirable to have only one global certification authority, in view of the vast and excessive powers that would *de facto* be conferred on it, and in view of the magnitude of the infrastructure to be established. There is a genuine lack of trust on the part of users in respect of such certification authorities, which are generally foreign (validity of certificates? security guarantees? protection of personal data? etc.).

The inherent limitations in public key infrastructures reside in:

- the complexity of an infrastructure, and the cost of deploying and managing it;
- the high level of security required to set up PKI services;
- the validity, duration and termination of certificates.

The potential problem areas in the implementation of PKI services include:

- Political problem: Most PKI infrastructures – certification authorities – belong to American (US) entities. This raises the question of performance and the issue of trust in these entities in view of the services they provide (creation, storage and distribution of private and public keys, identification data, notarization), the lack of guarantees in terms of possible misuse of data, neutrality in exchanges and available recourse in the event of a dispute with the certificate authority.
- Technological problem: Conventional encryption systems can be broken, some digital certificates offer no security or guarantees, fraud is possible, infrastructure security is provided by conventional security means which can be circumvented. Furthermore, the use of a key infrastructure shifts the problem of security of exchanges, without actually resolving it.
- Organizational problem: Infrastructure interoperability, deployment, management, maintenance, security, complexity, etc.

III.2.1.8 Signature and authentication

A sender encrypts a message with his private key. Any entity knowing the sender's public key will be able to decrypt the message, thereby confirming the fact that it was indeed created with the corresponding private key.

A document can be signed electronically (digital signature) using a public key encryption algorithm, as follows:

- creation of a message declaring the sender's identity – the signature (e.g. "My name is Alpha Tango Charlie") – which is encrypted with the sender's private key and attached to the message to be transmitted;
- the message and its signature are encrypted with the recipient's public key, and transmitted;
- the recipient decrypts the message with his private key and detaches the signature which he deciphers with the sender's public key.

We must be careful, however, in that there is nothing to prevent someone reusing the digital signature of a message in place of the real sender, and it is also possible to create a digital signature in a partner's place after stealing his private key. In order to increase the level of security of the digital signature, the signature is formed from the content of the message, thereby ensuring message integrity and sender authentication.

III.2.1.9 Data integrity

It is possible to verify that the data have not been altered during transmission by attaching a message digest which is transmitted at the same time as the data. The digest is derived from a hash function applied to the data. The recipient recalculates the hash value from the data received using the same function. If there is any discrepancy in the value obtained, it may be inferred that the data have been altered. The digest itself can be encrypted before the data are transmitted or stored.

Both symmetric and asymmetric key encryption systems are capable of determining whether the transmitted data have been altered, because they then become impossible to decrypt. This helps to check integrity, but is not capable of confirming that the data have not been completely destroyed.

For more effective integrity control, a function is applied to the original message which converts it into a short random sequence of bits, constituting a sort of digital fingerprint (digest).

A so-called one-way hash function generates a message digest, i.e. its digital fingerprint, which is shorter than the original message and incomprehensible. This is then encrypted with the sender's private key and attached to the message to be transmitted. On receipt of the message and its fingerprint, the recipient decrypts the fingerprint with the sender's public key, recalculates the fingerprint from the message received using the same hash function, and compares it with the fingerprint received. If the result is the same, the recipient has thus verified the sender's identity and is assured of the message's integrity, since, if the message is altered, even only slightly, its fingerprint is significantly modified.

By using a combination of encryption, signature and digital fingerprint techniques, messages can be marked to guarantee data integrity. These procedures consume considerable processor time and slow down significantly the performances of an operating environment.

III.2.1.10 Non-repudiation

The non-repudiation service is designed to prevent refusal or denial that a message has been sent or received or an action or transaction has taken place. It makes it possible to prove, for example, that an entity is associated with a given action or event.

Non-repudiation is based on a single signature or an identification proving who created the message. This service can be provided by means of a public key encryption algorithm. A trusted third party can also be employed as cybernotary.

III.2.1.11 Limitations of encryption-based security solutions

Confidence in encryption solutions on the market can only be relative, insofar as there are no guarantees or means of verification (existence of back doors in software? secret keys duplicated, divulged, etc.?). Also, there is no proof that algorithms currently deemed to be reliable will remain so in the near future.

III.2.2 Secure IP protocol

The need to accommodate security requirements militated in favour of a revision of version 4 of the internet protocol. Moreover, there was also a need to provide for a wider range of addresses and increase the number of available internet addresses, as well as to allow dynamic allocation of bandwidth to support multimedia applications. As a result, a revised version of the IP protocol has been produced called "internet protocol next generation" (IPnG), or IP version 6 (Pv6)[37].

III.2.2.1 IPv6 protocol

In 1994[38], the Internet Activity Board (IAB)[39] addressed the security requirements of the IP protocol. Version 6 of the IP protocol (IPv6) includes authentication and confidentiality facilities.

The main developments in IPv6 in relation to IPv4 relate to the following points [RFC 2460]:

– expanded address space and address hierarchy: address size increased to 128 bits (16 octets) from 32 bits (4 octets); addresses represented in hexadecimal numbers[40] separated by colons every two octets (e.g. 0123:4567:89ab:cdef:0123:4567:89ab:cdef), instead of dot-decimal notation;

---

37 IPv6: RFC 1883 in 1995, replaced in December 1998 by RFC 2460 – www.ietf.org/rfc/rfc2460.txt.

38 RFC 1636: Report of IAB Workshop on Security in the Internet Architecture, 8-10 February 1994.

39 www.iab.org/

40 Alphabet of hexadecimal numbering system (base 16): 0 1 2 3 4 5 6 7 8 9 A B C D E F.

– the possibility of dynamic bandwidth allocation to support multimedia applications;
– the capability to create virtual IP networks;
– supporting authentication and encryption procedures, using options headers;
– simplification of packet headers to facilitate and speed up routing.

Adopting IPv6 calls, *inter alia*, for modification of the addressing and address management mechanism[41], the installation throughout the internet environment of systems supporting IPv6, systems operating with both versions, large-scale synchronization of version migration, etc.

For all these reasons, version 6, which was specified back in 1995, is still not yet widely installed and no government incentive or international recommendation seems to be able to impose adoption of version 6 of the protocol throughout the network. Only a few private infrastructures incorporate IPv6.

Implementation of the new internet protocol (IPv6) with its built-in security functions is uncommon. Therefore, to meet network security requirements, an intermediate solution called IPSec[42], compatible with both IPv6 and IPv4, has been developed and adopted by the internet community. The Internet Engineering Task Force (IETF)[43] issued several documents in 1995 (RFC 1825 to 1829) specifying ways of securing an internet infrastructure.

III.2.2.2 IPSec protocol

With IPSec, the content of packets transported by the protocol can be made confidential. IPSec offers data confidentiality and authentication services at the level of transfer by the IP protocol, through the insertion of an authentication header (AH) or an encapsulating security payload header (ESP).

Each application, irrespective of the type of traffic it generates, can use these security services without any adaptation. IPSec operates in point-to-point mode (the data are secured between a sender and a receiver via a secure relationship between them).

The authentication header provides IP packet authentication and integrity services, thus guaranteeing that the data have not been altered during transmission and that the source address is indeed the one that appears on the packet.

The encapsulating security payload header allows the implementation of encryption mechanisms (symmetric encryption such as DES, Triple DES, RC5 or IDEA) and offers similar authentication services to those provided by the authentication header.

The encryption algorithms use keys which have to be generated and disseminated. Encryption key management is thus an important task to be carried out in implementing IPSec-based solutions. The key exchange protocols include, for example: Oakley key determination protocol[44], based on the Diffie-Hellman key exchange algorithm [RFC 2412]; Internet Security Association and Key Management Protocol (ISAKMP) [RFC 2408]; Internet Key Exchange (IKE) [RFC 2409].

III.2.2.3 Virtual private networks

With the installation of the IPSec protocol at access points to the internet network, it is possible to establish between those points a communication channel whose ends are authenticated (Figure III.8).

These ends are located in the organization's systems, and are thus physically protected. According to the option adopted, data carried over the connection may be encrypted. In other words, a secure route can be set up between two points of an unreliable infrastructure (this is the concept of virtual private

41 RFC 1886 identified in 1995 the modifications to be made in DNSs to support IPv6.

42 RFC 2401 – www.ietf.org/rfc/rfc2401.txt

43 www.ietf.org

44 Oakley key determination protocol: RFC 2412 – www.ietf.org/rfc/rfc2412.txt.

network). It should be observed that the term "network" in the expression "virtual private network" is something of a misnomer, since only a (virtual) logical connection is established.

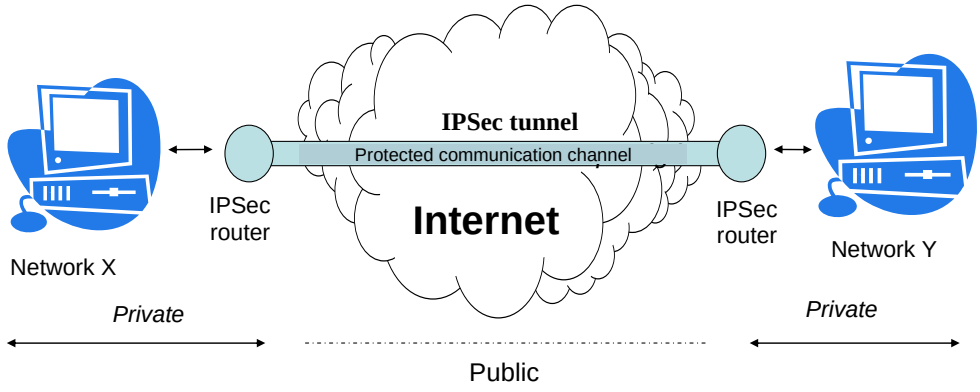
III.2.3 Security of applications

Most applications have a secure version, which generally allows authentication of correspondents and encryption of transmitted data.

An alternative to installing new secure versions of application protocols is to establish a common security mechanism offering generic security services for all applications. The secure sockets layer (SSL) software is now widely used, notably for the purpose of commercial transactions over the internet.

The extensive use of hypertext documents as well as the downloading of content, whether active or passive, pose numerous security problems relating, *inter alia*, to: source, author, authenticity, harmfulness, etc. Some responses to this new dimension of information system security are beginning to emerge: techniques for signature of XML documents, watermarking, management of electronic rights, so as to introduce some stability in terms of security. It has to be possible to maintain a given level of security, even if the object to be secured falls outside the physical borders of the environment in which its security is usually managed.

Figure III.8 – Establishment of a VPN using an IPSec communication channel



III.2.4 Secure sockets layer (SSL) and secure HTTP (S-HTTP) protocols

Secure sockets layer (SSL) is a software that ensures the security of application exchanges. It is supported by most web browsers on the market.

The two communicating entities in an SSL connection are authenticated through a certification procedure and a trusted third party. They then negotiate the level of security to be applied to the data transfer. The transmitted data are encrypted for the SSL communication (Figure III.8).

The installation of SSL has a significant impact from the point of view of the server, on account of the required certification, which necessitates a dialogue with a recognized certificate authority and also requires that the firewall application relays support SSL operation. Certification is sometimes considered as an impediment holding back the deployment of this solution.

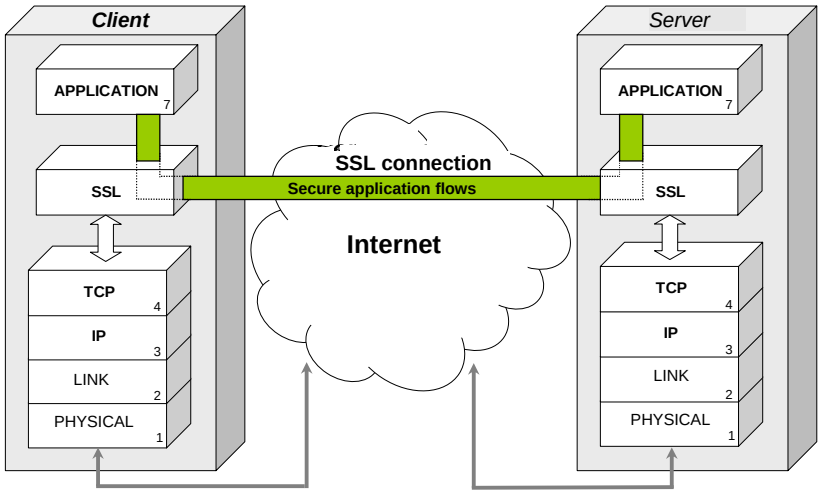
Extension to the HTTP protocol (secure HTTP, or S-HTTP) is an alternative solution developed by the CommerceNet association. S-HTTP offers the same security facilities as SSL, with the same certification constraints, but only supports HTTP data flows. This solution is not widely adopted.

III.2.5 E-mail and name server security

The security risks entailed in the use of an e-mail system relate to:

- message loss, interception, alteration or destruction;
- infection of systems through messages containing viruses, worms or Trojan horses;
- harassment: message bombardment, junk mail, spam affecting persons whose e-mail address is used without their prior agreement and with whom the sender (the spammer) has never been in contact. Spam involving the mass distribution of infected messages may contribute to the rapid propagation of viruses (spam + virus), with e-mail engines embedded in the virus code so that they are self-propagating;
- identity theft (an intruder pretends to be someone else, a system component transmits, listens to or intercepts messages not addressed to it, etc.);
- messages may be inserted, mixed, deleted or delayed;
- service may be refused on account of a defective component in the message system chain;
- disclosure of confidential information;
- repudiation (a party to the system denies having sent or received a message).

Figure III.8 – SSL (*secure socket layer)* architecture



To these must be added also all the threats associated with networks and their operation (attacks at the level of routing, name servers, etc.).

In order to offset these security limitations inherent in the way e-mail functions, new versions of the software incorporate encryption capabilities in order to ensure confidentiality, integrity and authenticity of information exchanged and of correspondents.

Security requirements for e-mail systems relate to:

- confidentiality and integrity (of a message or series of messages);
- non-repudiation (proof of sending, proof of receipt, signature, message certification);
- authentication of the identities of all parties to the e-mail system (users, intermediate elements, message memory, message transfer agents, etc.).

The greatest risk is probably the introduction of a virus, worm or Trojan horse through a message. One method of prevention is to install anti-virus software on each system in order to detect viruses and if possible disinfect it. An anti-virus software will detect only those viruses for which it is designed, and does not offer protection against new forms of infection, and the consequent need for constant updates demands a significant management effort.

Another possibility is to set up a quarantine server that rigorously scans every message received, with all its attachments. By using several anti-virus programs operating in parallel, the chances of catching an infected message can be improved further.

The original protocol used for e-mail on the internet, known as "simple mail transfer protocol" (SMTP), has been refined in the course of time so as to support multimedia message content, but also security mechanisms. Examples of these protocols include S/MIME (secure/multipurpose internet mail extensions), PEM (privacy enhanced mail) and PGP (pretty good privacy).

All internet applications rely, directly or indirectly, on the working of the domain name server (DNS) system, in which DNS servers relate logical names to the corresponding IP addresses. The DNS servers play a key role in ensuring that information is routed correctly. For this reason they are particularly sensitive components in the communication architecture, and require additional protection. Security mechanisms (control of access, authentication, logging, duplication, consistency, request and response encryption, etc.) are set up to prevent tampering with the information stored on the servers with the intention of deviating information to unintended recipients, denial-of-service attacks causing server overload or a network crash due to a deluge of fake requests, and bogus name servers being set up to obtain incorrect responses leading to transmission errors or intrusion.

III.2.6 Intrusion detection

Intrusions, incidents and anomalies must be detected and identified as soon as possible after they occur and be rigorously dealt with so as to ensure that the systems in question continue to function normally and remain protected.

An incident is an event which occurs unexpectedly. While incidents are for the most part not serious in themselves, they can nevertheless have severe consequences. An anomaly is an exceptional occurrence which can result in abnormal functioning of the information system and a breach of the security policy in force. Its causes may be accidental (for example, a configuration error) or deliberate (a targeted attack on the information system). An intrusion is characteristic of an attack and may be considered as an incident or an anomaly.

Intrusion detection refers to the set of practices and mechanisms used for detecting errors that may lead to breaches of the security policy, and for diagnosing intrusions and attacks (it includes anomaly and misuse detection)[45].

