JACEK LUCZAK

Poznan University of Economics, Faculty of Commodity Science,
Al. Niepodleglosci 10, 60 967 Poznan, Poland
jacek. luczak@ae. poznan. pl

FROM QUALITY MANAGEMENT TO INFORMATION SECURITY MANAGEMENT. RISKS CONNECTED WITH IT CURRENCY

Running of each economic activity is always connected with some risk. The quicker and more dynamic economic subject develops, the more range and extent of risk rise. The concrete risk in a company is shown in different forms of given hazard changing in time. It can have an exterior form (for example as delayed components supply from contracting party) or an interior form (for example failure of computer network or control of assembly line).

Developments of the global market as well as teleinformation give a lot of new opportunities of economic activity running through automation of production and financial processes. That enables global and quick communication or making agreements at a distance. On the other hand we have to notice that running of economic activity on basis of teleinformation technology is connected not only with benefits, but also with some risks. In analysis made by Internet Security Systems, that was published in a report[5], after having followed 20 sectors of economy, that were attacked in second quarter 2003, as the most exposed to risk were recognized: services-24. 23% , finances and insurance-19. 43%, trade-15, 69%, production-10. 6%, public administration-7. 56%, food and pharmaceutics industry-5. 16%, information technologies 4. 26% and health care-2. 86%. Unquestionable range and extent of risks as result of using of teleinformation technology in enterprise is always connected with the subject of economic activity. It is obvious that importance of some mentioned in this article hazards in subjects such as financial institutions will be different from hazards in enterprise making pictures or company trading with specific products.

The basic message of this article is to draw readers' attention to still not noticed sphere of Quality Management. If we still underestimate this problem, it can provide to disaster on the market of services and goods as well as for customers self. There are really not many situations that could be caparisoned with loss of information. All the more these situations are becoming more and more common and unfortunately very hard to detect. Even if they already are detected they cause very serious hazards. It is easy to imagine all the legal and financial after-effects as well as loss of credibility in a company, that allowed to uncontrolled access of third party to database of account customer.

Information Security Management Systems-ISMS become of great importance in age of information, when information resources as well as human resources are one of the most significant parts in each organization.

Risks

Undoubtedly to exterior risks belong computer viruses that spread in local and extensive networks. It is already a past when the only one sign of virus activity was giving information about virus author, plying simply melodies or presenting visual effects on the computer screen. Now viruses activity is far more ominous and losses caused by them can be really serious and provide to specific consequences for an enterprise-from suffering damage to image through spending financial resources essential to bring back accuracy of systems running or in extreme cases to reconstruct information and wasting of work time. Nowadays viruses can not only destroy data, damage files content or deform data record on disk. They cause often unstable work of local network or complete paralysis of its disk and make it impossible for example to make use of databases or extensive network. Often these viruses spread not only within local network, but also in extensive network and infect because of that other computers for example on basis of data from mailbox book.

Most often we meet following types of viruses:

- disk viruses-nesting in sectors that include information about hard disk structure
- files viruses-spread together with executive files (* EXE, * COM, * OVL, etc.)
- macro viruses-viruses working and reproducing in environment of single application or even its specific version, spread through program's macro commands (text files, spreadsheets, e-mails)

In spite of viruses we can also meet other programs that in illegal way interfering in operations system can cause damages. They are:

- Trojan horses-programs that include hidden functions designed most frequently to make it easier to take control over computer without knowledge of its owner. Installing of Trojan horse on enterprises computer can cause making passwords available to wrong people
- worms-programs that can duplicate, using to this purpose computer network

