@ HORUS

1ST Egyptian Electronic Insurance Newsletter

Volume 1, Issue 2 April 20, 2000

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 society values has been dematerialized, and information systems are at the core of the liberal

Continued on page 2

INSIDE THIS ISSUE

1 Computer and telecommunications risks: new risks, new solutions

1 Is man the weakest link in the chain

6 Ten Common Mergers Mistakes

Is man the weakest link in the chain?

Source: -Swiss Re Report

Accidents in complex, high-risk systems such as chemical plants, nuclear power stations, space, aviation or shipping can rarely be attributed to one single cause. They are usually the result of a combination of human, technical, organizational and environmental factors. If one regards an accident as a chain of events, the the last link is almost always man, whether as an operator in the control center, a captain on the bridge or a pilot in the cockpit. If the domino effect reaches the last link in the chain, then only an either-or situation remains: f uman eing akes he rong ecision when it matters most, the accident will be put down to human error. If he manages to halt the effects of the error just in time, then (the system) works. This study attempts to shed more light on the significance of the (human factor) and explain the role of man in interaction with technology, systems and the environment.

Regardless of the material consulted, human beings are always listed as the most common cause of accidents. It is not surprising therefore that the annual statistics on total losses from air accidents published by the International Air Transport Association (IATA) also cited human error as the cause of around 50% of total losses in 1994. In 1995, when (organizational) was added to the existing human, technical and (environmental categories, human beings remained top as the cause of around 40% of all accidents. Other statistics even attribute a considerably higher proportion to human error, for example Boeings Causal factors for air carrier accidents 1974-1983 (68.8%); or the Critical Incident Reporting System from the Anaesthesia Department of the University Hospital in Basle:

Mans role

In automated systems

It lists the (human factor as the cause of over 70% of incidents in the operating theatre.

Finding out the true causes of an accident is often difficult. They are sometimes hidden and very hard to find, whilst other factors seem all too plausible. It is precisely these (human factors) which are often merely symptoms of a root

continued on page 4

continued from page 1

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 consequ

largely determines the significance of the final consequences. Crisis situations can only be well managed through advance preparation, which requires the definit

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,

continued from page 2

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.

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.

continued from page 3

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.

Continued From Page 1

cause. Bearing this in mind, the analysis of accidents and incidents should do more than merely scratch the surface of events; it must search for the underlying causes of the problem.
The technology of complex working systems has developed rapidly over the last few years. This development looks set to continue well into the future. Ongoing automation is steadily forcing man into the role of system supervisor: controlling and regulatory functions are increasingly taken care of by technology.

Would it be wise for the ultimate goal of automation to focus on the elimination of man, the essential risk factor, from such systems? Statistics do not provide us with the answer. They take into account only accidents and catastrophes in which human error played a significant role.

In comparison, accidents and catastrophes, which were prevented by correct human action, are not taken into account. Or, as an information bulletin from a chemical company reported, (As the number of automated plants increased, so did the number of events whose cause could be attributed in part to the shortcomings of a component in the automatic system. (...) Several harmless events should be classified as near misses: if attentive employees had not taken the appropriate measures, the incidents could have had serious consequences for man, the environment and the plant).

Mans capabilities under threat
Despite mans superiority to technology in his ability to predict. Anticipate, think flexibly. And take decisions in imprecisely defined situations, his role in the complex working system is being increasingly undermined. The redefinition of the function allocation between man and technology has led to a new generation of human errors. Studies have identified a reduction in the ability of people who carry out supervisory functions in highly automated systems to detect system errors and carry out manual operations. This failing can be attributed to two phenomena, which accompany automation:

1- Loss of manual skills
Manual skills diminish when they are used rarely or not at all. Studies show that people who are charged with nothing more than the supervision of an automated system are slower and less efficient at regaining control over the system following a disturbance than those who operate a system manually. This is also the case for once experienced and practiced system operator. The result is that when a disturbance occurs, the operator does not possess the skills required to assume manual operation and the stress in such situations thus becomes even greater.

2- Loss of situation awareness
To overcome disturbances it is extremely important to remain constantly aware of the current situation. Past air accidents have shown that the loss of situation awareness plays an important role in many cases. Here, calculating the amount of time left in

Continued from page 4

which to act is an important factor, and one, which is all too often forgotten.
(Situation awareness) comprises the continuous awareness of relevant variables in a system, understanding of the significance of the systems current state with respect to operators aim and, on the basis of this understanding, the projection of future trends and events within systems.