An intrusion detection system (IDS) comprises three main functional blocks, namely data gathering, data analysis, and intrusion detection and response.

III.2.7 Environment partitioning

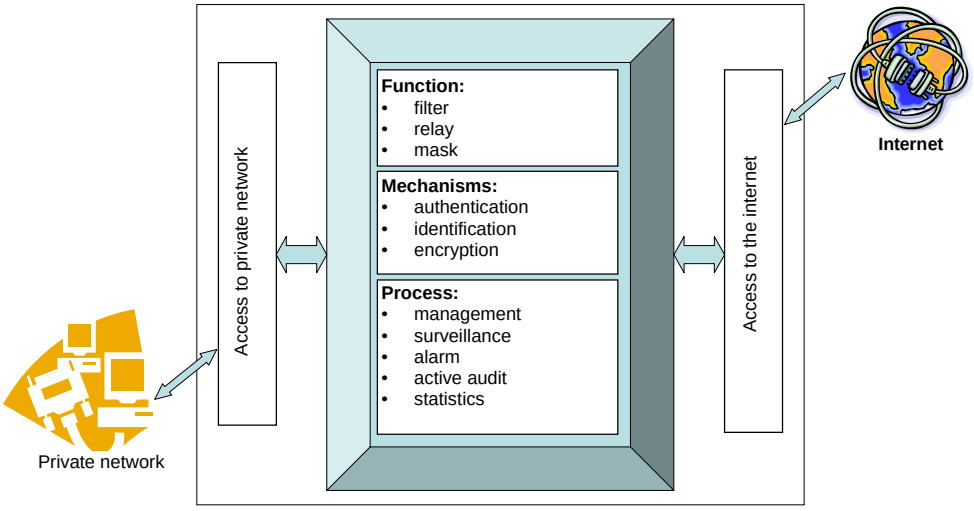
The separation and masking of a private environment vis-à-vis the public internet is achieved through the installation of one or more firewall systems.

---

45 Alessandri, D. et al. "Towards a taxonomy of intrusion detection systems and attacks" www.domino.watson.ibm.com/library/cyberdig.nsf/papers/5FA980EB952E09D085256AC600535997/$File/rz3366.pdf

A firewall is a system for filtering and, as the case may be, blocking data flows. It analyses the flow, authorizing it if it meets certain conditions, or otherwise rejecting it. By partitioning a network one can create separate IP environments by making the access points of the networks one wishes to separate physically independent of one another. This allows for the interconnection of two networks having different security levels (Figure III.9)[46].

Figure III.9 – Functional structure of a firewall



There are different types of firewall according to the nature of the analysis and processing to be carried out. They are generally categorized according to the level of data filtering provided: layer 3 (IP), layer 4 (TCP, UDP) or layer 7 (FTP, HTTP, etc.) of the OSI model.

An application firewall, also known as a proxy (proxy server, proxy firewall), acts as an application relay. Operating on the user's behalf, it establishes the required service. The purpose of the qualified proxy system is to provide address masking by application relay and to make the organization's internal environment transparent. It is intended to serve as a mandatory crossing point for all applications requiring internet access, and calls for the installation of a relay application on the user's workstation and on the firewall.

The installation and configuration of a firewall are based on the network architecture selected to meet the security and control requirements when connecting to different systems.

The firewall constitutes one of the tools used in implementing the security policy and is just one of the hardware and software components employed for that purpose, since a firewall on its own does not suffice to provide adequate protection for an organization's network and systems. It must be accompanied by tools, measures and procedures concomitant with the security objectives defined in accordance with the security policy. A firewall's effectiveness will depend essentially on its positioning vis-à-vis the systems it is to protect, as well as on its configuration and management.

46 Figure taken from "*Sécurité informatique et télécoms: cours et exercices corrigés*"; S. Ghernaouti-Hélie, Dunod 2006.

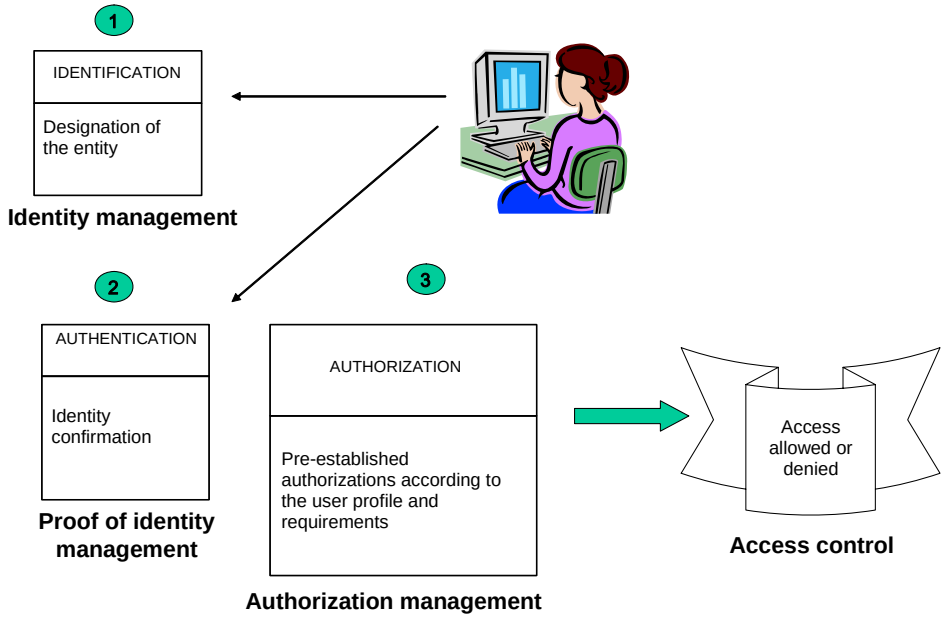
Although firewall and intrusion detection systems are able to perform certain security services, they are not in themselves adequate to ensure full protection of the information resources.

III.2.8 Access control

III.2.8.1 General principles

A logical access control mechanism, based on the identification and authentication of individuals and on the permissions or access rights that have been granted to them, serves to limit access to information resources (Figure III.10).

Figure III.10 – Basic components of logical access control



On the basis of an authenticated identification, the access control mechanism allows access, according to the user's profile, to the requested resources. This presupposes that the identity management, identity proof management and authorization management have been properly effected vis-à-vis the user.

The user profile contains all of the data on which access authorization decisions are based. It must be carefully defined in accordance with the access management policy.

The purpose of authentication is to associate the notion of identity with a given individual. Access authorization entails selective filtering of requests for access to the resources and services provided by the network in order to allow such access only to duly authorized entities.

The purpose of the authentication service is to check that the stated identity is the true one (proof of identity). This will generally depend on one or more of the following factors:

- a secret that is known to the entity in question, i.e. password or personal identification number (PIN);
- an item in the entity's possession (card, token, etc.);
- a feature unique to the entity (fingerprint, voiceprint, retina print, etc.).

Identity verification corresponds to a scenario in which the access requester states his identity and provides an item of proof that he alone is supposed to know or possess (e.g. password, confidential key, fingerprint). The authentication service then compares that information with the data stored in its authentication server.

An authentication server must be extremely well protected and secured by ad hoc mechanisms providing access control and secure systems management, and by encryption of the data it contains. An authentication server must not be vulnerable or subject to faults, since the overall security of the information and telecommunication infrastructure depends on its robustness.

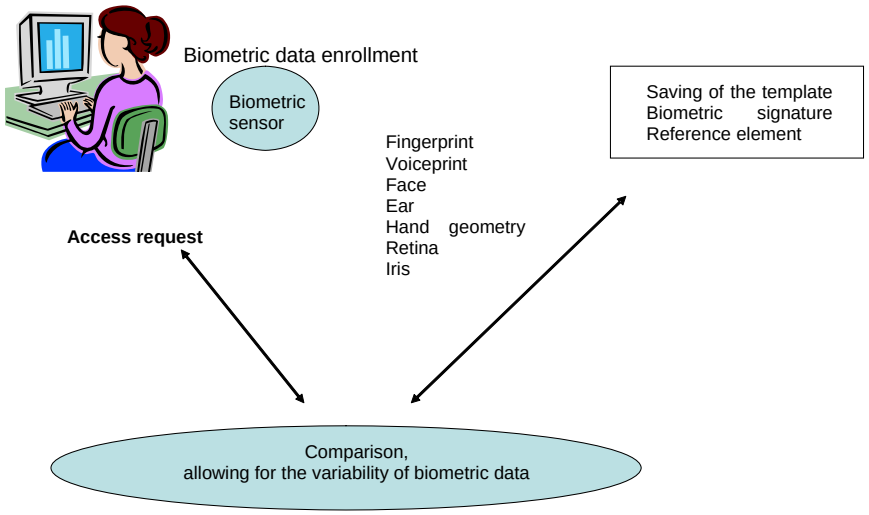
III.2.8.2 Contributions and limitations of biometry

Biometric individualization consists in using biometric data for checking the identity of individuals at the point of access to premises or within the framework of judicial supervision (by the police, etc.).

By using biometry to control access to information resources it is possible to do away with the password, replacing it with a physical characteristic from which a binary data value can easily be extracted.

To be able to use the physical characteristics of individuals in order to identify them and validate their identification, it is first necessary to extract and record their biometric characteristics in the form of a "biometric template". Such recordings must be highly reliable and securely stored (Figure III.11).

Figure III.11 – Biometric access control



The duration of the authentication process may be lengthy, since the comparison phase has to take account of the variations inherent in the live nature of the compared data. For example, a voice sample will never be fully identical. The comparison is based on statistical and probabilistic processing of the biometric data. The fuzziness that is included in the authentication system means that one can never be totally certain of the authentication result, i.e. the system is unable to determine with 100 per cent certainty that person "x" is who he or she claims to be. The error rate of such systems is still high, making it impossible to guarantee a high level of security. When combined with "conventional" authentication mechanisms based on passwords (dual verification), the biometric side serves to enhance the level of security provided.

The expanding use of biometric technology raises numerous issues of an ethical and ergonomic, not to mention economic, legal and technological, nature. Such issues include:

– the confidentiality of biometric data which may be considered private;
– cases in which biometric data may not be unique (identical twins);
– the fact that biometric data sensors are often seen as intrusive and are rejected by the majority of users in cases where a choice is available. They also constitute a threat to the freedom of the individual, e.g. a large number of sensors, such as video cameras, set up in public locations and operating without people's knowledge;
– cases of identity theft or of improper or fraudulent use of biometric data.

Given their lack of precision and continuing high purchase, deployment and operational costs, access control solutions based on the use of biometric data are not in mainstream use.

Summary of the limitations encountered when using biometric data for access control:

1 Biometric data used in the identification of an individual will vary through time.
2 Biometric data have to be captured and converted into a reference sample for storage in a database. As they are digitized, the data become fragile (and hence modifiable), and must therefore be accorded the best possible protection. For each access request, the user's biometric data must be captured; this raises the problem of acceptance of the capture method and associated feeling of intrusion that is in many cases unwelcome.
3 Access control based on biometric data is not 100 per cent failsafe owing to the variability of the human sample to be analysed during the authentication process. According to the system in use, the probability of false positive or false negative identification can be relatively high and will depend on the technology used to record the biometric data and quality of the operation.

III.2.9 Protection and management of communication infrastructures

III.2.9.1 Protection

The physical layer (layer 1) can contribute to the security of transmissions by producing line scrambling, i.e. by transmitting non-significant information in order to mask a flow of relevant data within an uninterrupted flow of unimportant data. However, were it necessary to protect transmissions against passive eavesdropping through capture of the electromagnetic radiation induced by the signal carried via the transmission media, the latter would have to be fully isolated in Faraday cages. Clearly, such a protection measure will be implemented only where absolutely necessary.

The physical security of transmission media, splice boxes and connection equipment must be properly set up and maintained.

The transmission infrastructure has to be protected against any form of radiation that could compromise the data transmission process, and against passive (data snooping) or active (modification, destruction or creation of data) attacks.

Knowing how to protect user connections is of paramount importance. To this end, they have to be identified (who are the users?), located (where are they?) and their requirements identified (what are the application flows being carried?). By responding to the general question "who does what and where?", one can identify the various security requirements pertaining to the transport network.

Securing the transfer of data comes down to integrating the security process within the communication infrastructure, which must therefore be capable of assimilating that process in its entirety. This more often than not requires the updating of all of the routers – a situation which can in some cases lead to problems of router interoperability and change management.

Furthermore, encrypting data at the "network" level generates data packets that are larger than unencrypted packets, with the result that their transfer occupies more bandwidth and communication resources. Together with the fact that the encryption process increases the packet processing time, the implementation of security at this level can thus have a significant effect on network performance.

The main advantage of encryption at the network infrastructure level lies in the independence of the application and of the encryption mechanisms associated with the transfer, which are thus fully transparent for the user.

By contrast, transaction security at the application level (data encryption as close as possible to the data-handling application) modifies the application itself, the data being encrypted upstream of their delivery to the network protocol that will route them to their destination, where they will be decrypted by the receiving application server. It is during the dialogue set up phase between the application entities (a client and a server, for example) that a session key is authenticated and negotiated. The complexity of this phase can vary, so the establishment time is likewise variable. Once it has been completed, however, encryption is generally quite rapid. It is independent of the execution platform and communication infrastructure.

Protection at the level of the work sphere of a user implementing a distributed application no longer depends on the data carrier or network, but rather on the user's immediate environment. The difficulty of protecting applications lies in the fact that the protection afforded has to encompass the entire application environment, the user's workstation (and no longer just the application itself), and, by extension, the user's physical environment (access to premises, etc.).

Protecting applications comes down to the question of individual user rights in regard to workstations, applications and the physical area within which they operate.

The basic functions of the operating system installed on the user's workstation play a prominent part in this protection (other parties unable to take control during a session, automatic disconnection after a certain period of time, etc.). This also includes network card protection, secure-mode support for application protocols (transmission of protected files, secure messaging, etc.) and mirroring and duplexing operations (protection of data by duplicating them on disks, write-operation and equipment redundancy).

Securing the transport infrastructure or securing the application comes down to addressing the same issue at different levels:

- the processes and users have to be authenticated;
- the sender and recipient use an identical encryption/decryption algorithm;
- each communicating entity must be in possession of the algorithm and of the encryption/decryption keys;
- the encryption/decryption keys must be managed;
- the data must be formatted prior to transfer.

III.2.9.2 Management

Where properly implemented, system and network management activities can ensure the levels of availability and performance that are necessary to the achievement of security. They include network surveillance and anomaly or incident (e.g. intrusions) detection – tasks that make a major contribution to the overall security of the network and of the information system it serves.

Good network management helps to keep infrastructures, services and data available with a high degree of efficiency. Through network management, particularly configuration, performance and incident management, it is possible to achieve the security objectives of availability and integrity.

Furthermore, the aspect of network management known as accounting management makes available all of the data necessary not only for invoicing users but also for performing the surveillance and audit functions that are of key significance where security is concerned. This can serve in the verification of actions in the context of proof or of non-repudiation.

Network management also contributes to achieving the confidentiality objective insofar as it ensures the absence of snooping or unauthorized access to the data. The access control function that is a component of network management is essential to the operational implementation of security.

The performance, quality of service, availability and reliability of a network depend to a large extent on the quality of management of the routers and of the facilities that allow for route-switching

according to the status of the network and traffic routing requests. Updating the routing tables of major networks is a real operational headache for network administrators insofar as any changes to the values in the tables must be synchronized in order to avoid malfunctioning and losses of data in transit. The network management protocols are designed, among other things, to enable the updating of routing tables. Network management can contribute to router security by establishing secure access points during their configuration, generating alarms in the event of intrusion attempts, and securing the router management and monitoring centres.

It is thus crucial, in order to prevent unauthorized individuals from introducing changes, to be able to provide the necessary protection by blocking or detecting, among others, the following actions:

- the modification of addresses contained in routing tables, IP packets, etc.;
- the modification of routes and illicit copying of transported data;
- flow monitoring;
- diversion, modification and destruction of data packets;
- denial of service, router attack, network flooding, etc.

It is important to be able to secure the processes whereby data are routed through telecommunication networks. "Network" service providers must protect all entities involved in this process, particularly routers and name servers, such that the quality of the routing service meets the security criteria of availability (the service is operational), confidentiality (the data are delivered to the right recipients) and integrity (the data are not modified during transfer).

