The ICT security issues and trends[*]

1. The global scenario: complexity and ambiguity

At present, security is a very complex issue. The very meaning of the word implies new reflections and reasoning which differ from the ones we were used to only two or three years ago. In recent past, both citizens and companies thought about security as something that had to do with stolen goods, frauds, sabotages and murders. Today, the same word implies more worrying thoughts: wars and terrorism, for example.

Complexity and ambiguity seem to be the key words identifying current geopolitics since the shift from USA-USSR bipolarism to an apparently simpler American hegemony. After 11th September 2001 the United States declared war on an elusive and ever changing entity - International terrorism - and not on a state.

In such a conflict, the information war plays a relevant role, as by using viruses and by transmitting false commands or signals it is possible to cause the information infrastructure of an enemy to collapse.

Even if information only makes army systems more powerful rather than representing a form of power itself, *hacker warfare* - carried out through viruses meant to destroy the memories of enemy computers - has a relevant weight in this kind of war.

Businessmen have therefore understood that self-defence, notably the prevention of negative events, has become a basic factor to carry out business and to protect the ability to add value to the production. In the past, crises were statistically limited and therefore often "mentally" acceptable in logic of benefits and cost. Today, investments on security are something you can not do without as crisis are more and more frequent and their damaging impact in terms of competition and operative capability grows heavier and heavier. Of course, investments on security

[*] Text edited by Priscilla Bigioni and translated by Roberta Grasselli.

are carefully valued through modern practices in risk analysis and risk management. The uncertain situation of world economy also suggests that, after all the difficulties they have been through in terms of economical results, companies will become more aware of the need to protect their resources and their activities. As it cannot be denied that they might try to face economical difficulties by making competition even fiercer in order to compensate their losses with an increase in their market share.

And it is a well-known fact that an extreme competition inevitably leads to opportunism and sometimes to infringements of the law too.

Geopolitical macro scenarios are unlikely to become simpler or rosier in the near future. According to the most accredited observers, the international confrontation shows no lessening symptoms.

On the other hand, it is a plausible theory that terrorism and big crime organizations might develop new levels of connection using ICT. In this case, a tougher collaboration at a European level would become essential.

2. The ICT security role

Following the pervasive application of information and communication technologies, ICT systems are now the basic core and the reservoir of all pieces of information that are fundamental to organizations. According to the Computer Emergency Response Team – Coordination Center (CERT), the current generation of information systems is based on the Internet and this raises quite worrying security issues. On the one hand, ICT systems are both more and more complex and vulnerable with a growing presence of bugs at a developing stage as well as in their production. On the other hand, launching damaging attacks against the systems requires less complex skills.

ICT environments are also more heterogeneous and complex and as a consequence are likely to be exposed to new types of intrusions. The spread of wireless radio connections has opened new attack fronts, which are difficult to defend, as they are intrinsically accessible to anybody (*broadcast communication*). The Internet itself has a more hierarchical structure and has turned into a net of protected isles that are almost inaccessible from outside intruders (Intranet and VPN). The widespread launch of open source and commercial products before they are ready to defeat competition, in a time that goes by faster thanks to global connection, has caused users to become accustomed to ever-faulty software, which always need to be maintained through the applications of patches.

In spite of all that, most of the attacks still take advantage of well-known points of weakness that still have no solutions, in the never-ending race between attackers and defenders.

3. Risk analysis and FTI Security Observatory "OCI"

When analysing risks to ICT systems, the basic elements are represented by the availability of quantitative as well as qualitative data about attacks that took place, how they were detected and what operative and economical consequences they had. In Italy, *Sicurforum Italia* set up the ICT Security and Crime Observatory (OCI) in order to identify and understand the typology and the size of the phenomenon with regards to its features and impacts. In collaboration with the SPACE Center of the Bocconi University, *Sicurforum Italia* defined the methods of investigation of the Observatory by elaborating data gathered from a significant group of research organizations and businesses and by periodically supplying the results through reports and seminars.

