Computer and telecommunications risks

New risks, new solutions

Source: - Scor Re Report

Only a few years ago, there was a great deal of talk about computer risks. Today, people talk more about risks concerning information systems as a whole, which means both computer systems of any type and telecommunication systems. This concept can he extended to all information media, including written and oral.

Phenomenology of the risks concerning information systems

CAUSES

Three main types of causes can be identified: accidents, errors and malicious acts. In general, malice is the most frequently mentioned: it represents three out of four by 2000. The essence of our societys values has been dematerialized, and information systems are at the core of the liberal economy. This explains the increase of malicious attacks on these systems. Malice will therefore be a growing concern in the future.

The three types of causes mentioned above however are only immediate technical causes. The deeper causes are rarely technical in nature in fact they involve problems on a human or organizational level, etc., which are much harder to quantify. Human beings cannot be modelised and it is difficult to implement effective preventive measures at this level. The keys to the future will therefore probably be in education and dissuasion.

CONSEQUENCES

a. Technical consequences

Three components of the information systems can be affected:

Availability

The information system can suddenly fail or stop providing its service at the level of effectiveness needed for its use.

Integrity

The static and dynamic information used may no longer comply with the requisite standards.

Confidentiality

There is the possibility that information be intercepted by an unauthorized third party who uses it in a way which could damage the company.

b. Final consequences

Beyond the technical consequences, one must be able to express the final consequences. These are observed well after the occurrence of the technical consequences, after the so-called (crisis situation) is over. The way the crisis situation is managed largely determines the significance of the final consequences. Crisis situations can only be well managed through advance preparation, which requires the definition of a (contingency plan).

Twenty years ago, the final consequences of computer risks were perceived only in financial terms. Today, computer systems are at the core of most economic activities and therefore losses can have qualitative and ethical consequences, etc.

SECURITY MECHANISMS

a. Detection

Detection is at the center of this mechanism. The detection of computer-related damage is not always simple. Between occurrence and detection of the damage, several days, weeks or months can pass, making the final consequences considerably worse.

b. Prevention

In computer security, there can he many overlapping causes. It is therefore illusory to try to analyze the causes individually and think one can avoid them by setting up preventive measures.

c. Pre-prevention

Confronted with these risks, which involve human beings as well as technology, one must set up pre-preventive measures focusing on people and procedures. The information systems of the 21st Century, which will become more and more open and complex, will he difficult to control by technical means. There will be a lot of work ahead of us in terms of dissuasion and, consequently, education.

d. Protection

To fight against the consequences, there are protective means which consist of classifying the most important computer assets (data, procedures) for the company and trying to isolate them by technical means in order to minimize the impact of damage on the vital parts of the information system. Analysis of the vital parts must be very precisely conducted. Consequently, the analysis of computer risks for complex systems is a relatively complicated science.

e. Post-protection

Lastly one can have post-protection measures, which mostly work by risk transfer: not only insurance, but also contractual means. Many of the intermediaries of the communication process can assume part of the responsibility, if there is such a provision in the contract. In terms of liability, there is no clear distinction between operator and user. For example, in an exchange of computerized data between two organizations, the responsibility of both can be strongly implicated. All contracts, especially for subcontracting, must therefore be closely examined by the insurers and reinsures if they want to try to manage computer risks. Fifteen years ago, computer systems had very precise configurations and could therefore he easily insured. Today, analysis of interconnections makes risk analysis much more unwieldy. However it is crucial in terms of liability risks.

Breakdown of causes and consequences

BREAKDOWN OF CAUSES

Computer risk is not yet a major risk for insurers. Which is characterized by two parameters: the probability of occurrence and its impact. The probability of occurrence is low, but the individual impacts of a loss can be enormous. For the ten largest banks in France, the maximum possible computer-related loss exceeds *5* billion French francs.

a. Malice

- Theft
- Fraud.
- Computer hacking crimes mostly cases of sabotaging the competition. They constitute a major risk for the future. Anything goes when it comes to weakening ones competitors in the liberal world in which we live.

b. Errors

Errors in the design and production of large systems account for the most worrying phenomenon: Windows NT, for example, includes several million instructions. It should come as no surprise that dozens of errors are hidden in them. Will these errors have serious consequences? They are impossible to prevent. In large systems, it is extremely difficult to locate the source of an error.

c. Accidents

Physical accidents always increase faster than the value of the computer equipment installed. This is because one tends to have blind faith in well-known means of prevention without worrying about the consistency of these means as a whole.

Failures are still extensive. Even with failure-tolerant systems, the number of claims continues to rise and involves higher and higher amounts.

BREAKDOWN OF THE CONSEQUENCES

The consequences of these losses can he expressed as 40% in terms of availability, 23% confidentiality and 37% integrity. The latter two aspects are the most talked about today, especially in electronic trading. Yet it is availability which has the greatest economic consequences. The best way to paralyze a competitor is still to block his information system at a vital moment.

General factors which modify the risks

TECHNICAL ELEMENTS

How can one control an information system which is completely open and interconnected? Security often goes hand in hand with pinpointing of responsibility. The second element which makes any system vulnerable is the revolution in telecommunications, whose networks never cease to expand and diversify. If a loss is incurred, the legal proof of responsibility would be impossible to fix. Lastly, Most companies use software packages developed by service suppliers and sold in multiple copies. Thus, the cumulative risk grows incessantly.

THE INTERNET

There is no central authority. A large proportion of the servers used has very vulnerable operating systems. The number of parties involved in a transaction is very high. Lastly, we are talking about a network of networks, which is therefore uncontrollable. What are the main risks on the Internet? They are mainly risks of malice, theft of identity or divulgence of confidential information.

EVOLUTION OF THREATS

Malice is expected to represent nearly three-quarters of the causes and confidentiality and integrity risks will also increase considerably. It is the combination of telecommunications and computer technology, which is at the root of this evolution.

Solutions

Confronted with these threats, we can call on a wide variety of services and solutions. The technical resources grow each year. But the real problem is not technical. The real problem is in setting up consistent architectures capable of providing security for complex systems. There are also regulatory and legal questions, especially concerning the limits imposed by various governments on the use of efficient cryptography systems. We must find a compromise between system security and the need for governments to be able to monitor communications in their efforts to fight crime.

New threats

Multimedia and tele-conferences can now be subject to dynamic modification of thee image in real time, which can have devastating consequences. The development of home-working and electronic trading will inevitably bring about an increase in fraud.

Discussion

What is the economic importance of cross-border viruses?

Viruses represent only 20% of the cost of computer hacking crimes. But the real problem is specifically-targeted hacking carried out using highly complex means. In order to be protected against viruses, one only needs to have the technical resources and follow the appropriate procedures. Technically speaking, there is a whole range of high-quality anti-virus products.