The delivery of data to authorized parties is not guaranteed by a network service, since the delivery service does not verify that data delivered to the right address are actually delivered to the parties authorized to receive them. For this, an additional check of the "access control" type has to be performed. If, moreover, the data are sent without encryption and tapped into en route, they will be intelligible to unauthorized third parties. Where the data are of a sensitive nature, they should be encrypted to make them unintelligible.

Monitoring of an information network entails constant observation of its functioning. The purpose of such monitoring is to ensure not only that the quality of service of the network is acceptable, but also to detect problems, incidents, errors and anomalies that degrade network performance and could jeopardize the security of the resources, with a view to responding both promptly and appropriately. Network monitoring allows for the tracing of actions and events so that they can be logged for subsequent analysis (this comes under the heading of auditing). It also helps to ensure resource availability by verifying that the network is functioning correctly. It is therefore a crucial function within the framework of network management, since it plays a part in performance, incident, configuration, user and security management.

PART IV

A COMPREHENSIVE APPROACH

Section IV.1 – Various aspects of the law regulating new technologies

IV.1.1 Personal data protection and e-commerce[47]

This section discusses personal data protection as it pertains to e-commerce in particular and identifies, on the basis of the situation in France and Switzerland, the main texts of law with which system administrators and security managers in organizations offering online e-commerce services must be familiar. The general principles governing the conduct of business in cyberspace can thus be extrapolated and adapted to developing countries.

IV.1.1.1 E-commerce: what's illegal "offline" is also illegal "online"

E-commerce can be discussed from the point of view of electronic business conducted either with consumers (business-to-consumer (B2C)) or between companies (business-to-business (B2B)). E-administration, for example, can be categorized in the same way, i.e. as electronic business with either citizens or other private or public institutions. This is an important legal distinction because commercial law tends to differentiate between transactions between companies and those with consumers.

In either situation, security, together with appropriate internet marketing and sales tactics conducted in compliance with an appropriate legal framework, is the cornerstone of e-commerce. By instilling trust based on security tools and respect for the law and thus creating a context that is conducive to the exchange of data, countries can encourage the general public to adopt information technology and telecommunication services and at the same time develop a true service economy.

The need to define an appropriate legal framework for the use of new technologies has seen the appearance of new laws drafted to supplement the existing legislation, much of which also applies to cyberspace. No matter what, however, what is illegal "offline" is just as illegal "online"! Cyberspace is an international and transborder space, and it is therefore very difficult to pin down who has jurisdiction to resolve the legal issues arising from e-commerce. This is why internet transactions must specify the offer's limits and provide accurate information on which courts have jurisdiction in the event of a dispute.

IV.1.1.2 The duty to protect

Personal data protection is a key aspect of e-commerce. Consumers must be informed about the nature of the data collected, used and communicated by online advertisers or businesses. They must know beforehand how the data concerning them is to be used and communicated and who else will have access to it. They must also be informed about the steps taken to protect that data. An effective privacy policy must be clearly expressed, easy to find and consult, visible and understandable when the business transaction takes place. It must be posted on the company website.

The company must also adopt adequate security measures for protecting the customer data collected and processed. It must take care to ensure that the third parties involved in transactions are able to meet security requirements.

IV.1.1.3 Respect for fundamental rights

The confidentiality of personal data and digital privacy are fundamental human rights.

The example of the European Directive

A European directive has existed on the subject since 1995, and since the early 1970s a number of countries have adopted national legislation on personal data protection and control of the use of public

Comment [P1]: Should a different heading style be used here? The paragraph directly under the heading says nothing about the European Directive, whereas the paragraphs under the following two headings discuss national legislation in terms of the European Directive. Perhaps the following two headings should be in a different character size, as they are more in the nature of subheadings.

47 This section was written in collaboration with Igli Taschi, Postgraduate Assistant at the University of Lausanne.

records containing nominative information, in order to avoid the risk that personal data will be stored unnecessarily or improperly.

The situation in France

One example is the French *Loi informatique et libertés* [Information Technology and Civil Liberties Act], which was published in January 1978 and revised in August 2004. The revised version was immediately applicable and introduced legal concepts adapted to the new forms of processing that have emerged in the information society and digital economy. It transposes Directive 95/46/EC of October 1995. Its aim is to reinforce the rights and protection afforded to physical persons and to strengthen the obligations incumbent on those processing data.

Legislation of this kind usually contains provisions relating to: the definition of nominative or personal data; rights of access, objection and correction; the purpose of the processing; data collection, storage and updating; the security of nominative records; the sale of data; the monitoring of crossborder data flows.

It is often supplemented by other legal instruments such as, in the case of France, the *Loi sur la sécurité quotidienne* [Daily Security Act] of 15 November 2001, which stipulates that data relating to an electronic communication, except billing information, must be deleted or rendered anonymous. What are known as "indirect" data (URLs visited, IP addresses of the servers consulted, message subject lines) must also be deleted.

The situation in Switzerland

Switzerland adopted the Federal Act on Data Protection on 19 June 1992 (Germany: Act of 21 January 1977; Belgium: Act of 8 December 1992; Canada: Personal Information Protection and Electronic Documents Act of 1982; United States: Privacy Act of 1974; 1988 Statute on Databases and Privacy).

Comment [P2]: The closest I could find was a California Database Protection Law.

In Switzerland, data protection is guaranteed first and foremost by the revised Federal Constitution that entered into force on 1 January 2000, article 13/2 of which reads: "*All persons have the right to be protected against the abuse of personal data*"[48].

The most important federal texts are the 1992 Data Protection Act and the implementing regulations of 14 June 1993. The Data Protection Act applies irrespective of the medium and technology used to collect and process the data. It applies both to private individuals and to the federal authorities, to physical persons and corporate entities, no matter how the data were processed. Article 3 defines personal data as "*all information relating to an identified or identifiable person"*. The Act also defines rules relating specifically to sensitive personal data and personal profiles.

Processing is broadly defined to include "*any operations relating to personal data, irrespective of the equipment and procedures used, and in particular the collection, storage, use, modification, communication, archiving or destruction of data"*. Article 2/2 nevertheless lists a number of areas in which the Act does not apply, such as pending legal proceedings and "*personal data that is processed by a natural person exclusively for personal use and that is not disclosed to a third party"* (subparagraph a). In a decision handed down on 5 April 2000, the Federal Tribunal ruled that the secrecy of telecommunications extended to electronic messages. Article 43 of the Swiss Federal Telecommunications Act also contains an obligation of secrecy: "*It is prohibited for any person who has been or is in charge of providing a telecommunication service to provide a third party with information on user traffic; such a person is also prohibited from enabling anyone else to communicate such information to third parties*". Article 44 of the Act, which is supplemented by articles 6 to 11 of the Federal Council's Ordinance on Postal Communications and Telecommunications Surveillance of 1 December 1997, establishes the procedure for and conditions of surveillance.

Comment [P3]: I have deleted the references to the Systematic Compendium of federal legislation (RS), because I don't think they're meaningful to English-language readers and they were not systematically included.

The Swiss rules governing the protection of private data on the internet are in many ways similar to those of the European directive on the same subject.

---

[48] Except where otherwise indicated, quotations from French or Swiss legal texts are translated from the original French by the ITU Translation Services.

IV.1.1.4 The economic value of legislation

Legislation on the handling of personal data and the protection of privacy in the electronic communication sector encourages organizations to manage their information technology and network security well (user data, communication and employee surveillance, save management, automated processing of personal data, etc.). Organizations must equip themselves with adequate means of security and control.

The economic value of the investments needed to guarantee a minimum level of security (physical and legal protection) varies with the organization's potential material losses and risks to its reputation and image. Legislation is thus an endogenous factor of security.

IV.1.2 E-commerce and contracting in cyberspace[49]

This section discusses various aspects of contracts as they pertain to business transactions conducted in cyberspace and identifies the main Swiss and European legislative texts regulating such transactions. The Swiss legislation and the principal European directives cited contain a number of basic principles that can be adapted to other countries and national laws.

IV.1.2.1 The choice-of-law issue

The first legal problem posed by e-commerce is the definition of the geographical area within which the electronic transaction takes place. The characteristics of the internet (international coverage, digital technology, mode of operation) are incompatible with the concept of geographical State borders, and information flows do not stop at international frontiers.

Data and services are accessible and can be provided remotely, no matter where the internet users and servers are located. The seller and the customers are often interacting from different countries. Knowing whose law is applicable in the event of a dispute is therefore vitally important and constitutes a key point of any offer. In this respect, transactions carried out over the internet must indicate the offer's limits and provide specific information on which courts have jurisdiction in the event of a dispute[50].

The contracting parties may agree on a choice of law and court of jurisdiction. In the absence of a choice-of-law clause, it has to be determined whether the contract comes within the scope of an international treaty such as the UNIDROIT Principles of International Commercial Contracts (1994), a form of *netiquette*; or the Hague Convention of 15 June 1955. International treaties are not binding, however, except where they have been expressly incorporated into the contract.

If neither of these solutions is possible, the rules of contract law apply.

In Swiss law, for example, these are set out in the 1987 Federal Act on International Private Law, article 1 of which stipulates[51]:

"[1] This Act regulates in an international context:

a. the jurisdiction of Swiss courts or administrative authorities;

b. the governing law;

c. the prerequisites for the recognition and enforcement of foreign decisions;

d. bankruptcy and composition with creditors;

---

49 This section was written in collaboration with Igli Taschi, Postgraduate Assistant at the University of Lausanne.

50 *Lex fori* is a private international law doctrine referring to the law of the country in which proceedings are to be conducted.

51 Source for the English version of the Federal Act on International Private Law: Jerome H. Farnum, B.A., J.D., *Swiss Federal Act on International Private Law, English Translation of Official Text*, Swiss-American Chamber of Commerce/Schulthess, Zurich, 2004 (revised edition).

e. arbitration.

[2] International treaties remain reserved."

The basic principle is as follows: the contract is subject to the law of the State with which it is *most closely* connected (art. 117/1 of the Act). Generally, this refers to the provider of the goods or services if explicitly so included in the general conditions, with one exception: article 120 of the Act, which regulates *Contracts with consumers*, stipulates that:

Comment [P4]: There is a mistake in the French: the citation is of article 120/1 and 120/2 .

"Contracts for a performance relating to normal consumption which is intended for the consumer's or for his family's personal use and not connected with his professional or commercial activities shall be subject to the law of the State in which the consumer has his ordinary residence if:

a. the offeror has received the order in that State;

b. in that State the conclusion of the contract was preceded by an offer or advertisement and the consumer has carried out the necessary legal acts for the conclusion of the contract, or

c. the offeror has prompted the consumer to go abroad and deliver his order there.

[2] A choice of law is excluded."

The content of the site, for example the language used or the currency listed, may be indicative of the offeror's target market and thus of the law applicable.

In cases in which the choice of law has not been determined by agreement between the parties, it is possible to file suit at the defendant's place of residence or headquarters location.

IV.1.2.2 Contracts concluded electronically

The rules applicable to contracts concluded electronically are on the whole the same as those that apply to so-called traditional contracts. A contract has been concluded when one party has made an offer and the other party has accepted that offer.

The European Directive

Directive 97/7/EC of the European Parliament and the Council of Europe, of 20 May 1997, deals with issues of distance sales and e-commerce. It stipulates that in good time prior to the conclusion of any distance contract, the consumer shall be provided with the following information:

a) the identity of the supplier and, in the case of contracts requiring payment in advance, his address;
b) the main characteristics of the goods or services;
c) the price of the goods or services including all taxes;
d) delivery costs, where appropriate;
e) the arrangements for payment, delivery or performance;
f) the existence of a right of withdrawal, except in the cases referred to in Article 6 (3) of the Directive;
g) the cost of using the means of distance communication, where it is calculated other than at the basic rate;
h) the period for which the offer or the price remains valid;
i) where appropriate, the minimum duration of the contract in the case of contracts for the supply of products or services to be performed permanently or recurrently.

The most important point concerning the conclusion of the contract relates to the definition of what constitutes an "offer" and what constitutes "acceptance of an offer". The goods "displayed" on an internet site with an indication of price, the associated advertising information, do not constitute an offer, but rather a call for bids within the meaning of the Swiss Code of Obligations, article 7 of which

provides that : "[2] *The sending of tariffs, price lists, and the like does not itself constitute an offer […]".*[52]

Sending an electronic message or an order form is also considered a call for bids.

A firm offer has been made, and the contract entered into, when the buyer accepts or clicks on "Purchase". He does not express intent to buy merely by visiting a site, any more than he does by entering a shop. On the other hand, the display of goods on a website constitutes an offer only if the seller indicates the stock on hand and that stock decreases subsequent to the order, or if the nature of the goods is such that the seller is always in a position to fulfil the order.

Comment [P5]: In fact, the text says that the contract is concluded at two different points: once when the buyer accepts the offer, and again when he receives electronic confirmation (see next paragraph).

The contract is concluded once the recipient of the service, i.e. the consumer wishing to purchase the goods displayed, receives electronic confirmation from the seller, but only if both documents are sent within a short time of each other. A distinction is made in this respect between a contract that becomes known to both parties at the same time and one that does not.

A contract inter absentes? *Yes but …*

A contract concluded over the internet is considered to be a contract *inter absentes*, which implies that the offer must be accepted within a reasonable time, as stipulated in article 5 of the Swiss Code Obligations:

"Art. 5:

b. Among persons not present

[1] If the offer is made to a person not present without setting a time limit, the offeror shall remain bound until such time as he should reasonably expect receipt of a reply dispatched properly and in due time.

[2] The offeror may thereby presume that his offer arrived in due time.

[3] If the declaration of acceptance was dispatched in due time, but arrived with the offeror only after expiration of that time, the offeror is bound unless he gives notice, without delay, of his intent not to be bound."

However, if the contract data are exchanged via a discussion forum, a chat room, instant messaging or internet telephony, the contract is considered to be known to both parties at the same time and acceptance must be immediate. Article 4/1 of the Swiss Code of Obligations stipulates: *"If an offer is made to a person present without the setting of a time limit, the offeror shall be deemed no longer to be bound if the offer is not accepted forthwith."*

IV.1.2.3 Electronic signature

The reader is able to check a message's integrity and thus ensure that it was not modified during transmission and ascertain who the sender is thanks to a system of asymmetric encryption; the sender can therefore not deny that he sent the message (concept of non-repudiation). These information security services are performed using a digital certificate to "sign" a digital document. By analogy with a handwritten signature, an electronic signature is a digital signature of data. Associated concepts are (private and public) encryption keys and certification authority (also known as a trusted third party, or TTP).

For the electronic signature to be considered as transposing the handwritten signature on a paper document into the digital world, it must be uniquely linked to the signatory, it must be capable of identifying the signatory and it must be created using means that the signatory can maintain under his sole control.

---

52 Source for the English version of the Code of Obligations: Rebecca Brunner-Peters, J.D., et al, *Swiss Code of Obligations*, Volume I, Contract Law, Articles 1-551, English Translation of the Official Text, Swiss-American Chamber of Commerce/Schulthess, Zurich, 2005 (revised).

Swiss law considers that electronic signatures have the same effect as written signatures. According to article 14 of the Code of Obligations:

"[1] A signature must be handwritten.

[…]

[2bis] A qualified electronic signature based upon a qualified certificate issued by a provider of certification services recognized within the meaning of the Federal Act on Electronic Signatures of December 19, 2003, shall be equivalent to a handwritten signature. Deviating legal or contractual provisions remain reserved".

Electronic signatures are governed by the Federal Act on Electronic Signatures of 19 December 2003, which defines electronic signature, describes the various forms it can take and lists those involved in implementing the signature mechanism and in issuing digital certificates.

"Art. 2 Definitions

For the purpose of this Act:

a. electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

b. advanced electronic signature means an electronic signature which meets the following requirements:

1. *it is uniquely linked to the signatory,*
2. *it is capable of identifying the signatory,*
3. *it is created using means that the signatory can maintain under his sole control,*
4. *it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;*

c. qualified electronic signature means an advanced electronic signature based on a secure arrangement for producing the signature within the meaning of art. 6/1 and 6/2, and on a qualified certificate that was valid at the time of its creation;

d. signature key means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

e. signature verification key means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;

f. qualified certificate means a certificate which meets the requirements laid down in art. 7;

g. certification service provider (provider) means an entity that certifies data in an electronic environment and issues digital certificates for that purpose;

h. recognition body means the entity which, according to the rules of accreditation, is authorized to recognize and oversee the providers;

[…]".