Data gathered during those years allow formulating some remarks. First of all, it must be said that it is not easy to obtain information by the organizations that are attacked. Organizations often wish to safeguard their prestige or their public image, but there is also another reason: it is sometimes difficult to identify the methods of certain attacks. Moreover, historical series dealt with a non-homogeneous group of systems and situations for two main reasons. First of all, the group has always consisted of two hundred subjects (businesses and Public Administration) structured according to the segmentation of an information expenditure, and it underwent some variations that were independent from the gatherer because of sudden unavailability of data rather than the re-organization or the merging of businesses. Secondly, the types of environments and applications prevailing in information systems experienced an evolution and therefore, from a certain point of view, they are no longer victims of certain attacks but they are now the targets of new types of attacks. As a consequence, certain techniques of attacks became obsolete or were more easily prevented, while new techniques have been developed by taking advantage of the vulnerability of the new systems.

As a result, the value of historical series is just an indicator of an overall trend and can provide interesting comparative evolution lines – as it happens with the yearly surveys by CSI-FBI in the United State -, even if this is statistically limited.

The FTI Observatory aims at recording deliberate attacks against ICT systems and not at measuring risks stemming from their bad functioning, the improper use or phenomena which are accidental and external such as natural disasters or accidents (flooding, earthquakes, fires, black-outs, etc.).

The classification of attacks that is being used is simple and easily understandable by those who received the questionnaire: persons in charge of the ICT divisions and ICT security.

The following are the categories of attacks referred to:

- Virus contamination (both at workstation and server levels);
- Theft of information equipments containing data (laptops, hard disks, floppy disks, tapes, etc.);
- Denial of service;

- Trojan horses;
- Piracy and information frauds (abuse of ICT resources, illegal copying of software or data, etc.);
- Non authorized access and changes to information;
- Non authorized use of computers (systems, applications, e-mail);
- Non-authorized access and changes to systems and applications.

The point of view of the attacked comes first: we asked information about detected attacks but also opinions about the attacker's aims and damages caused by the attacks. Damages that can be divided into:

- direct damages, that occurred at the same time or immediately after the attack (loss of information, theft of devices, etc.);
- indirect damages, of economical nature and indirect consequence of the attacks (interruption or reduction of operative activities, costs of resetting, etc.);
- consequential damages, which occur after returning to the previous "status of normality" and include loss of image and competitive power, organizational problems with the staff, etc.

OCI data from FTI confirm that Italy follows the international trends, with some peculiarities, of course. In particular we noticed:

- the steady growth and the critic development of the virus phenomenon, sharpened by the increasing use of e-mails and the exchange of programs on the net, through the applet activation and hostile agents during the connections to web sites which are unsafe or not safe enough (as showed also by data collected by Security*Net* Observatory);
- the growing menace to the privacy and the integrity of information, sharpened by new and more complex distributed environments that are based on Internet protocols and have a better interoperability between systems of different organizations (outsourcing, virtual extended businesses, Intranet/Extranet);
- resetting of the attacked systems, which sometimes takes too long;
- an increasing, but still limited, use of preventive measures, of detection and monitoring of the risk and the security of the systems that, in many cases, leads to ignoring the fact of being under attack.

Numbers from OCI confirm the importance of the initiatives of coordination and regulation at a national as well as at international level. These EU initiatives include: the creation of the European Network and Information Security Agency (ENISA), an agency that coordinates public and private operators to provide the internal market with higher levels of security; the proposal of the EU Commission for a common approach in European ICT security policy (COM (2001) 298 final); the creation in Italy of the "ICT security committee for the Public Administration" as well as the ICT security actions carried out in Italy by the Department for Technological Innovation through the security directive in the P.A. issued on 16th January 2001.

The technical and cultural commitment to ICT security must go on. We need to shift from a "specialized" phase - where ICT security is a prerogative of technicians of information systems – to an "aware" phase – where ICT risks and security strate-

gies are analysed by the highest managerial spheres of each organization, taking into consideration their economical and organizational impact. In 2002, OECD guidelines – "Towards a Culture of Security" - provided a very good course to follow. They update the guidelines given in 1992 and recommend the growth of ICT security culture within users as well as suppliers of ICT products.

