INFORMATION SECURITY AS AN ELEMENT OF SECURITY STRATEGY OF A COMPANY

Marian KPOCZEWSKI, Marek TOBOLSKI

Summary: A general definition of security, namely the state of peace, harmony and safe development, usually refers to a building. In case of information security we mean the totality of an information security system of a particular information or public institution. This term includes also the totality of information and processes which are to realize a company's interest. Fundamental aims that information security in a company has to accomplish is ensuring and maintaining this security at a particular time. Information and communications security is one of conditions that have to be met to ensure information security, but it is not its only attribute. Information and communications security is understood as a group of processes aiming to define, accomplish and maintain a particular level of confidentiality, integrality, availability, accountability, authenticity and reliability, namely attributes of security in information and communications systems [4].

Key words: security, threats, information, enterprise.

1. Norms, standards and tools supporting the maintenance and development of information security

Along with the development of information and communication systems in a computer network, there arose a need to standardize issues related to the security of these systems, especially information essential to their functioning (Figure 1).

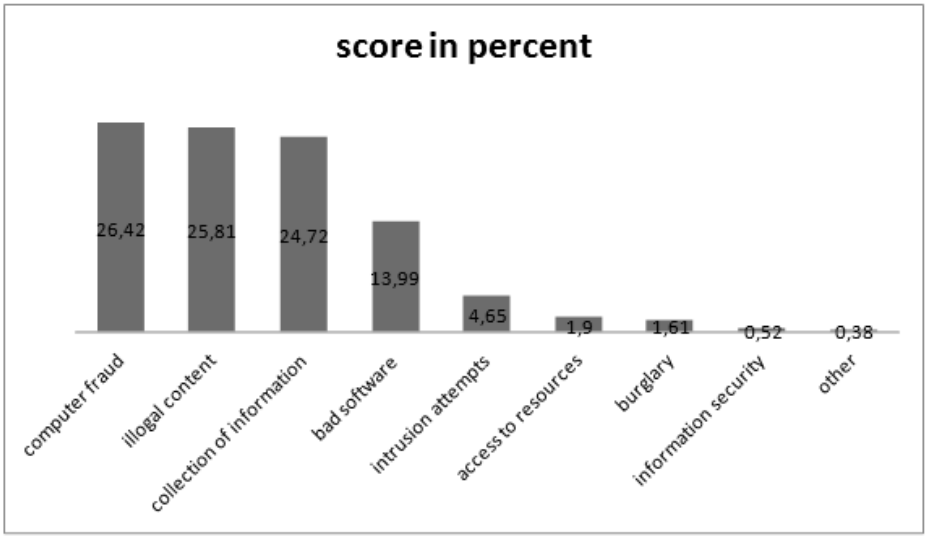

Fig. 1. Percentage distribution of issues related to information security

The main aim of standardization was to determine the methods of information protection, as well as to evaluate the effectiveness of actions based on these methods. First attempts to study this subject were made around the rapid development of informational technologies in the United States. The first mature document was Orange Book developed by the United States Government Department of Defense. Along with the development of technology, standards have been developed rapidly, they had the support of international communities as well as associations and other non-governmental organizations inspired by business. At present information security standards are updated on a daily basis, which is caused by a rapid technological development (Table 1). As far as this subject is concerned, numerous directives and recommendations, which include the term "standard" in their title, are being created. Therefore, it is appropriate to ask when such documents are standards and if standardization bodies have to participate in the process of their creation.

Tab. 1. Decriptinn of safety elements according to PN-13335-I standard

Name	Description
Confidentiality	This ensures that information is not made available or disclosed to unauthorized persons, entities or processes.
Authenticity	This ensures that the identity of an entity or resource is the same as has been declared; this is related to users, processes, systems and even institutions; authenticity is connected to investigations aiming to check whether somebody or something is what they say they are.
Availability	This is related to being available and ready to be used at a request within the specified timeframe by somebody or something which has the right to do so.
Data Integrity	This characteristics ensures that data have not been changed or destroyed in an unauthorized way.
System Integrity	This characteristics consists in a system fulfilling its intended function in its own expressive way, free from unauthorized manipulation, intentional or accidental.
Integrity	Data and system integrity.
Accountability	This ensures that actions of an entity (e.g. an user) can be explicitly attributed only to this entity.
Reliability	This characteristics refers to consistent, intended behavior and results.

There are plenty of standards which are understood as good practices or local recommendations of interested industry environments or audit companies, but the most general division includes the following standards [5]:

- Official – drawn up by standardization bodies, among which we differentiate:
- International organizations, e.g. ISO (International Organization of Standardization), IEC (International Electrotechnical Commission), ITU (Telecommunication Standardization Sector of the International Telecommunications Union),
- Regional organizations, e.g. CEN (Committee European de Normalization), ETSI (European Telecommunications Standards Institute), NAFTA (North America Free Trade Area),

– National organizations, e.g. ANSI (American Nations Standard Institution), SCC (Standard Council of Canada) or Polish PCN (Polish Committee for Standardization).

other – refers to all standards including recommendations of interested organizations, companies and industry associations.

Experience shows that such a division has a very symbolic nature. Some solutions developed by organizations or companies, when they have numerous supporters, are handed over to standardization organizations so that official standards can be drawn on their basis. This was the case for Ethernet network or electronic cards. What is more, there are examples of official standards, which did not catch on or were displaced by company solutions.

In order to ensure maximal data security, enterprises should undergo supervision and within their capabilities try to carry out inspection of security of own systems and solutions. The tools which facilitate the process of an automated installation process are automatic scanners. Scanners are equipment and software solutions which enable to perform a series of check-ups and attacks in order to find "holes" in software or equipment infrastructure in a short time. Using this kind of auto-testing of own IT infrastructure provides us with only a partial answer since the manner in which they operate is based on the search for known errors without analyzing errors in the manner in which this software is being used.