Electronic signature and the European Directive

Directive 1999/93/EC of 13 December 1999 on a European framework for electronic signatures distinguishes between three types of electronic signature depending on the degree to which the encryption mechanisms have been integrated and the level of security afforded.

Comment [P6]: The French text of the directive refers to only two kinds of electronic signatures: electronic signatures and advanced electronic signatures. I found no mention of the "signature électronique certaine" mentioned by the author in the last paragraph of this section.

There are various types of electronic signatures. First, a message can simply be "signed' without the signature being linked to the content of the message (the basic concept of electronic signature). In this case, anyone can "detach" the signature from the message and use it in the place of the signature's rightful owner. To overcome this shortcoming, a cryptographic function can be used to link the signature to the content of the message and to validate the sender's authenticity and the message's integrity on reception (concept of advanced electronic signature).

Lastly, the Directive discusses secure electronic signatures, which are based on the security provisions of Annex II on requirements for certification service providers issuing qualified certificates[53].

Comment [P7]: See Comment 6 above. Might these be the "secure signature devices" referred to in Annex III?

IV.1.2.4 Right of revocation

The ease with which items can be bought on the internet can incite some consumers to act hastily. The right of revocation is especially important in this context.

In Switzerland, the right of revocation is regulated in article 9 of the Code of Obligations, paragraph 1 of which sets out the following principle: "*If the offeror revokes his offer, and such revocation reaches the other party prior to […] the offer, […] the offer shall be deemed not to have been made*". The same principle applies to revocation of acceptance.

Right of revocation and the European Directive

In the European Union, the right of revocation is regulated by Directive 1997/7/EC of 20 May 1997, which stipulates that for any distance contract the consumer has a period of at least seven working days in which to withdraw from the contract without penalty and without giving any reason. If the supplier has failed to fulfil the obligations laid down in article 5, in particular as concerns the conditions and procedures for exercising the right of withdrawal, the period is three months.

IV.1.2.5 Managing disputes

Those involved in a dispute arising from a validly concluded contract will have to furnish evidence, whether the contract was concluded electronically or not. It is therefore always advisable to keep a record of the transaction, such as a copy of the electronic message or a screen print.

The situation in France

In France, article 109 of the Consumer Code does not specify what form the evidence must take in respect of B2B. E-mails, like paper documents, are therefore admissible. In respect of B2C, however, written proof is required for transactions in excess of a certain sum. The aim is to protect the average consumer, who has neither the capacity nor the legal resources to make his case in the event of a dispute with a commercial firm.

E-mails may, however, be admissible as evidence under the legal texts governing electronic signature. This means that an e-mail signed electronically will be considered to be valid proof if the above provisions on electronic signatures are respected.

Comment [P8]: I am not sure what is being referred to here. The EU directive? The Swiss Electronic Signature Act?

General conditions

Quite often distance contracts comprise general conditions that are an integral part of the contract. For these general conditions to be valid in the event of a dispute, they must be easy to access and consult online, and the customer must be clearly informed that they are part of the contract.

Online dispute resolution

Given the international nature of e-commerce, means have been developed for resolving disputes that bypass the traditional courtroom. The concept of online dispute resolution (ODR) was born of the desire to find immediate solutions to the non-performance of contracts concluded over the internet. This type of dispute resolution is based on conciliation, which involves negotiation, mediation and arbitration.[54] It is quicker, cheaper and more convenient for the users. The drawback is that it is based on codes of conduct and recommendations, also known as soft law (such as ICANN's Uniform Domain-Name Dispute Resolution Policy), making decisions difficult to enforce.

Comment [P9]: UNCITRAL has model laws on conciliation, but not on ODR.

---

53 http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

54 This mechanism for resolving disputes is the subject of a model law drawn up by the United Nations Commission on International Trade Law (UNCITRAL).

IV.1.3 Cyberspace and intellectual property[55]

IV.1.3.1 The branches of law protecting intellectual property

Intellectual property rights are protected by several branches of law, essentially:

- trademark law;
- copyright law;
- patent law;
- design and model law;
- the law protecting plant varieties;
- the law on semiconductor topographies;
- the law on public coats of arms and other public signs.

The law on unfair competition also affects intellectual property rights.

IV.1.3.2 Copyright and neighbouring rights

This is the branch of law that protects:

- the authors of literary and artistic works;
- performers, the producers of phonograms or videograms and audiovisual communication enterprises.

A work is a creation of the literary or artistic spirit; it is individual in nature, no matter what its value or intended purpose. Creations of the spirit include:

- works that use language, be they scientific, literary or other;
- musical and other acoustic works;
- works of fine arts, in particular sculptures and graphic works;
- works with a scientific or technical content, such as designs, plans, maps, or sculpted or modelled works;
- architectural works;
- works of applied arts;
- photographic, cinematographic and other visual or audiovisual works;
- choreography and mime;
- computer program (software);
- projects, titles and parts of works that are individual in nature.

Copyright entitles the author (the physical person who created the work) or the presumed author (the person who brings out the work until such time as the author has been designated) to moral and proprietary rights.

It is not necessary to deposit the work with an office or to register the rights, although some countries do have copyright deposits. Ideas cannot be protected unless they are set down because only the tangible work can be protected.

The term "moral rights" refers essentially to recognition of authorship and to the right to decide whether, when, in what way and under what name the work will be released, whereas "proprietary rights" relate to the use of the work (production and sale of copies, presentation, distribution, broadcast, etc.).

Transfer of ownership of the work, whether a copy or the original, does not imply transfer of copyright. Copyright is assignable and inheritable.

---

[55] This section was written in collaboration with Professor Sarra Ben Laggha, Tunis Polytechnic, lecturer at the University of Lausanne.

The term "neighbouring rights" refers to the rights of performers (the physical persons who perform a work or who participate artistically in its performance), of phonogram or videogram producers and of audiovisual communication enterprises.

IV.1.3.3 Trademark law

The purpose of a trademark is to distinguish the products and/or services of the trademark owner from those of other companies. The trademark identifies an object (and not a subject of law, which tends to be identified by a name or a company name).

It is not possible to obtain trademark protection for:

- signs that are in the public domain;
- forms that correspond to the nature of the product or that are inherent to its use;
- misleading marks;
- marks that are contrary to the law in force or to the principles of morality.

The mark must be registered to benefit from protection. A registered mark may be opposed if:

- it is identical to a mark previously registered for an identical product;
- it is identical or similar to a mark previously registered for similar products and/or services and there is a risk of confusion.

IV.1.3.4 Patent law

Patents are issued for industrial inventions. They cannot be issued for the obvious byproducts of technical developments, for plant or animal varieties, or for the essentially biological processes used to produce plants or animals; they can be issued for microbiological processes and the products obtained using such processes.

The patent is granted (under specific conditions) to the person who filed for it (the inventor, his successor in law or a third party who owns the invention on other grounds).

If several people invent the same product or process independently, the patent is granted to the person who filed first or whose filing has priority.

IV.1.3.5 Intellectual protection of a website

On the internet, and particularly in regard to websites, protecting the intellectual property of a website involves several branches of law[56]:

- regarding the domain name:
  - the registration of the domain name does not as such confer any specific exclusive right to the owner;
  - to protect the domain name, recourse must be had to the legal bases, which are:
    - trademark law;
    - the law governing company names;
    - the right to a name;
    - competition law;
- regarding the content of the site:
  - and specifically the distribution of works via the internet:
    - if the content was created specifically for the site, it is protected by copyright;
    - the digitization of an existing work and its online distribution are a form of reproduction that requires the consent of the author of the original;

---

56 See Philippe Gilliéron, *Propriété intellectuelle et Internet*, University of Lausanne (CEDIDAC No. 53), 2003.

– links to other sites: the use of a simple hyperlink infringes no exclusive right since it involves no reproduction; deep links (which direct the user to a specific page within another site, bypassing the site's home page) are another matter. The issue is whether the page in question is a work or not. As a rule, questions like this are regulated by competition law, the decisive criterion being the way in which the hyperlinks are used. Fair use is a key concept here.

IV.1.3.6 The complementary nature of technical and legal protection

Technical measures are being introduced to ensure respect for copyright. Legislation is being adopted to ensure those measures are not circumvented. Copyright thus enjoys legal protection, technical protection, and legal protection of the technical protection.

IV.1.4 Spam: a number of legal considerations[57]

IV.1.4.1 Context and nuisance

Broadly speaking, spam[58] refers to the sending of unsolicited messages. Its characteristics are as follows:

– the unsolicited messages are sent en masse, over and over;
– the message has a commercial purpose or is malicious in intent (phishing, taking over the computer, introducing malicious software such as a virus, adware, spyware, etc.);
– usually the addresses have been obtained without the owner's knowledge (in violation of the rules relating to the protection of personal data);
– the content is often illegal, misleading or harmful.

Because it is unsolicited, spam may in some circumstances be considered as an aggressive sales or advertising technique. Today, it takes the form not only of e-mail messages, but also of SMS on cell phones or on new multimedia equipment such as pocket PCs.

Spam generates costs for all internet users. These costs are generally related to the time it takes to process the messages and to the acquisition of spam-blocking tools. Spam also has a social cost, in terms of loss of user confidence, lower productivity, etc.

According to a study by the anti-spam firm Clearswift, published in the *Journal du Net* on 13 September 2005, spam falls into the following categories:

Types of spam	June 2005
Health	43.86%
Products	37.65%
Finance	9.06%
Pornography	5.32%
Phishing	1.41%
Betting	0.1%
Other	2.32%

57 This section was written in collaboration with Igli Taschi, Postgraduate Assistant at the University of Lausanne.

58 The word "spam" was originally a trademark registered by Hormel and stood for "spiced pork and meat", a kind of corned beef served to American soldiers during the Second World War. Its current use to refer to the sending of unsolicited e-mail apparently stems from a well-known Monty Python sketch in which the word "spam" was sung over and over, drowning out the voices of the other protagonists.

Spam can take the form of various kinds of "scams", one of the most common of which is the so-called Nigerian letter[59]. Phishing consists in sending a message purporting to come from a known institution, for example a bank, and inviting the receiver to connect to a fake site and to enter his access codes and other sensitive information, which will subsequently be used without his knowledge.

Spam can also be sent for destructive purposes or to block the recipient's in-box, making it impossible for him to receive messages and denying him the use of internet resources. Mail "bombing" comes in various forms: large messages that create problems of processing and temporary storage, vast numbers of messages, dispatch to a huge number of recipients in order to flood the server, or usurpation of the sender's address.

IV.1.4.2 Legal remedies for spam

Spam is covered by several branches of law, in particular data protection and unfair competition law; spammers also incur criminal liability.

The situation in Switzerland

Switzerland has no legal provisions explicitly regulating the use of spam.

From the point of view of data protection, according to the Swiss Federal Data Protection Commissioner and his document *Aide-mémoire concernant les messages publicitaires indésirables diffusés par courrier électronique (spams)*[60], electronic addresses are personal data that can be used to identify a person. Under article 12/3 of the Data Protection Act, "*As a general rule, a person's rights cannot be infringed if the person affected has made the data generally available to the public and has not expressly prohibited processing*". The processing of electronic addresses by a spammer constitutes an infringement of privacy (art. 4/3) that has been committed in bad faith (art. 4/2) and without the consent of the person concerned (art. 13/1). It therefore constitutes a violation of data protection.

"Art. 4 Principles

1 All processing of personal data must be undertaken in a lawful manner.

2 Processing must be conducted in good faith and must not be excessive.

3 Personal data may only be processed for the purpose either for which it was collected, or which is evident from the circumstances, or which is provided for by the law."

The Data Protection Act entitles the persons concerned to have recourse to the courts (art. 15, which refers to art. 28 ff of the Swiss Civil Code).

European Directive

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data sets the minimum standards for the constitution of records and data processing. Article 10 specifies that the data subject must know the purpose for which the data were collected and the identity of the controller.

The situation in France

In France, the Information Technology and Civil Liberties Act incorporates infringements of the right to privacy resulting from computer records or processing into the French Penal Code. The 2004 amended version of the Act introduced 14 articles laying down stiffer penalties for misuse of personal data.

---

59 The sender introduces himself as the heir to a recently deceased wealthy person, sometimes in a distant country. The "heir" claims to be having problems claiming his rights and proposes to use the victim's bank account in exchange for a large sum to compensate the victim for his trouble. The victim has to advance the money for the expenses related to the transaction. These are invariably attempts to swindle people out of their money.

60 See www.edsb.ch/f/doku/merkblaetter/spam.htm.

The situation in the United States

The United States is the biggest source of spam. On 1 January 2004, Congress enacted the CAN-SPAM Act, by virtue of which spammers can be prosecuted. The Act prohibits the "harvesting" of e-mail addresses from websites and bans programs that generate addresses by means of "dictionary attacks" that randomly combine letters and numbers.

Spam is also a problem from the point of view of unfair competition when it is used for advertising purposes.

Spam, advertising and unfair competition

Advertising on the internet is regulated by the general legal provisions on advertising, not by any specific legal framework. In November 2001, the Swiss Commission for Fair Play in Commercial Communications issued an advisory opinion on spamming, which it considers a particularly aggressive sales method. From the advertising point of view, such a method can only be used in compliance with certain basic rules, whether to conduct "traditional" business or e-commerce. Those rules are:

Comment [P10]: When you search for commission - suisse - loyauté on Google you get directed to the site of the "Commission pour la loyauté dans la Communication commerciale". There is no English version.

- the protection of young internet users;
- respect for the human being;
- respect for fair, truthful and honest advertising;
- respect for the legal privacy of internet users;
- ease of navigation.

Article 3 of the Swiss Federal Act against Unfair Competition stipulates that: "*Unfair competition occurs in particular when someone:*

[…]

b. provides inaccurate or fallacious information on himself, his business, his company name, his products, his works, his services, his prices, his inventory, his sales or business method or, by providing such information, provides a third party with an advantage over their competitors;

c. displays or uses inaccurate titles or occupational designations of a kind to make others believe he has certain distinctions or capacities;

d. takes measures of a kind to lead to confusion with another person's merchandise, works, services or business."

But it is letter h of article 3 that touches on the essence of the problem. It stipulates that: "*Unfair competition occurs in particular when someone:*

[…]

h. hampers the customer's freedom to decide by using particularly aggressive sales methods."

When used for commercial purposes with the intensity described above, spam may be covered by this article.

Spam and criminal intent

When spammers act with criminal intent they incur penal responsibility. Even if their message is commercial in nature, the content can lay them open to prosecution.

Spam and pornography

A majority of spam messages invite the reader to visit pornographic sites. This is a criminal offence under article 197 of the Swiss Penal Code, in particular if the message makes the content available to people who do not wish to receive it (art. 197/2) or to persons under the age of 16 (art. 197/1).

Spam, fraud, viruses and the sale of prohibited items

Fraud is a criminal offence under article 146 of the Swiss Penal Code. It is defined as obtaining a financial advantage from the victim for the purpose of self-enrichment. Seen from this angle, the "Nigerian letter" certainly qualifies as fraud.

Spam can sometimes be the best means of infecting machines with viruses. In Swiss law, if the introduction of a virus results in data corruption (if the victim's data are modified, erased or rendered unusable), the spammer can be prosecuted under article 144*bis* of the Penal Code.

Swiss law also prohibits the use of spam to sell medicines. Article 32 of the Swiss Law on Medicinal Products and Medical Devices prohibits advertising that encourages excessive, abusive or inappropriate use of medicinal products or advertising for medicinal products that cannot be sold on the Swiss market or that are obtainable only by prescription.

IV.1.4.3 Regulating spam

There are two opposing methods of regulating spam: the opt-in approach and the opt-out approach.

The opt-in approach, which is also called permission marketing, is more respectful of the internet user in that it consists in sending him only the targeted advertising which he has explicitly agreed to receive, by either selecting or deselecting a box; agreement may also be inferred, but in that case the visitor must be clearly informed of the commercial nature and of the consequences of subscription.