4. The role of standards

In modern companies, notably in those providing services, information plays a key role, and its importance is so extraordinary that sometimes it is even taken for granted. Besides, the *information content* is generally considered as an element that adds value while technology, or the resource dealing with the *information content* - that will be called *computer resource* -, is often considered as the element that must ensure the preservation of this value. It follows that the effort to provide companies with safe information is still mainly technological. As a result, companies choose technological countermeasures and count on the fact that *information resources* can ensure them a predefined level of security.

The creation of standards has contributed to spread this point of view, besides trying to rationalize products and to defend the markets.

Standards – at first TCSEC, then ITSEC, and today ISO15408 (Common Criteria), and to a certain extent the standards ISO9001:1994 and IS-17799 as well – represent an emblematic example.

In latest years, *Common Criteria* (CC) have become an ISO/IEC standard, notably the standard IS-15408 in 1999. This is one of the reasons that made them famous with regards to other evaluation criteria, as there are no other criteria issued by an international standardization body. When an evaluation is successfully carried out according to CC, a proper organization issues an ICT security certificate. Such an organization can be considered as a third party in front of those who ask and pay for the evaluation/certification as well as those subjects who attach importance to the fact that a company has or has not an ICT security certificate (the so-called "*certificate users*").

Only one year after CC had become standard ISO/IEC, the same international body was involved in the first part of another ICT security standard certification, developed in Great Britain. It was the well-known BS7799 that became IS-17799 in its ISO/IEC version. Perhaps those who were not expert got a bit confused at first, but now most people understand that, besides having in common ICT security, the CC and the BS7799 certificates aim at certifying quite different things. Actually, CC certify an ICT product or system, while BS7799 certifies a process used by an organization – a private business as well as a public body- to ensure its internal ICT security. Such a process is defined by the standard acronym ISMS (*Information Security Management System*). In other words, the BS7799 certificate can be considered as a company certificate belonging to the same category of

the ISO9000 certificate but which is issued especially for ICT security.

5. Regulation and Business Continuity

The whole of the laws Italian companies refer to is undergoing many changes recently. First of all, the government passed a decree implementing the reform of the company law (the so-called Vietti reform). The new law is characterized by a wide statutory independence as to governance models and relations among partners. It also makes a clearer differentiation between joint-stock companies and limited companies and, not least, included new financial tools for companies.

In the same period, the Committee of Basel defined a new set of rules concerning the activities of financial institutions. This set of rules known under the name of "Basel II" was extremely innovative and had great influence on credit policies and on the internal governance structures of financial institutions. The availability of new financial tools together with the bank application of the Basel II set of rules from the year 2007 introduces a new type of business relations among the Italian companies, the bank system and the financial market. It also creates the need to choose new tools for the management and the administration of internal and external risks of financial institutions.

All of these regulations have one common feature: they recognize the fundamental role of the management as well as of the monitoring functions that verify the activities of the business in order to develop a careful management of risks. The aim is:

- achieving business goals;
- carrying out a behaviour that is consistent with the expectations of the company;
- transparency towards shareholders and stakeholders.

In such a context, monitoring activities must play a relevant role in ensuring that companies conform to laws, but it is important that they perform efficient internal monitoring activities and a proper risk management.

When an organization has a strong culture and master internal monitoring, it owns the basis to set up and manage a company system able to face anomalous events so that activities can be regularly carried out and strategic goals achieved. It follows that the government will not be efficient until the major risks for the organization itself are defined and mapped. For that reason, risk management should be a continuous and dynamic process that follows the strategic goals of the company as guidelines and should be supported by proper methods and a reliable infrastructure too.

When approaching risk analysis, it is very important to choose a common internal language that unambiguously identifies a model to define, value, measure and monitor, or minimize, risks.

In such a context, a relevant role is played by operative risks that cause losses

concerning: human mistakes; frauds; improper contracts; violation of the regulations; fault tolerance (ability to face the unavailability of the systems); security of the technological systems.