Burglaries on enterprises servers in order to steal, delete, temporary immobilize or destroy data-this is the next very real hazard that has to be taken into account. There are many examples of it, but most important thing is, that entrepreneur should realize, that also his/her server/computer may be in danger. Nowadays burglaries occur not more only in very big companies-they can affect also small and medium enterprises, government or council organizations as well as private persons. As example we can remember a burglary that was made in 1992 by 22 old men from Krakow, that broke in local entrepreneur's computer and destroyed data worth 5.000 zl. Significant part of burglaries is made by young people in order to check them or come into being in circle of hackers. These people in most cases make modifications of web sides leaving behind them a trace in form of "I was here" and they don't destroy or steal any data. Independent of perpetrator's motives it is worth to remember about securities of data from possible theft or damage or even revealing information to other people. It is also important to remember that spending on securities should be adequate to losses that we can suffer because of burglary. It is difficult to show concrete actions, because risks are always dependent on branch, type of enterprise, range of using teleinformation technology and extent of running economic activity. In some companies it is enough to introduce everyday archiving of data, to buy facilities keeping equal level of voltage, to isolate critical data from enterprises network that has access to the Internet as well as creating procedures of access to sensitive data (both in electronic and paper form) on basis of competence division in economic unit. Not always introducing of such a scheme will be sufficient and possible for the sake of type, branch or character of enterprise. Because of that in other companies can be advisable to introduce biometrical access to rooms where sensitive data are stored, to buy specific equipment that meet security requirements.

In established security policy following techniques should be taken into account as hazards situated between exterior and interior:

- collecting by competition information about enterprise through searching rubbish is one of the oldest techniques in order to steal company data; about popularity of this method decides easy way of getting information as well as impunity in case of arrest

- using sociotechnique in order to get access to data (for example receivers, passwords etc.) is a method as effective as searching rubbish; the British research showed that for example in United Kingdom 70% of office worker are likely to trade their security for one chocolate and 34% give their password when you just ask them to do it[6]

To counteract sociotechniques it is most efficient to precise exactly procedures of access to data and their consistent applying without any exceptions.

To exterior risks belong undoubtedly:

1. Recruitment process of employees that in future will have access to company sensitive data. It happens that competition send under a pretence of finding a job a person whose aim is gaining confidential information.
2. Possibility of leakage of sensitive data in case of shortage:
   - division of network into segments and complying with techniques and appliances limiting and controlling access
   - establishing circulation of electronic documents as well as paper documents-preparing of documents circulation must take into consideration competence division in a company

In order to counteract leakages of information man should rise workers qualifications so that they are aware of that documents circulation doesn't finish in throwing documents into basket.

3. Policy should also specify what kind of information carriers employees are allowed to use and on what computers. It means to define own, adapted to enterprise's individual needs, clear criteria that must answer following questions: who, where, on what and when can use computer equipment. Procedures in this scope have to be clear defined as well as results of not to follow them.
4. To possible risks we can also include managing resources and systems using in a company. The report of above mentioned subject shows that in second quarter 2003 year 727 new gaps were introduced into database. Among new discovered gaps 209 represent a high level of risk (they enable instant remote or local access or getting logins/passwords in not authorized way), 377 a medium level and 141 a small level. Unfortunately the weakest cell in a chain is always a man operating a system. Even the best system or application must be updated after some time what in most cases belong to administrator's duties. The longer the delay in updating of a system and first of all of critical programs/places in which gaps connected with security were found, the bigger possibility of successful attack.

Conclusion

Using of computer technology in running of economic activity undoubtedly make it easier through supporting decision processes, automation of financial or production processes, offer new possibilities of development through on-line sale as well as make easier to communicate with contracting parties. In spite of unquestionable many benefits there are also a lot of risks, that entrepreneurs should not only be aware of, but also know how taking economy rules into consideration they can counteract them. When we construct security policy we should apply complex solutions, adequate in financial sense to possible hazards and losses that can result from them.

Established security policy should in a precise and unambiguous way specify behavior procedures in relation to each person connected anyway with using in company teleinformation system, and it shouldn't be any exceptions from this rule. The main point is first of all to specify exactly rights and duties of each user of teleinformation system included administrators of computer systems and member of leadership as well. Procedures of security policy should be updated as in technical development new hazards connected with using teleinformation technology will occur.

References

[1] http://news. bbc. co. uk
[2] www. hacking. pl
[3] www. mks. com. pl
[4] http://gtoc. iss. net
[5] http://gtoc. iss. net
[6] BBC News: "Passwords revealed by sweet deal" http://news. bbc. co. uk/1/hi/technology/3639679. stm
The Register: John Leyden "Brits are crap at password security"
http://www. theregister. co. uk/2004/04/20/password_surveys/