The opt-out method consists in "unsubscribing" and establishes the right to refuse to receive messages *a posteriori*. Every advertisement sent must give the recipient the possibility of unsubscribing from the list. Opt-out records can be constituted lawfully (for example by buying an opt-in list) or harvested using a random procedure.

Swiss and American lawmakers have chosen the opt-out approach, whereas the European Union tends to favour the opt-in approach, as demonstrated by Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Because spammers tend to act anonymously and from abroad, litigation is expensive and complicated and usually involves engaging a lawyer.

IV.1.4.4 Technical means of dealing with spam

Technical restrictions

The impact of spam can be limited by using technical means to restrict, for example, the number of recipients per message, the number of messages per source, and the number of messages per unit of time.

Blacklists

Blacklists work on the principle that mail can be classified using the server's reputation as a criterion. The reputation of a mail server that has recently delivered spam is tarnished in that it can be assumed that it will send more spam in the future. The server can be identified by its IP address.

Filters that use key words

Key-word filters block messages containing certain key words. They are ineffective because spammers can easily write their messages to get around the filters.

Profiling technology

Spam consists in sending massive numbers of identical messages. Profiling technology is used to profile the message content and compare it to a database of contents considered to be spam.

Policy to combat malicious software

A growing variety of "malware" (viruses, Trojan horses, bots, etc.) is being used to install e-mail servers on infected machines. The aim is to make it easier to propagate spam. Fighting spam also means hunting down malicious software.

Anti-spam software can help filter and block spam at the level of the e-mail server and thus limit its spread, but it is not always effective. Legitimate messages do not reach the recipients (concept of false positives) and genuine spam is allowed through (concept of false negatives).

Comment [P11]: I suspect the author confused false positives and negatives.

User attitude is a key aspect of the fight against spam. The scope of the problem can be limited, for example, if users treat messages knowledgably (they should be aware of the risk of identity theft, check what use will be made of their e-mail address before divulging it in an online form, use several e-mail addresses, avoid certain sites, learn not to open messages from unknown senders, delete spam without reading it, never reply and never to click on the hyperlinks in a spam message, etc.).

IV.1.4.5 Complementarity between technical and legal means

Because legal remedies have little impact on the spread of spam, a technological solution is required. Only by using both technical and legal means can the phenomenon of spam be combated. Every spammer who is discouraged by a rule of law or effectively prevented from spamming by a technical solution means millions and millions of unsent messages.

IV.1.5 Summary of the main legal issues relating to cyberspace[61]

IV.1.5.1 Legal status of the commercial internet

The legal status of the commercial internet is defined by the legal status of the information technology tools used.

In respect of e-mail, the issues are message content, mailbox address and the fact that an address can be used to identify – and steal – an identity, a distinctive sign or a company name. These points are regulated by each country's civil law.

In respect of websites, the concept of work, whether it is audiovisual or not, raises copyright issues. A hyperlink raises the question of content, responsibility, whether or not it is protected, and problems relating to search engines.

IV.1.5.2 Cybercontracts

Contracting in cyberspace raises not just legal issues. It also requires the existence of technical mechanisms for actually concluding the contract (tools and procedures used (globality, intangibility, delocalization)).

The following are important from the legal point of view:

- the offer, its status (distance or not), acceptance;
- advertising and soliciting, spam, etc;
- performance;
- online acceptance of the offer and the information technology used to indicate acceptance;
- the right to withdraw;
- choice of law and jurisdiction.

These points are governed by various European directives, namely:

- EC Regulation No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters;
- Directive 2000/31/EC on e-commerce;

---

61 This section was written in collaboration with Igli Taschi, Postgraduate Assistant at the University of Lausanne.

– Directive 98/34/EC of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations;
– Directive 97/7/EC on the protection of consumers in respect of distance contracts.

Also relevant are the 1996 UNCITRAL model law on e-commerce, the 1998 WTO Geneva Ministerial Declaration on global electronic commerce and the 1997 Joint EU-US Statement on electronic commerce.

IV.1.5.3 Electronic documents and signatures

Electronic documents that are signed electronically raise issues of validity. The aim is to be able to guarantee the legal validity of the signature in order to identify the signatory and to ascertain that he intended to sign the document and therefore takes responsibility for the content.

Examples of relevant legal texts are Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures (European Union), Law No. 59 of 15 March 1997 (Italy), the Electronic Signatures in Global and National Commerce Act of 30 June 2000 (United States) and the Electronic Communication Act of 25 May 2000 (United Kingdom).

IV.1.5.4 Electronic payments

Electronic payments that involve credit cards, cheques or electronic money can be intercepted by third parties, for example when the service supplier and the recipient communicate, and the relevant information misused.

See Directive 2000/46/EC of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions for one example of a legal text.

Comment [P12]: hard to know whether this is supposed to be a subheading or an example.

IV.1.5.5 Protection of domain names

Domain names are a new form of intangible asset that can have considerable commercial value. They must be considered from the point of view of how they relate to:

– trademarks and domain names;
– distinctive signs;
– business names and domain names.

In addition to national legislation on trademarks, names and patents, the US Anticybersquatting Consumer Protection Act (ACPA) is relevant.

IV.1.5.6 Intellectual property

Intellectual property on the internet raises issues relating to copyright, trademarks and patents. Suffice it to mention the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, and, in European legislation, the 1995 Green Paper on Copyright and Related Rights in the Information Society and Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonization of certain aspects of copyright and related rights in the information society.

IV.1.5.7 Protection of digital privacy

Spamming is an infringement of the right to digital privacy (see Directive 97/7/EC on the Protection of consumers in respect of distance contracts and Directive 97/66/EC concerning the Processing of personal data and the protection of privacy in the telecommunication sector, which prohibits direct marketing using spam).

IV.1.5.8 Other legal issues

Among the many other legal issues that have to be considered when defining an appropriate legal framework for use of the internet are questions such as:

– antitrust legislation (see the US Antitrust Guidelines for Collaboration among Competitors, April 2000);

– the liability of suppliers and technical intermediaries (to what extent the supplier is liable for the internet user's activities, criminal activities, child pornography, etc.);
– the inviolability of postal secrecy.

Section IV.2 – Prospects

IV.2.1 Educate – train – heighten awareness among all cybersecurity stakeholders

It is important to make all internet stakeholders aware of the importance of the security issues involved and of the basic measures which, if clearly stated and intelligently implemented, will strengthen user confidence in data processing and communication technologies, including the internet. The internet should be an asset for everyone and not of exclusive benefit to criminal activity.

Steps must be taken to foster a culture of and multidisciplinary approach to security and to control the risk that information technologies will be used to criminal ends. Both States and organizations must have a strategic vision of these problems.

Education, information and training must be provided in data processing and communication technologies, and not just in security and deterrents. Heightening awareness of security issues must not be limited to promoting a culture of security. There must first be an information technology culture. The stakeholders must also be given the means to learn to manage the technological, operational and information-related risks they incur in using the new technologies.

The virtual nature of the internet, and its recreational aspects, can blind especially young people and novice users to its considerable capacity to do harm. The consequences can be horrendous both for organizations (companies, administrative or community organizations) and individuals who fall victim to it. Controlling the technological risks means more than hunting down hackers or setting up technological barriers. The most serious consequences are sometimes due to sheer negligence resulting from incompetence, misconceived or poorly implemented technology, excessive authority for system administrators, mismanagement, etc.

IV.2.2 A new approach to security

Awareness of the digital world's vulnerability and of the difficulties inherent in controlling not only information and telecommunication technologies and infrastructures but also marketed security solutions should raise serious questions about our dependence on a hard-to-manage technology. Data being taken hostage by information technology systems is an eventuality which cannot be ignored.

It is wishful thinking to believe that technological and legal solutions will make up for conceptual errors and poor management of information technology and telecommunications, whether at the strategic, tactical or operational level. What is more, conventional security measures can protect the sensitive or crucial resources of people, organizations and States effectively only if they are implemented in ways that are transparent, verifiable and controllable.

Putting in place a comprehensive security approach incorporating prevention, protection, defence and reaction means adopting the human, legal, technological and economic means of doing so.

IV.2.3 The characteristics of a security policy

Generally speaking, a sound security policy is the outcome of a risk analysis and is comprehensive and coherent, providing a targeted response to security needs in a given context.

The policy must be:

– simple and easy to understand;
– implementable by trained and alert personnel;
– easy to implement;
– easy to maintain;

– verifiable and controllable.

Security policy should not be static. It must be periodically reviewed, optimized and adapted to developments in the context in which it is implemented. It must be possible to configure and customize it for user profiles, in the light of flows, the context and the geographical location of the stakeholders. Security policy will vary in time and space.

Security policy may be broken down into policies for access control, protection, crisis management, follow-up and optimization, trust.

IV.2.4 Identifying sensitive resources in order to protect them

A clearer picture is obtained of environments and their protection needs by producing a complete and accurate inventory of all the resources and players in the security chain. The values of different categories of resources are identified in order to determine how sensitive (or critical) they are, and thus which must be secured as a priority. The degree of sensitivity depends on the consequences if data are lost, altered or divulged. The more serious the consequences for the organization, the more sensitive and valuable the resource.

Each resource is viewed as a security target; the relevant risks and how they might arise (through user error, wrong parametering, accidentally, through malicious use, sabotage, logical attack, etc.), the inherent and applicable security mechanisms (configuration, parameters, etc.), and the technical and organizational constraints have to be identified in order to determine the technical and organizational feasibility of the security policy for each target.

IV.2.5 Objectives, mission and fundamental principles of cybersecurity

The objectives of cybersecurity are:

– confidentiality (no illicit access): to maintain the secrecy of the information and limit access to authorized entities;
– integrity and accuracy (no false information, no mistakes): to maintain the integrity and uncorrupted state of data and programs;
– availability (without delay): to maintain continuous, uninterrupted and unimpaired availability;
– longevity (no destruction): to store data and software for as long as required;
– non-repudiation and imputability (no dispute): to guarantee the origin, source, destination and truthfulness of an action;
– respect for digital privacy;
– authentication (no doubt as to the identity of a resource).

Comment [P13]: Or the identity of a source?

Each mission can be broken down into the following component activities:

– development of a security plan based on a prior risk analysis;
– definition of the vulnerability perimeter arising from the use of new technologies;
– continuous protection at a level commensurate with the risks incurred;
– implementation and validation of the security structure, measures, tools and procedures;
– monitoring, audit, control and development of the information system and its security;
– optimization of information system performance in line with the level of security required;
– alignment of needs with risks and costs.

The fundamental principles underpinning any action to promote cybersecurity are as follows:

– vocabulary (need to agree on a common language defining security);
– coherence (cybersecurity is the outcome when the tools, mechanisms and procedures needed to prevent, detect, protect against and correct damage arising from mistakes, maliciousness or natural factors are harmoniously integrated);

– managerial will (it is the responsibility of management to make available the means needed to implement and manage a cybersecurity plan);
– finance (the cost of security, of control measures, must be in proportion to the risk);
– simplicity, universality and discretion (the security measures must be simple, flexible, easily understood by the users; they must not be provocative so as not to lure potential attackers);
– change and continuity (security must be dynamic in order to integrate system modifications over time and changing needs and risks; the systems must be constantly operational);
– evaluation, control and adaptation (in order to ensure the level of security is in keeping with real needs).

IV.2.6 Success factors

IV.2.6.1 Strategy guidelines

Successful implementation of a security strategy requires:

– a strategic will;
– a simple, accurate, understandable and applicable security policy;
– publication of the security policy;
– centralized security management and some degree of automation of security procedures;
– trust and integrity among the people, systems and tools involved;
– procedures for registration, surveillance and audit;
– determination not to imperil resources;
– a legal framework that is applicable nationally and internationally;
– respect for legal constraints.

IV.2.6.2 Guidelines for internet users

The following guidelines represent simple, economical and relatively effective measures that internet users can adopt to make their resources and e-activities more secure[62]:

– switch off the computer when it is not in use;
– do not open e-mails from unknown senders;
– use a regularly updated anti-virus for minimal protection;
– do not divulge your password and change it often;
– do not divulge personal data on yourself or on others on the internet;
– never allow someone else to use your account to surf the internet;
– use encryption systems to protect data;
– do not visit immoral sites and do not download or circulate illegal programs or files;
– do not engage in acts on the internet that are prohibited and punishable in the non-virtual world (fraud, defamation, etc.);
– do not be complacent about the level of protection you have;
– bear in mind that, as in the non-virtual world, every act on the internet is carried out by an individual and that individual may not be honest.

IV.2.6.3 Guidelines for securing an e-mail system

The following basic guidelines can help protect an e-mail system.

Protect the server by:

– using anti-virus software;

---

62 Drawn from *Sentiment de sécurité sur Internet*, a post-masters dissertation on law, criminality and security written by Anne-Sophie Perron, working under S. Ghernaouti-Hélie, Lausanne, 2005.

– filtering messages using certain parameterable criteria (size, attachments, etc.);
– configuring it correctly;
– managing it efficiently so as to ensure availability;
– avoiding default maintenance accounts;
– providing it with physical protection.

In respect of the user:

– install, manage and impose the use of anti-virus software;
– define the rules for using the message system (do not open executable files, etc.);
– promote awareness of the potential risks;
– obtain a pledge of appropriate use of information technology resources;
– correctly configure each user's work station and message application;
– implement secure versions of the e-mail system;
– use encryption procedures for confidential messages and authenticate the sources.

IV.2.6.4 Guidelines for protecting an internet-intranet environment

The following basic guidelines on the use of firewalls will help protect internet-intranet environments:

– firewalls must be protected and secured against unauthorized access (concept of a trusted system with a secure operating system);
– all traffic (incoming and outgoing) must transit via the firewall;
– only traffic defined by the security policy as valid and authorized should be allowed to pass the firewall;
– the firewall must be configured to filter out everything that is not explicitly authorized;
– the firewall cannot at the same time be the company web server;
– if the data on the internal network are highly sensitive, access to the internet must be via machines that are not connected to the internal network;
– a firewall cannot secure the environment against attacks or illicit access that do not transit via it. It is ineffective against crimes committed within the company.

A firewall is not an anti-virus. It must therefore also be protected against viruses. In absolute terms, every system providing connectivity (e-mail servers, communication servers, etc.), every machine containing data (archive, database server, etc.), and every user workstation must be equipped with anti-virus software.

PART V

ANNEXES

Annex A – Glossary of main security terms[63]

Access control

Mechanism that serves to protect a resource (a service, system, data or program) from inappropriate or unauthorized use.

Accident

Unforeseeable incident causing prejudice to an entity.

Active attack

Attack which alters the targeted resources (affecting integrity, availability, confidentiality).

Anonymity

Characteristic of an entity whose name is unknown or which does not reveal its name, allowing an entity to use resources without being identified (incognito). Provision should be made to respect the wish of certain users who may have a valid reason for not revealing their identity when making statements on the internet, in order to avoid excessive restriction of their freedom of expression, to promote the free expression of ideas and information and ensure protection against unauthorized online surveillance by public and private entities. On the other hand, judicial and police authorities should be able to obtain information on individuals responsible for illegal activities, within the limits set by national law, the European Convention on Human Rights and other international treaties such as the Convention on Cybercrime.

Antivirus

Virus-detection programme.

Asset

Something that has a price and which represents a form of capital for its owner (concept of sensitive asset). In terms of security it is important to determine assets and to classify them by degrees of importance, in order to implement the requisite adequate measures of protection and thereby avoid losing them or at least minimize the adverse impact of their loss.

Asymmetric cryptographic algorithm

Algorithm based on use of a pair of keys (one for data encryption and the other for decryption).

Attack

Assault, aggression or action against and causing prejudice to individuals or resources. There are different types of computer-related attacks.

Auditability

The extent to which an environment lends itself to being analysed for the purposes of analysis and audit.

---

63 Taken and adapted from the glossary in "*Securité informatique et réseaux, cours et exercices corrigés*", S. Ghernaouti-Hélie, Dunod, 2006.

Auditor

Person conducting an audit.

Authentication

The act of authenticating. Authentication serves to confirm (or refute) that an action, a declaration, an item of information is authentic (original, genuine). Process used in particular to verify the identity of an entity and to ensure that it matches the previously recorded identity of that entity.

Authenticity

The character of that which is authentic. The characteristic allowing for attestation, or certification of validity. Often associated with the fact that an item of information or an event has not been altered, modified or falsified and that it was indeed produced by the entity claiming to have originated it.