The role of human beings

Is often underestimated

Why does loss of situation awareness often occur with technological systems? One of the reasons is that during mainly supervisory activities, attention levels fall and complacency increases. This fact is reinforced by the excessive trust placed in automation. In addition, the process of automation has downgraded man from (active processor) to (passive recipient of information); this is also detrimental to attention levels.
Using the argument that human actions are unreliable per Se, systems designers try to design (fail safe) systems or replace the human element completely by machines. However, the more technical and highly developed a system is, the more important and essential the human being becomes to this system. This apparent paradox also becomes evident in the interest shown in the human factor that has increased parallel to technological development.
It is possible for human beings to succeed where technology fails: by taking charge of a disturbance at the decisive moment, implementing the right measures and thus averting an accident or at least minimizing its effects. Even systems that have been fully automated as a result of human error are reliant on human supervision. And there is a general consensus that, even with fully automated systems. The ultimate responsibility must lie with human beings.
The main argument in favor of high-tech systems is often a higher level of safety. Without doubt, the efficiency of traditional safety precautions such as alarms and warning systems or redundancies have been increased by further technological developments.
Despite all the safety precautions. Accidents continue to happen. Why? Complex systems are different in that they are made up of a variety of individual components, a high level of integration and a certain autonomous momentum and intransparency. This means that, despite the best engineers. (Intelligent) technology and reliable risk assessment, disturbances to different components and processes in such systems will occur which no designer had ever considered and for which no operator or pilot had been prepared.
This explains why it is possible to gain new information on system dependencies from almost any accident. The information can then be used to help avoid similar accidents in the future. Fortunately, an accident does not have to happen for lessons to be learnt; it is possible to extract this knowledge from near misses (incidents) and draw corresponding conclusions. The danger is that new findings often simply lead to the introduction of an additional safety system. Such overlapping renders the system as a whole more complex and thus less transparent for human beings.

Incident reporting systems:

Learning from other peoples mistakes

Analyzing incidents has crucial advantages over the analysis of accidents. Incidents not only provide a far broader database, but also allow those involved to be questioned in detail, which is not always the case following serious accidents. In addition, the analysis of incidents identifies both conditions conducive to error and control mechanisms.

Accidents rarely happen without warning. The combination of disturbances and errors which contribute to an accident. As well as the period in which they occur, are usually unique; individual reactions and behavior are not, however,

Accidents often result from errors, which have occurred before. Disasters have been averted in the past because the chain of error was not complete. For example. An aeroplane flew into a mountain in poor visibility because the pilot had misinterpreted a map. Six weeks previously. Another pilot had made the same error. Because visibility was good on that occasion, the pilot had been able to change course in time.

Had the pilot pointed out the problems with the map following this incident, the other pilot might have beers able to read it properly. To draw knowledge from such experience and errors. NASA launched the Aviation Safety Reporting System (ASRS) shortly after this accident. The aim of the program is to collect and analyze data
involving incidents throughout the country from pilots, air traffic controllers, mechanics, flight personnel, etc.

Incident reporting:

Based on trust and motivation

The mere existence of an incident reporting system does not promote the efficient and active prevention of accidents. More important is the quality of the incident reporting system.
An indispensable element of this system is trust. The operator or pilot must be able to rely on the fact that reporting will not bring disadvantages of any kind. This reinforces the need for active nurturing and protection of the basis of
Trust. One small breach of confidence can lead to a breakdown in the entire system:
Those affected will no longer report incidents. For this reason, many incident reporting systems are anonymous.

Continued from page 5

The second key to the systems success is motivation: operators and pilots must be informed of why and how an incident should be reported, and what the consequences may be. Only when they have proof that their incident reports are helping to improve safety (in the forms of regular feedback) will they be sufficiently motivated to play an active role. Motivation leads to widespread involvement, which in turn gives the reporting system the necessary anchorage.
The quality of the incident reports is fundamental to the success of the system. It forms the basis for analysis. The results of which can then be implemented in the form of measures to improve safety.

Human beings:

A safety - or a risk - factor?

What importance should thus be attached to the human factor in complex reporting systems? Given the problems discussed in this study, it is extremely important to consider human beings not only as a (risk factor) but also as an essential (safety factor). Man should be supported in his function as a safety factor in the best way possible: by technology (system designers speak of (human-centered automation)). By regulations governing the use of technology. By training, and by an optimal working environment.

TEN COMMON MERGER MISTAKES

Source:- Aon Report

Recent research indicates that when mergers and

Almost exclusively on legal and financial matters,
Ignoring important issues surrounding employee integration
And transitioning. Clearly, companies need to be better prepared to
Handle the human aspects of mergers and acquisitions.
Following are ten culture-related mistakes that
Companies commonly make as they go through the
pre- and post-merger processes:

1. Failing to fully communicate to employees the reasons for the merger.

2. Failing to allocate sufficient time to promote the cross-business relationships needed to drive the merger

3. Neglecting to define clearly the future roles and responsibilities of key leaders

4. Failing to help people see the potential opportunities available to them in the combined organization

5. Overwhelming the acquired firm with requests for information

6. Failing to address skepticism at each company about

7. Ignoring or minimizing employee fears about possible workforce consolidation and suspicions that they will receive unequal treatment (In the absence of responses to such concerns, employees will supply ideas

8. Failing to develop specific plans for retaining key personnel ahead of time

9. Overlooking or ignoring differences in work practices at the merging businesses (These include communications. practices, conflict handling, risk-taking orientation, reward and incentive practices, values, team and workgroup relationships, and observance of formal hierarchy.)

10. Adopting an overly controlling management style as the means to ensure that goals and expectations are met (A much more effective strategy is to spark employee motivation with rewards and incentives.)

This newsletter been prepared and edited by

Gamal Sakr ACII

Dear Reader

If you have
Any subject for which you are looking to get more information Or
Want to receive this news letter on your e-mail Or
Have any contributions to the Newsletter

Send an e-mail to

gamal.sakr@mailcity.com