Actually, operative risks have very different origins and it is difficult to define them exhaustively. Analysts admit that risks can be divided into two different components: *Event Risks* and *Business Risks*. The former refer to potentially catastrophic events (natural disasters, system downtimes, frauds) that imply operative losses. The latter refer to wrong strategic choices that involve a decrease in the income margins. Both of them have the following features in common:

- they permeate the whole structure: they are originated by the external context where a company operates, by the company counterparts, by the internal activities and by the structure of the company itself;
- they are not homogenous: the types of risks and losses are not similar. Event and business risks have different natures, they have potential impacts that vary a lot and can arise at any phases of the company processes;
- they do not directly depend on productivity: a higher and accepted perspective of risk is not always strictly related to productivity.

Company managers have to fully understand the added value of an efficient monitoring of risks. If risks are not managed to prevent them from affecting the cash flow, they will inevitably affect the capital cost as the risks to the company increase. This is clear in the case of current investments in technology and human resources carried out to create a business continuity system or a disaster recovery system. Investments in such activities can be regarded as tools for minimizing operative risks (*Event Risks*), which are often perceived as unavoidable costs for probable risks by company managements.

As a result, the concept of continuous operativity should acquire a wider meaning that also involves availability: such activities have to be considered as a step towards a new management of company flows. In this case, also Business Risks will be covered and investments will contribute to the company income.

6. The activities against computer crimes and computer forensics

The Internet has increased the variety of economic and business relations, has encouraged the professional development of individuals and the circulation of opinions, has spread knowledge and has favoured consciousness. In this situation, the potential growth of illicit activities and criminal behaviours is inevitable: awareness and adaptability become essential elements to prepare all steps to protect the rights and the freedom of which the web is the direct expression. Certain criminal environments favour the Internet because of some peculiarities of the web: its high speed, data can be easily obtained and concealed, anonymity, its cross-border nature.

In these characteristics it is possible to identify the causes of negative situations

that the Police systematically has to face: technical problems in identifying criminals, and legal problems concerning the enforcement of the law and the finding of evidence. Charging criminals and prosecute them is also very difficult even though their actions are transversal and committed at an international level.

Then, it is evident that all the actions taken by the Magistracy and the Police in order to oppose the criminal phenomena are extremely important and that they should be coordinated according to the so-called forensic information science at an international level. In other words, those activities should be carried out by taking into consideration the discipline that studies the analysis and the solutions of cases connected with information crimes, including the ones that implied the use of a computer, that were directed against a computer and those crimes where a computer represents a source of evidence. Forensic information science aims at preserving, identifying, acquiring, documenting and interpreting data on a computer. In brief, it aims at "giving voice to information evidence".

The information system examined by an investigation can be a personal computer or a server, in this case we are in the field of *computer forensics*. When there are at least two computers connected we talk about *network forensics*, instead.

7. The contents of the book

All of these issues are tackled by the numerous contributions of the book. Sergio Pivato and Giorgio Pacifici deal with global economic and geopolitical issues. Carlo Sarzana describes the basic elements of ICT security regulation, notably with reference to Public Administration; Bruschi, Monga and Rosti define the new technical and applicative context of ICT security. Pozzi, Bozzetti and De Lorenzo present data from the OCI-FTI observatory, while Fulvio Berghella describes data by the SecurityNet Observatory about viruses in Italy. As to information attacks, Sirmi and Symantec present data from their international and national observatory. Gianluca Braghò illustrates the discipline of information crimes basing his contribution on his personal experience as a magistrate who coordinates this kind of investigations. With their contributions, the Italian investigative police (Arma dei Carabinieri, Guardia di Finanza, Polizia Postale e delle Comunicazioni) testify the commitment and the technical skills that are necessary to oppose new crime phenomena; Cesare Maioli introduces computer forensics issues.

The definition of strategic and organizational policies in the field of security (through the use of standards too) is the subject dealt with by Roberto Masotti, Raoul Savastano, Luigi Sciusco and Franco Guida.

Finally, the book contains real case studies about ASP applications (by Zini, Busuoli and Fraulini), peculiarities of the information security systems in the Public Administration (by Mariano Lupo, Raffaele Visciano) and computer forensics (by Antonio Gammarota, Pierluigi Perri).