Authority

A body with the power to exercise prescribed functions. Generally used to refer to a body in charge of issuing digital certificates.

Authorization

The act of authorizing, allowing, entitling. Permission to carry out certain actions, grant rights, obtain right of access to a service, information, a system, etc.

Availability

Security criterion whereby resources are available and usable order to meet requirements (no denial of authorized access to systems, services, data, infrastructure, etc.).

Backdoor, trapdoor

Usually refers to a portion of code incorporated into software that allows unauthorized entities to take control of systems, copy information, etc., without the owner's knowledge.

Backup plan

The set of technical and operational means foreseen to ensure the sustainability of information and the continuity of activities, no matter what the problems encountered.

Breach

Effect of or deterioration resulting from an act of aggression or attack whose impact may be: tangible (physical or material alteration, logic malfunction, disorganization of procedures, etc.); logical (non-availability, loss of integrity, breach of confidentiality); strategic (in particular as concerns finance, additional costs for hosting, transportation, telecommunications, expertise, purchase/rental of hardware and software, personnel, outsourcing, operating losses (profit margin, cash flow, customer losses), loss of funds or goods, etc.).

Bug

A programming error. By analogy, a conceptual or implementation defect that is revealed by malfunctions.

Certificate, public-key certificate

The set of data issued by a certification authority (trusted third party) and used to provide security services (confidentiality, authentication, integrity). A digital certificate uses public-key encryption. The certificate includes the value of the subject's public key, attested by the fact that the certificate is signed by the issuing certification authority.

Certification Authority (CA)

Trusted third party for the establishment, signature and publication of public-key certificates.

Chief security officer (CSO)

The person in charge of the security of information technology systems.

Cipher

Encryption algorithm used to transform plain text into ciphertext.

Ciphertext – see *Cryptogram.*

Compliance

Conformity, agreement with; compliance with standards.

Confidentiality

Keeping information and transactions secret. The nature of that which is secret. A security objective aimed at preventing the disclosure of information to unauthorized third parties and at protecting that information from reading, eavesdropping and illicit copying, whether accidental or deliberate, while it is being stored, processed or transported (concept of data confidentiality).

Cookies

Files written to internet users' hard file without their knowledge, when they access certain websites, and that collect data on the users with a view, in principle, to customizing the web services offered.

Countermeasure

System security function, measure, procedure or mechanism aimed at reducing the level of vulnerability and at countering a threat before it becomes a reality.

Cryptanalysis

The set of methods used to analyse previously encrypted information in order to decrypt it; cryptanalysis is therefore also referred to as “decoding”. The more robust the encryption system, the more difficult cryptanalysis becomes.

Cryptogram, ciphertext

Data that have been cryptographically transformed. Encrypted data, text or message. Data obtained by encryption.

Cryptographic algorithm

Algorithm used for data encryption in order to make the data confidential; it is based on a mathematical function and an encryption key.

Cryptographic period

Period of time during which a system's keys are not changed.

Cryptography

The mathematical application used to write information in such as a way as to render it unintelligible to those who do not have the means of decrypting it. See *Encryption*.

DDoS (distributed denial of service)

A saturation (or denial of service) attack launched from several systems simultaneously.

Digest

The string of characters formed when a hash function is applied to a series of data.

Digital signature

By analogy with a handwritten signature, the digital signature obtained via an asymmetric encryption algorithm is used to authenticate the sender of a message and to ascertain the message's integrity.

Direct losses

Identifiable losses resulting directly from a security defect.

Dissuasion

Means used to deter malicious attackers from carrying out an attack, by persuading them that what they stand to gain is negligible in comparison to the losses that the system they threaten to attack could inflict.

DoS (denial of service)

A saturation attack aimed at causing the target to collapse so that it can no longer perform as expected.

Efficiency

The quality of that which has the anticipated effect, which produces useful results. Characteristic of security measures that are relevant and have a genuine capacity to protect a resource.

Emergency plan

The set of technical and organizational means foreseen to respond optimally to a serious incident that is harmful to the organization and affects the smooth conduct of operations.

Encryption, encipherment

The cryptographic transformation of data (cryptogram) to guarantee confidentiality. Encryption consists in making data incomprehensible to anyone who does not have the decryption key. Plain text is encrypted using an algorithm and an encryption key in order to create ciphertext, which can be decrypted using the corresponding decryption key (except in cases where the encryption is irreversible). The inverse operation is called decryption, or decipherment.

Ethics

The discipline dealing with what is good or bad. The set of moral rules adopted by a community.

Failure

Malfunction, breakdown making the resource unavailable.

Firewall

Hardware or software used to isolate or mask resources, to filter data, to control flows, and thus to protect the private information environments of organizations connected to the internet.

Flaming

Technique which consists in sending a large number of inappropriate messages in order to undermine the credibility of a discussion group.

Flooder

A malicious program used to slow communications between the access provider and the internet user or to disconnect the user.

Hack, hacker

The act of entering a system illicitly. A person who, for whatever reason, enters someone else's system without authorization and unlawfully. The attack may be passive or active.

Hacking

The series of operations used to breach an information technology system.

Hash function

In the context of encryption, this is also referred to as the digest function. Starting from the message data, it generates a message digest, i.e. a kind of digital fingerprint, which is shorter than the original message and incomprehensible. This is then encrypted with the sender's private key and attached to the message to be transmitted. On receipt of the message and its fingerprint, the recipient decrypts the fingerprint with the sender's public key, recalculates the fingerprint from the message received using the same hash function, and compares it with the fingerprint received. If the result is the same, the recipient has thus verified the sender's identity and is assured of the message's integrity, since, if the message is altered, even only slightly, its fingerprint is significantly modified.

Identification

The process by which one can recognize a previously identified entity.

Identity

Information used to designate and distinguish, if possible in a unique and unambiguous fashion, a specific entity within a naming domain.

Impact

Expresses the level of consequences produced by an attack (**financial impact**: cost of the attack; **logic impact**: undermines availability, integrity, confidentiality; **strategic impact:** detrimental to the organization's survival; **tangible impact**: a real, directly observable effect).

Impact gravity

Assessment of the seriousness of an incident, weighted by its frequency of occurrence. It is important to quantify impact gravity in order to pinpoint and prioritize security requirements, for example: no/negligible impact (0), little impact (1), moderate impact (2), strong impact (3), disastrous impact (4).

Imputability

The quality that makes it possible to impute an operation to a user at a given time with certainty. The fact of being able to identify who is to be held accountable in the event of a violation of the rules.

Indirect losses

Losses generated indirectly by a security defect.

Integrity

The state of something that has remained intact. Security criterion which, if met, makes it possible to ensure that a resource has not been altered (modified or destroyed) in unauthorized fashion.

Intranet

An organization's internal, private network using internet technology and usually insulated from the internet by firewalls.

Intrusion detection system (IDS)

System for detecting incidents that could result in violations of security policy and diagnosing potential breaches.

IPSec (Internet Protocol security)

A version of IP that offers security services. IPSec opens a logical communication channel (IP tunnel) between two correspondents on the public internet. The tunnel ends are authenticated and the data transported through them can be encrypted (concept of encrypted channel or virtual network).

IPv6 (Internet Protocol version 6)

Update of IPv4, incorporating, *inter alia*, built-in mechanisms for implementing security services (authentication of source and destination entities, confidentiality of transported data).

Key

Encryption or decryption key, usually a mathematical value for an encryption algorithm. Unless they are public, encryption keys should not be disclosed: they are a secret means of protecting another secret (the information that was encrypted in order to ensure its confidentiality).

Key management

Management of encryption keys; generation, distribution, archiving, destruction of keys in keeping with security policy.

Logic bomb

A malicious program triggered by a specific event (such as a birthday date) and intended to harm the system in which it is lodged.

Loss of essential service

Total or partial unavailability or malfunction of the resources required for a system or organization to operate properly.

Malevolent

Said of hostile actions liable to harm an organization's resources, which may be committed directly or indirectly by people inside or outside the organization (theft of hardware, data, disclosure of confidential information, illicit breaches, etc.).

Malware

A generic term for a program such as a virus, worm or Trojan horse, or any other form of attack software that acts more or less independently.

Masquerade

Type of attack based on system decoys.

Non-repudiation

The capacity to prevent a sender from subsequently denying having sent a message or performed an action. Guarantees the availability of evidence that can be submitted to a third party and used to prove that an event or action occurred. Evidence that a message was sent by a specific person at a given time, without having been subsequently modified. Such evidence should be verifiable by a third party at any time. Without non-repudiation, information senders and recipients could deny that they received or sent the information in question.

No-opt

Service in which the customers cannot choose how the information on them is used (possibility that their right to data privacy will be infringed).

Notarization

Registration of data for the purposes of evidence.

One-way hash function

A function that can be used to calculate the data fingerprint, but not to generate data that have a specific fingerprint. This function must avoid producing collisions, i.e. the same profile being generated from different messages.

Passive attack

Attack which does not alter a target (passive listening, breach of confidentiality).

Password

Confidential information to be produced by an authorized user in order to prove his identity during the authentication procedure for requesting access to a resource.

Patch

A software update aimed at repairing a weak spot identified after the software was installed.

Penetration tests

These are used to analyse and test the degree to which systems are protected and the robustness of security mechanisms.

Phreaking

The illegal use or misuse, at the individual's or the operator's expense, of telecommunication services (by a phreaker).

Prevention

Set of measures taken to avert a danger, a risk, aimed at preventing threats from materializing, at reducing the frequency of incidents with a view to protection.

Privacy protection

Protective measures to ensure that information on internet user activities is not disclosed to any unwanted parties and is not used for purposes other than those to which the owner has consented. This refers to the right of individuals to verify the information concerning them that can be collected either directly, or indirectly by observing their internet behaviour and the sites they visit.

Private key

Key used in asymmetric encryption mechanisms (public-key encryption) that belongs to an entity and that must be kept secret.

Privilege-management infrastructure (PMI)

Infrastructure supporting management of privileges, authorizations and clearances.

Protection

The act of protecting, the state of being protected. Is said of a security measure that helps detect, neutralize or reduce the effects of an attack.

Public key

Generally speaking, in asymmetrical cryptography, an entity's public key must be made available to those who wish to send it encrypted data so that it can decrypt the data using the corresponding private key.

Public-key cryptography

An asymmetric encryption system that uses two-key ciphers, or a key pair: one is a secret private key, the other a public, publishable key. The two keys are complementary and indissociable. It is not possible to use the mathematical relationship between them to calculate the private key.

Public-key infrastructure **(PKI)**

Infrastructure supporting the implementation of asymmetric (public key) encryption, including, *inter alia*, management and distribution of encryption keys and digital certificates.

Reliability

A system's capacity to function without incident for a given period of time.

Repudiation

The fact of denying that one has taken part in all or part of an exchange.

Revocation

Notification that a private key has lost its integrity. The corresponding public key certificate must no longer be used. In respect of contracts, also refers to the right to withdraw an offer or acceptance of an offer.

Risk

The relative likelihood that a threat will materialize, measured in terms of probability and impact.

Risk analysis, risk assessment

Process of identifying and assessing risks (estimation of probability of occurrence and impact).

Risk management

Ongoing process of risk assessment conducted by an organization in order to control risks and keep them to an acceptable level. Can be used to determine the security policy best adapted to protecting the organization's assets.

Sabotage

A malicious act, vandalism, deliberate harm aimed at preventing an organization, an infrastructure, a service or a resource from operating normally; can result in losses.

Safety

The quality of that which is not harmful.

Secure sockets layer (SSL)

Software used to secure exchanges on the internet, developed by Netscape and supported by most web browsers on the market.

Security

The situation in which someone or something is not exposed to any dangers. Mechanism aimed at preventing a harmful event or at limiting its repercussions. **Physical security**, for example, refers to the measures taken to protect environments physically or materially, whereas **logic security** refers to software procedures and means of protection.

Security administrator

Individual responsible for establishing or implementing all or part of a security policy.

Security audit

A methodical analysis of all security components, players, policies, measures, solutions, procedures and means used by an organization to secure its environment, conducted with a view to monitoring compliance, evaluating the fit between the organizational, technical, human and financial resources deployed and the risks incurred, and optimizing, rationalizing and enhancing performance.

Security measures

All technological, organizational, legal, financial, human, procedural and resources and means of action used to meet the security objectives established by the security policy. They are usually categorized by their functional role (preventive measures, protective measures, deterrent measures, etc.).

Security need

For an environment requiring protection, the identification and expression of levels of availability, integrity and confidentiality associated with the resources and values requiring protection.

Security policy

Security frame of reference established by an organization, reflecting its security strategy and laying down the means of implementation.

Sensitivity

Characteristic of an entity indicating its value or importance.

Session key

Secret key generated using an asymmetric encryption system when the correspondents open a working session, and whose life span is limited to the session; the key is used to encrypt large volumes of data using a symmetric encryption algorithm.

S-http

Secure version of the http protocol that allows secure exchanges between a customer and a web server.

Sniffer

Software used to eavesdrop on data being transported on a network.

Sniffing

The act of passive eavesdropping in order to harvest connection parameters that are then used without the knowledge of their legitimate owners to commit unauthorized breaches.

Social engineering

Techniques, procedures and measures used by malicious attackers, who usually take advantage of the users' credulity to, *inter alia,* obtain their passwords and connection parameters and usurp their digital identity, in order to trick and breach the system by pretending to be authorized visitors.

Spammer

Someone who engages in spamming.

Spamming

Technique involving the sending of unsolicited messages to an electronic message system.

Spoofer

Someone who engages in spoofing.

Spoofing

Technique used to usurp IP addresses in order to breach a system.

Spyware

Program that sends sensitive information from the infected computer to the attacker.

Steganography

Technique used to hide an item of information within another in order to transport or store it covertly. Watermarking is a steganographic application that consists in placing indelible marks on an image.

Threat

Sign, indication, harbinger of a danger. Action or event liable to take place, to turn into an attack on an environment or resource and breach security.

Traffic analysis

Observation and study of information flows between source and destination entities (presence, absence, amount, direction, frequency, etc).

Trapdoor – see *Backdoor*.

Trojan horse

A malicious program hidden within a legitimate program and introduced into systems for the purpose of hijacking them (theft of processor time, corruption, modification, destruction of data and programs, malfunctions, eavesdropping, etc.).

Trust

Assured reliance on someone or something (a qualitative, subjective, highly relative criterion).

User charter

Document drawn up by an organization listing the rights, duties and responsibilities of its employees in respect of the use of the information technology and telecommunication resources it makes available to them, signed by the parties concerned.

User profile

List of user attributes that help to manage the network and systems to which the users are connected (identification and authentication parameters, rights of access, authorizations and other useful information) for the purposes of access control, billing, etc.

Virtual private network (VPN)

This concept refers to the use of IPSec to open a secure private communication channel over a non-secure public network. It is often used by an organization to connect its various sites via the internet while guaranteeing the confidentiality of the data exchanged.

Virus

Malicious program introduced into a system without the users' knowledge. The program has the capacity to duplicate itself (either in identical form or, in the case of a polymorphic virus, by

mutating), to damage the environment in which it is executed and to contaminate other users with which it is in contact. There are different kinds of viruses, depending on their signature, their behaviour, how they reproduce, how they infect machines, the malfunctions they cause, etc. **Worms, Trojan horses** and **logic bombs** are malicious codes belonging to the generic family of viruses.

Vulnerability

A security defect that could result in an intentional or accidental breach of security policy.

Annex B – Table of contents of ISO/IEC standard 17799:2005, which serves as a reference for security management

6.2.1 Identification of risks related to external parties

6.2.2 Addressing security when dealing with customers

6.2.3 Addressing security in third party agreements

7 ASSET MANAGEMENT

7.1 RESPONSIBILITY FOR ASSETS

7.1.1 Inventory of assets

7.1.2 Ownership of assets

7.1.3 Acceptable use of assets

7.2 INFORMATION CLASSIFICATION

7.2.1 Classification guidelines

7.2.2 Information labelling and handling

8 HUMAN RESOURCES SECURITY

8.1 PRIOR TO EMPLOYMENT

8.1.1 Roles and responsibilities

8.1.2 Screening

8.1.3 Terms and conditions of employment

8.2 DURING EMPLOYMENT

8.2.1 Management responsibilities

8.2.2 Information security awareness, education, and training

8.2.3 Disciplinary process

8.3 TERMINATION OR CHANGE OF EMPLOYMENT

8.3.1 Termination responsibilities

8.3.2 Return of assets

8.3.3 Removal of access rights

9 PHYSICAL AND ENVIRONMENTAL SECURITY

9.1 SECURE AREAS

9.1.1 Physical security perimeter

9.1.2 Physical entry controls

9.1.3 Securing offices, rooms, and facilities

9.1.4 Protecting against external and environmental threats

9.1.5 Working in secure areas

9.1.6 Public access, delivery, and loading areas

9.2 EQUIPMENT SECURITY

9.2.1 Equipment siting and protection

9.2.2 Supporting utilities

9.2.3 Cabling security

9.2.4 Equipment maintenance

9.2.5 Security of equipment off-premises

9.2.6 Secure disposal or re-use of equipment

9.2.7 Removal of property

10 COMMUNICATIONS AND OPERATIONS MANAGEMENT

10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES

10.1.1 Documented operating procedures

10.1.2 Change management

10.1.3 Segregation of duties

10.1.4 Separation of development, test, and operational facilities

10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT

10.2.1 Service delivery

10.2.2 Monitoring and review of third party services

10.2.3 Managing changes to third party services

10.3 SYSTEM PLANNING AND ACCEPTANCE

10.3.1 Capacity management

10.3.2 System acceptance

10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE

10.4.1 Controls against malicious code

10.4.2 Controls against mobile code

10.5 BACK-UP

10.5.1 Information back-up

10.6 NETWORK SECURITY MANAGEMENT

10.6.1 Network controls

10.6.2 Security of network services

10.7 MEDIA HANDLING

10.7.1 Management of removable media

10.7.2 Disposal of media

10.7.3 Information handling procedures

10.7.4 Security of system documentation

10.8 EXCHANGE OF INFORMATION

10.8.1 Information exchange policies and procedures

10.8.2 Exchange agreements

10.8.3 Physical media in transit

10.8.4 Electronic messaging

10.8.5 Business information systems

10.9 ELECTRONIC COMMERCE SERVICES

10.9.1 Electronic commerce

10.9.2 On-Line Transactions

10.9.3 Publicly available information

10.10 MONITORING

10.10.1 Audit logging

10.10.2 Monitoring system use

10.10.3 Protection of log information

10.10.4 Administrator and operator logs

10.10.5 Fault logging

10.10.6 Clock synchronization

11 ACCESS CONTROL

11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL

11.1.1 Access control policy

11.2 USER ACCESS MANAGEMENT

11.2.1 User registration

11.2.2 Privilege management

11.2.3 User password management

11.2.4 Review of user access rights

11.3 USER RESPONSIBILITIES

11.3.1 Password use

11.3.2 Unattended user equipment

11.3.3 Clear desk and clear screen policy

11.4 NETWORK ACCESS CONTROL

11.4.1 Policy on use of network services

11.4.2 User authentication for external connections

11.4.3 Equipment identification in networks

11.4.4 Remote diagnostic and configuration port protection

11.4.5 Segregation in networks

11.4.6 Network connection control

11.4.7 Network routing control

11.5 OPERATING SYSTEM ACCESS CONTROL

11.5.1 Secure log-on procedures

11.5.2 User identification and authentication

11.5.3 Password management system

11.5.4 Use of system utilities

11.5.5 Session time-out

11.5.6 Limitation of connection time

11.6 APPLICATION AND INFORMATION ACCESS CONTROL

11.6.1 Information access restriction

11.6.2 Sensitive system isolation

11.7 MOBILE COMPUTING AND TELEWORKING

11.7.1 Mobile computing and communications

11.7.2 Teleworking

12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

12.1.1 Security requirements analysis and specification

12.2 CORRECT PROCESSING IN APPLICATIONS

12.2.1 Input data validation

12.2.2 Control of internal processing

12.2.3 Message integrity

12.2.4 Output data validation

12.3 CRYPTOGRAPHIC CONTROLS

12.3.1 Policy on the use of cryptographic controls

12.3.2 Key management

12.4 SECURITY OF SYSTEM FILES

12.4.1 Control of operational software

12.4.2 Protection of system test data

12.4.3 Access control to program source code

12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

12.5.1 Change control procedures

12.5.2 Technical review of applications after operating system changes

12.5.3 Restrictions on changes to software packages

12.5.4 Information leakage

12.5.5 Outsourced software development

12.6 TECHNICAL VULNERABILITY MANAGEMENT

12.6.1 Control of technical vulnerabilities

13 INFORMATION SECURITY INCIDENT MANAGEMENT

13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES

13.1.1 Reporting information security events

13.1.2 Reporting security weaknesses

13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

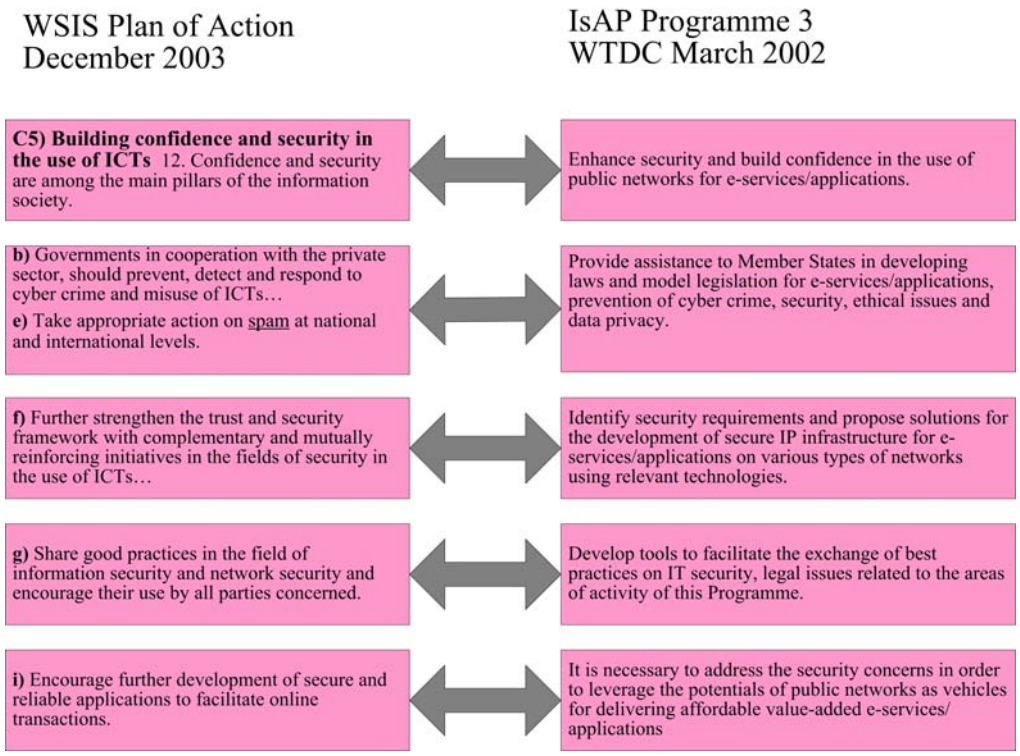
13.2.1 Responsibilities and procedures

13.2.2 Learning from information security incidents

Annex C – Mandate and activities of ITU-D in cybersecurity

For further information:
http://www.itu.int/ITU-D/e-strategy/e-security

The strong synergies between the priorities of this Programme in cybersecurity and the Geneva WSIS Plan of Action can be seen in the almost one-to-one mapping shown below. The Tunis Agenda of 2005 identified ITU as the lead organization to facilitate and moderate actions aimed at the implementation of the Geneva Plan of Action in the domain of building confidence and security in the use of ICT. Within ITU-D, cybersecurity for ICT applications is one of the six priority domains in Istanbul Action Plan Programme 3.



Activities of ITU-D in security and confidence

Through WTDC-02 Istanbul Action Plan Programme 3, ITU assists developing countries in a number of ways: implementing projects, guidance in the formulation of national policies and strategies, elaboration of appropriate legislation promoting the development and use of cybersecurity and trust for the conduct of critical transactions in domains such as health, education, commerce and communication between government agencies and officials.

Projects delivering security and trust services for ICT applications

Projects using advanced security and trust technologies based on public key infrastructure (PKI), including biometric authentication, smart cards, ITU-T X.509 digital certificates and digital signature

techniques, have been deployed and are operational in Bulgaria, Burkina Faso, Cote d'Ivoire, Cambodia, Georgia, Peru, Senegal, Paraguay and Turkey (business sector). For 2004-2005, there are ongoing and implemented activities related to cybersecurity technologies for ICT applications in Afghanistan, Barbados, Bhutan, Bulgaria (Phase III), Cameroon, Jamaica, Rwanda, Turkey (e-health and e-government) and Zambia (for e-signatures).

Thanks to ITU, several developing countries have for the first time become actively involved in the deployment and use of services aimed at building security and trust, thereby extending the benefits of ICTs beyond commercial applications to societal ones such as government and health.

In Georgia, the ITU project addresses its challenges by delivering cost-effective solutions for the secure transmission, access and processing of digitized government documents, thereby increasing the efficiency and transparency of government services. Senior level officials of the Ministry of Transport and Communications of Georgia will be provided with solutions to enhance work-flow automation and enable officials to digitally sign and disseminate official documents, thus replacing the slow and rather expensive paper-based methods. Authorized access to sensitive documents will be made possible through security and trust solutions to establish the identities of authorized personnel within the ministry.

In Paraguay, the ITU project assisted in the implementation of a platform providing a secure and trusted internet-based mechanism for operators and service providers to exchange sensitive information (such as income declarations) in electronic format with the National Regulatory Agency. The project uses ICT tools to streamline the process of issuing licences to operators of public telephones and increases efficiency in the business process of the regulator.

Assistance was provided in the establishment of national policy frameworks on the use of digital certification and the operations of certification authorities. ITU assistance has also included the definition of technology specifications and policy guidance for the implementation of a national platform in Jamaica and Barbados for issuing and managing digital certificates, providing strong authentication services and ensuring the security and trust for e-government and e-business transactions.

In Cameroon, the ITU project enables the secure transmission of sensitive government documents via the internet and provides internet-based online government services to citizens in urban and remote areas where the physical administrative infrastructure does not exist. Based on electronic signature and encryption technologies, solutions such as strong authentication, data confidentiality, data integrity and non-repudiation make it possible to address some of the cybersecurity threats including identity theft.

In Bulgaria, ITU assistance in the implementation of an e-security platform enables highly secure communication between the Ministry of Transport and Communications, Ministry of Finance, the Council of Ministries and the Communications Regulation Commission (CRC) using public key infrastructure (PKI) and PKI-enabled applications. It permits a secure, efficient and cost-effective interaction between senior level government officials, thereby supplementing face-to-face meetings and increasing productivity. All data exchanged between the participating officials is secured, digitally signed through the use of data confidentiality, non-repudiation, data integrity and strong authentication techniques.

The strategic goal of the project in Turkey is to improve healthcare services by developing a secure health information medium that enables healthcare providers (primary and secondary healthcare), health professionals and citizens an easy and safe access to health related information by using latest ICTs. The cornerstones of the project are development of primary healthcare information systems supporting the family doctors' system, implementation of electronic health records and development of interoperable systems between healthcare service providers including primary healthcare centers, hospitals and public/private insurance agencies.

Addressing national and regional policies and strategies

A workshop was organized for 128 countries to share information and best practices in security and trust technologies and policies for e-business.

ITU has organized workshops and seminars addressing technology strategies for e-security in number of countries (e.g., Azerbaijan, Cameroon, Chile (for Mercusor States), Mongolia, Pakistan, Paraguay, Romania, Seychelles, Syria and Uzbekistan. Security and trust were amongst the main topics discussed at the November 2004 ITU Regional E-government and LP Symposium for the Arab region which resulted in the Dubai Declaration emphasizing the need for continued ITU activities in cybersecurity for e-applications and services.

A cybersecurity manual is currently being developed to assist developing and least developed countries in building local capacity and raising awareness on some of the key challenges in security for the information society. This manual will explain some main problems such as spam, malware (viruses, worms, Trojan horses), data privacy, lack of authentication, need for data confidentiality and data integrity. Scheduled to be completed in November 2005 other subjects to be covered include guidelines and best practices on legislation for cybersecurity and examples of methods that have been applied to protect critical infrastructure. For 2005, ITU-D has organized the following events:

1 ITU/EU (ENISA) Regional Seminar on cybersecurity for CEE, CIS and Baltic States;
2 Subregional Seminar on cybersecurity for information and communication networks:
3 WSIS Thematic Meeting on cybersecurity organized by ITU-D, ITU-T and the General Secretariat.

Assistance in the formulation of appropriate legislation

ICT applications require an appropriate legal and policy environment to address, in particular, data privacy, prevention of cybercrime, security, ethical issues, electronic signatures, certification authorities and electronic contracts in order to create confidence, protect the rights of parties and encourage the use of ICT applications.

ITU has provided assistance to the following countries in the elaboration of model legislation covering areas such as e-commerce, data protection, online transactions, digital certification, authentication and encryption: ASETA Member States (Bolivia, Columbia, Ecuador, Peru and Venezuela), Burkina Faso, Cape Verde, Mauritania, Mongolia and Tanzania.

As part of its efforts to provide guidelines and case studies to developing countries on legislation for data privacy, ICT applications, prevention of cybercrime, a report based on research and analysis containing practical examples on how some countries have addressed legislation on the prevention of cybercrime is now available. The work was undertaken by Ms Michela Menting Yoell of the University of Essex, United Kingdom, during a three-month internship at ITU/BDT E-strategies Unit as part of the requirements for an LLM degree in information technology, media and e-commerce. A PDF version of this report can be downloaded from here: Research on legislation in data privacy, security and the prevention of cybercrime.

Annex D – Main ITU-T Questions relating to security under study in the 2005-2008 study period

Extracted from
http://www.itu.int/ITU-T/studygroups/com17/questions.html

Questions assigned to ITU-T Study Group 17 (study period 2005-2008)

Study Group 17: Security, languages and telecommunication software

Question 2/17 – Directory services, directory systems, and public key/attribute certificates

Directory services

a) What new service definitions and profiles are required that can take advantage of widely supported Directory technologies, e.g. X.500 and LDAP?

b) What changes to the E and F-series of Recommendations and/or what new Recommendations are required to specify enhancements to, and to correct defects in, existing Directory service definitions and profiles?

Directory systems

a) What enhancements are required to the Directory to better support current and potential users of the Directory, such as stronger consistency of Directory information across replicated sites, support operation on user specified associated aggregates of directory attributes, improve performance when retrieving large numbers of returned results, or resolution of confusion caused by multiple directory service providers holding different information under identical names?

b) What further enhancements are required to the Directory to interoperate with and to support services implemented using the IETF's LDAP specification, including possible use of XML for accessing directories.

c) What further enhancements are required to the Directory to allow its use in various environments, e.g. resource constrained environments, such as wireless networks, and multimedia networks?

d) What further enhancements are required to the Directory to improve its support of such areas as Intelligent Network, communication networks and public directory services?

e) What changes to the X.500-series Recommendations and/or what new Recommendations are required to specify enhancements to, and to correct defects in, the Directory?

Directory systems work will be done in collaboration with ISO/IEC JTC 1 in their work on extending ISO/IEC 9594, which is common text with Recommendations X.500-X.530. Liaison and close cooperation will also be maintained with the IETF particularly in the areas of LDAP.

Public-key/attribute certificates

a) What further enhancements are required to public-key and attribute certificates to allow their use in various environments, e.g. resource constrained environments, such as wireless networks, and multimedia networks?

b) What further enhancements are required to public-key and attribute certificates to increase their usefulness in areas such as biometrics, authentication, access control and electronic commerce?

c) What changes to Recommendation X.509 are required to specify enhancements to, and to correct defects in, X.509?

Public-key/attribute certificates work will be done in collaboration with ISO/IEC JTC 1 in their work on extending ISO/IEC 9594-8, which is common text with Recommendations X.509. Liaison and close cooperation will also be maintained with the IETF particularly in the areas of PKI.

Question 4/17 – Communications systems security project

The subject of security is vast in scope and topics. Security can be applied almost in every aspect of telecommunication and information technology. The approach to specify security requirements can be one of bottom-up or one of top-down:

– Bottom-up approach is where area experts devise security measures to strengthen and protect their particular domain of the network, i.e. biometrics, cryptography, etc. This is the most widely adopted way but it is fragmented as to how security is being studied in various organizations.

– Top-down approach is the high-level and strategic way of looking at security. It requires knowledge of the overall picture. It is also the more difficult approach because it is harder to find experts with detailed knowledge of every part of the network and thus its security requirements than area experts with particular knowledge of one or two specific areas.

– Another alternative is a combination of bottom-up and top-down approaches, with coordination effort to bring the different pieces together. This has often proved to be extremely challenging with varying interests and agendas.

This Question is dedicated to the vision setting and the coordination and organization of the entire range of communications security activities within ITU-T. A top-down approach to the security question will be used with collaboration with other study groups and other SDOs. This project is directed towards achieving a more focused effort at the project and strategic level.

Question

a) What are the deliverables for the communications systems security project?

b) What are the processes, work items, work methods and timeline for the project to achieve the deliverables?

c) What security compendia and handbooks need to be produced and maintained by ITU?

d) What security workshops are needed?

e) What is needed to build effective relationships with other SDOs in order to advance the work on security?

f) What are the key milestones and success criteria?

g) How can Sector Member and administration interest be stimulated and momentum be sustained on security work?

h) How could security features become more attractive to the marketplace?

i) How to articulate clearly the crucial interest to governments and the urgent need to protect global economic interests, which depend on a robust and secure telecommunications infrastructure?

Question 5/17 – Security architecture and framework

Taking into account the security threats to communication environment and the current advancement of security countermeasures against the threats, new security requirements and solutions should be investigated.

Security for new types of networks as well as security for new services should be studied.

Question

a) How should a complete, coherent communications security solution be defined?

b) What is the architecture for a complete, coherent communications security solution?

c) What is the framework for applying the security architecture in order to establish a new security solution?

d) What is the framework for applying security architecture in order to assess (and consequently improve) an existing security solution?

e) What are the architectural underpinnings for security?

i) What is the security architecture of emerging technologies?

ii) What is the architecture for end-to-end security?

iii) What is the security architecture for mobile environment?

iv) What technical security architectures are required? For example:

a) What is the open systems security architecture?

b) What is the IP-based networks security architecture?

c) What is the NGN security architecture?

f) How should the upper and lower layer security model Recommendations be modified to adapt them to the changing environment and what new Recommendations may be required?

g) How should architectural standards be structured with respect to existing Recommendations on security?

h) How should the security framework Recommendations be modified to adapt them to emerging technologies and what new framework Recommendations may be required?

i) How are security services applied to provide security solutions?

Question 6/17 – Cybersecurity

Numerous protection and detection mechanism have been introduced such as firewalls and intrusion detection systems (IDS), but most of them focus only on technical aspects. While these technical solutions are important, more consideration and discussion is needed on cybersecurity from the point of international standardization.

Question

The following areas of cybersecurity should be studied:

- processes for distribution, sharing and disclosure of vulnerability information;
- standard procedure for incident handling operations in cyberspace;
- strategy for protection of critical network infrastructure.

Question 7/17 – Security management

Question

a) How should security risks in telecommunications systems be identified and managed?

b) How should information assets for telecommunications systems be identified and managed?

c) How should specific management issues for telecommunications carriers be identified?

d) How should information security management system (ISMS) for telecommunications carriers be properly constructed in line with the existing ISMS standards?

e) How should occurrences of security incidents in telecommunications be handled and managed?

Question 8/17 – Telebiometrics

Question

a) How can identification and authentication of users be improved by the use of safe and secure telebiometric methods?

b) How is the new part of IEC 60027 "Physiological subset" to be used in ITU-T to provide elements for a suitable model for categorization of safe and secure telebiometric devices?

c) What security levels reference system should be used for bringing safe and secure telebiometric solutions in a hierarchical order?

d) How should issues of biometric authentication technologies for telecommunications be identified?

e) How should requirements of biometric authentication technologies for telecommunications based on Cryptographic technology such as PKI be identified?

f) How should model and procedure of biometric authentication technologies for telecommunications based on Cryptographic technology such as PKI be identified?

Question 9/17 – Secure communication services

Question

a) How should secure communication services be identified and defined in mobile communication or web services?

b) How should threats behind communications services be identified and handled?

c) What are the security technologies for supporting secure communication services?

d) How should secure interconnectivity between communication services be kept and maintained?

e) What security techniques are needed for secure communication services?

f) What security techniques or protocol are needed for emerging secure web services?

g) What secure application protocols should be applied for secure communication services?

h) What are the global security solutions for secure communication services and their applications?

Annex E – Bibliographical references

Didactic reference text describing the ITU-T security standards deployed in the telecommunication world:

> *Security in telecommunications and information technology: an overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunication. ITU-T, October 2004: http://www.itu.int/itudoc/itu-t/86435.html*

Some reference works

Ross Anderson: Security Engineering, A Guide To Building Dependable Distributed Systems, Wiley, 2001, ISBN 0-471-38922-6

Matt Bishop: Computer security: art and science, Addisson-Wesley, 2002, ISBN 0-201-44099-7

Ulyses Black: Internet Security Protocols, Protecting IP Traffic, Prentice Hall, ISBN 0-13-014249-2

Dorothy E. Denning: Information Warfare and Security, Addison-Wesley, 1999, ISBN 0-201-43303-6

Arnaud Dufour, Solange Ghernaouti-Hélie: *Internet – PUF, Que sais-je?* N° 3073 – ISBN 2-13-053190-3

Niels Ferguson, Bruce Schneier: Practical Cryptography, Wiley, 2003, ISBN 0-471-22357-3

Solange Ghernaouti-Hélie: *Internet & Sécurité – PUF Que sais-je?* N° 3609 – ISBN 2-13-051010-8

Solange Ghernaouti-Hélie: *Sécurité informatique et réseaux, cours et exercices corrigés* – Dunod 2006.

Raymond Panko: Corporate Computer and Network Security, Prentice Hall, 2004, ISBN 0-13-038471-2

Guillaume Poulin, Julien Soyer, Marc-Éric Trioullier: *Sécurité des architectures Web, «ne pas prévoir c'est déjà gémir»*, Dunod, 2004.

Bruce Schneier: Beyond Fear, Thinking Sensibly About Security In An Uncertain World, Copernicus Books, 2003, ISBN 0-387-02620-7

Bruce Schneier: Secrets and Lies: Digital Security in a Networked World, Wiley, 2000, ISBN 0-471-25311-1

Bruce Schneier: Applied Cryptography, Protocols, Algorithms and Source Code in C, Second Edition, Wiley, 1996, ISBN 0-471-11709-9

Simon Singh: Histoire des codes secrets, JC Lattès, 1999, ISBN 2-7096-2048-0

William Stallings: Cryptography And Network Security, Principles and Practice, Prentice Hall, 1999, ISBN 0-13-869017-0

William Stallings: Network And Internetwork Security, Principles and Practice, Prentice Hall, 1995, ISBN 0-13-180050-7

William Stallings: Network Security Essentials, Applications and Standards, Prentice Hall, 2000, ISBN 0-13-016093-8

Reference sites

Sites in French:

French Prime Minister's site: http://www.premier-ministre.gouv.fr

(See in particular under: *Technologie de l'information dans la thématique: communication*)

http://www.internet.gouv.fr: site relating to development of the information society

French public service portal: http://www.service-public.gouv.fr. Leads to all online services, see under «*se documenter*»

French public service site on law: http://www.legifrance.gouv.fr

French documentation service site: http://www.ladocfrancaise.gouv.fr

http://www.foruminternet.org/: Information and discussion forum on law, the internet and networks

French National Civil Liberties Commission: http://www.cnil.fr

French Central Office for combating ICT-related crime: http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic

Information System and Network Security Observatory: http://www.ossir.org

Clusif: www.clusif.asso.fr.

Panorama of cybercrime: https://www.clusif.asso.fr/fr/production/ouvrages/

Other sites

CERT: www.cert.org (Computer Emergency Response Team)

NIST: http://www.nist.gov (US National Institute of Standards and Technology)

NSA: http://www.nsa.gov (US National Security Agency)

CSE: http://www.cse.dnd.ca (Canadian Telecommunication Security Centre)

CESG: http://www.cesg.gov.uk (UK National Technical Authority for Information Assurance)

BSI: http://www.bsi.bund.de (German Federal Information Security Office) – site in German and English

DSD: http://www.dsd.gov.au (Defence Signals Directorate operating in Australia and New Zealand). Site devoted to digital watch and information security.

National White Collar Crime Center: IFCC – Internet fraud complaint center: http://www1.ifccfbi.gov/index.asp; Internet Fraud – Crime Report – 2004: http://www1.ifccfbi.gov/strategy/2004_IC3Report.pdf

Newsletters

Cryptogram – Bruce Schneier: [schneier@counterpane.com] crypto-gram-list@listserv.modwest.com

Internet Rights Forum infoletter: infolettre@listes.foruminternet.org

US-CERT Security Bulletins: security-bulletins@us-cert.gov

Cyberpolice information letter: http://cyberpolice.over-blog.com/ cyberpolice.over-blog.com [newsletter@over-blog.com]

Annex F – OECD Guidelines for the security of information systems and networks: Towards a culture of security

Preface

The use of information systems and networks and the entire information technology environment have changed dramatically since 1992 when the OECD first put forward the *Guidelines for the Security of Information Systems*. These continuing changes offer significant advantages but also require a much greater emphasis on security by governments, businesses, other organizations and individual users who develop, own, provide, manage service and use information systems and networks ("participants").

Ever more powerful personal computers, converging technologies and the widespread use of the Internet have replaced what were modest, stand-alone systems in predominantly closed networks. Today, participants are increasingly interconnected and the connections cross national borders. In addition, the Internet supports critical infrastructures such as energy, transportation and finance and plays a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information. The nature and type of technologies that constitute the communications and information infrastructure also have changed significantly. The number and nature of infrastructure access devices have multiplied to include fixed, wireless and mobile devices and a growing percentage of access is through "always on" connections. Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially.

As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security. For these reasons, these Guidelines apply to all participants in the new information society and suggest the need for a greater awareness and understanding of security issues and the need to develop a "culture of security".

F.1 Towards a culture of security

These Guidelines respond to an ever changing security environment by promoting the development of a culture of security – that is, a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks. The Guidelines signal a clear break with a time when secure design and use of networks and systems were too often afterthoughts. Participants are becoming more dependent on information systems, networks and related services, all of which need to be reliable and secure. Only an approach that takes due account of the interests of all participants, and the nature of the systems, networks and related services, can provide effective security.

Each participant is an important actor for ensuring security. Participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks.

Promotion of a culture of security will require both leadership and extensive participation and should result in a heightened priority for security planning and management, as well as an understanding of the need for security among all participants. Security issues should be topics of concern and responsibility at all levels of government and business and for all participants. These Guidelines constitute a foundation for work towards a culture of security throughout society. This will enable participants to factor security into the design and use of all information systems and networks. They propose that all participants adopt and promote a culture of security as a way of thinking about, assessing, and acting on, the operations of information systems and networks.

F.2 Aims

These Guidelines aim to:

- Promote a culture of security among all participants as a means of protecting information systems and networks.
- Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.
- Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.
- Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.
- Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.
- Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

F.3 Principles

The following nine principles are complementary and should be read as a whole. They concern participants at all levels, including policy and operational levels. Under these Guidelines, the responsibilities of participants vary according to their roles. All participants will be aided by awareness, education, information sharing and training that can lead to adoption of better security understanding and practices. Efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy[64].

1) Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

2) Responsibility

All participants are responsible for the security of information systems and networks.

Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a

---

64 In addition to these Security Guidelines, the OECD has developed complementary recommendations concerning guidelines on other issues important to the world's information society. They relate to privacy (the 1980 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*) and cryptography (the 1997 *OECD Guidelines for Cryptography Policy*). These Security Guidelines should be read in conjunction with them.

timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

3) Response

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

Recognizing the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

4) Ethics

Participants should respect the legitimate interests of others.

Given the pervasiveness of information systems and networks in our societies, participants need to recognize that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognizes security needs and respects the legitimate interests of others.

5) Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

Security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

6) Risk assessment

Participants should conduct risk assessments.

Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

7) Security design and implementation

Participants should incorporate security as an essential element of information systems and networks.

Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimize security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organization's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

8) Security management

Participants should adopt a comprehensive approach to security management.

Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.

9) Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.

Recommendation of the Council concerning guidelines for the security of information systems and networks: Towards a culture of security

THE COUNCIL,

Having regard to the Convention on the Organization for Economic Co-operation and Development of 14 December 1960, in particular, Articles 1 b), 1 c), 3 a) and 5 b) thereof;

Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

Having regard to the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [Annex to C(85)139];

Having regard to the Recommendation of the Council concerning Guidelines for Cryptography Policy of 27 March 1997 [C(97)62/FINAL];

Having regard to the Ministerial Declaration on the Protection of Privacy on Global Networks of 7-9 December 1998 [Annex to C(98)177/FINAL];

Having regard to the Ministerial Declaration on Authentication for Electronic Commerce of 7-9 December 1998 [Annex to C(98)177/FINAL];

Recognizing that information systems and networks are of increasing use and value to governments, businesses, other organizations and individual users;

Recognizing that the increasingly significant role of information systems and networks, and the growing dependence on them for stable and efficient national economies and international trade and in social, cultural and political life call for special efforts to protect and foster confidence in them;

Recognizing that information systems and networks and their worldwide proliferation have been accompanied by new and increasing risks;

Recognizing that data and information stored on and transmitted over information systems and networks are subject to threats from various means of unauthorized access, use, misappropriation, alteration, malicious code transmissions, denial of service or destruction and require appropriate safeguards;

Recognizing that there is a need to raise awareness of risks to information systems and networks and of the policies, practices, measures and procedures available to respond to those risks, and to encourage appropriate behaviour as a crucial step towards the development of a culture of security;

Recognizing that there is a need to review current policies, practices, measures, and procedures to help assure that they meet the evolving challenges posed by threats to information systems and networks;

Recognizing that there is a common interest in promoting the security of information systems and networks by means of a culture of security that fosters international co-ordination and co-operation to

meet the challenges posed by the potential harm from security failures to national economies, international trade and participation in social, cultural and political life;

And further recognizing that the *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* set out in the Annex to this Recommendation are voluntary and do not affect the sovereign rights of nations;

And recognizing that these Guidelines are not meant to suggest that any one solution exists for security or what policies, practices, measures and procedures are appropriate to any particular situation, but rather to provide a framework of principles to promote better understanding of how participants may both benefit from, and contribute to, the development of a culture of security;

COMMENDS these *Guidelines for the Security of the Information Systems and Networks: Towards a Culture of Security* to governments, businesses, other organizations and individual users who develop, own, provide, manage, service, and use information systems and networks;

RECOMMENDS that Member countries:

Establish new, or amend existing, policies, practices, measures and procedures to reflect and take into account the *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* by adopting and promoting a culture of security as set out in the Guidelines;

Consult, co-ordinate and co-operate at national and international levels to implement the Guidelines;

Disseminate the Guidelines throughout the public and private sectors, including to governments, business, other organizations, and individual users to promote a culture of security, and to encourage all concerned parties to be responsible and to take necessary steps to implement the Guidelines in a manner appropriate to their individual roles;

Make the Guidelines available to non-member countries in a timely and appropriate manner;

Review the Guidelines every five years so as to foster international co-operation on issues relating to the security of information systems and networks;

INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to promote the implementation of the Guidelines.

This Recommendation replaces the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 [C(92)188/FINAL].

Procedural history

The Security Guidelines were first completed in 1992 and were reviewed in 1997. The current review was undertaken in 2001 by the Working Party on Information Security and Privacy (WPISP), pursuant to a mandate from the Committee for Information, Computer and Communications Policy (ICCP), and accelerated in the aftermath of the September 11 tragedy.

Drafting was undertaken by an Expert Group of the WPISP which met in Washington, DC, on 10-11 December 2001, Sydney on 12-13 February 2002 and Paris on 4 and 6 March 2002. The WPISP met in Paris on 5-6 March 2002, 22-23 April 2002 and 25-26 June 2002.

The present OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002.