As in many other cases, it turns out that the weakest link in the sphere of information security is man. Nevertheless, using the abovementioned scanners significantly facilitates the recognition process and system safety regarding the vulnerable software parts. These products are not difficult to use and do not require specialist technical knowledge, and that is why such test can be carried out by technical personnel with medium-level qualifications. As a result of using such scanners, we gain detailed reports which should be analyzed in detail by appropriately trained personnel in further stages of the verification process. However, it should be kept in mind that they can detect only known errors which already are in the database of defined errors.

The most important issue exerting influence on the quality of a test is validity and completeness of the database of defined errors. Here we can make an analogy of antivirus software – the older the virus database is, the less effective and useful it is. The most common scanning system are [1]:

– ISS Internet Scanner – a comprehensive and very expensive tool.
– Axent NetRecon – a significantly simpler and cheaper solution, unfortunately also less precise.
– eEye Retina.

In the course of using automatic systems supporting security control, companies very often make mistakes which give them a false sense of security in a situation when the actual state is completely different. A quite common mistake occurring in organizations is using securing systems "at the front", but leaving "the back door" open through which all, even the most advanced protection measures. An important element that has to be taken into consideration as early as at the stage of IT solution design is maintaining an optimal level of security of the whole system. Even the largest investment in protection system infrastructure will not protect a company from threats of unauthorized access if software operating on these systems is out of date. As in many other spheres of life we need to remember that information security in our organization is as strong as its weakest link.

Another mistake which significantly decreases the level of security level is lack of knowledge or involvement in adapting monitoring systems or scanners. Installing a ready-

made solution, that is one with default settings, does not guarantee us full control and test adapted to our reality and expectations. Unfortunately, too often we trust technology and forget that it works only if we meet particular conditions. There is no such thing as universal technology which will protect everything. Some companies often say: "We have firewall so our network is secured". Of course firewall will protect out network but only on condition that it is configured to operate in our environment. Another example are encryption technologies. Using a public encryption key, such as PGP, we use the option of information encryption without a signature. This does not guarantee us the origin of e-mail – this is what the signature is responsible for. Moreover, when using encryption technologies we often forget about the rule that encrypted information is as safe as the encryption password. Unfortunately, sending encrypted information in an attachment together with a password is still a common practice. This kind of "protection" measure does not give us any guarantee of information security. Bearing in mind all of the abovementioned threats, it should be remembered that personnel training, their education in this respect is something even the most advanced protection systems cannot go without.

2. Information as a the most precious good in an enterprise

Information has a number of various definitions, depending on the field which defines it, it focuses on varying attributes and highlights its different meaning. From the perspective of an enterprise, for which information is or may be an important determinant influencing its financial effectiveness, information should be: complete, significant, timely, suitable, reliable and intelligible.

These features guarantee that particular information is significant for an enterprise. In the context of free market specificity, information has certain value at a particular time for particular business entities. It means that the information itself at different times may have extremely varied meaning, in some situations it may bring huge benefits to a company, in other ones it does not have absolutely any meaning in economic sense. From the perspective of a business entity which aims to pursue its business objectives, we may differentiate four areas of information security: administration-organization, formal-legal, technical-programming and physical.

Information security is nothing else than "information protection which consists in making it impossible and difficult to gather information on the physical nature of current and planned state of affairs and phenomena in one's own operating space and making it difficult to transferring information entropy to announcements and physical destruction to data carriers.

At each level of information security management [2]: strategic, tactical, operational and data processing, the basic aim is not to allow it to be disclosed. It needs to be highlighted that too broad understanding of security may hinder transfer of information in a country, company etc. – information that is necessary for their effective and successful functioning.

System for monitoring safety is a series of actions which can ensure information security only when they are linked and form a planned process. In such an arrangement, the whole system is as strong as its weakest link. Therefore, a security system is not effective without rules, procedures or monitoring processes. Information security is also each action, system or a method which secure information resources gathered, processed, transferred and stored on computers and in IT networks. That is why information security needs to be

understood as a result of physical, legal, personal and organizational, as well as IT security of a business entity [6].

The issue of information security needs to be perceived as a continuous process as part of which business entities improve their defense mechanisms which aim to increase the sense of safety. Actions taken when they are faced with a threat reflect enterprises' understanding of security and their approach to it. These actions are difficult and expensive, which unfortunately in many cases may be the reason why they are not taken.

3. The nature of information storage and protection.

Management of information system security has its aims whose accomplishment guarantees that a company's information security will be increased. These aims are related to three main areas of security:

- Knowing real threats to information system – for this purpose threats to which an information system is susceptible should be identified, threats linked to the security of this system should be known and evaluated.
- The system should be protected in a suitable way – by selecting appropriate methods of security management and security mechanisms which will be suitable for current needs.
- Monitor and maintain the established security level – by constantly monitoring threats and using security mechanisms and evaluating their effectiveness.

Achieving the abovementioned aims is not easy and often is connected to expenses, e.g. financial costs or costs related to infrastructure or the necessity to provide more human resources. Crime committed in business comprise a very specific group since by posing threats to companies or institutions, they pose threats to their resources, e.g. to databases, financial resources, or such values as reputation, relations or trade privileges of a

The term of information security threats of a company can be defined by identifying the following threat zones [7]:

- Chance threats – these include various kinds of disasters or accidents which directly influence information security of an organization.
- Traditional threats – these include diversion activities, sabotage or espionage. The aim of attacks of this kind is disinformation or obtaining information in an illegal way.
- Technological threats – these include all threats in which we deal with collection, storage and processing of information in computer networks. Cyberterrorism is a typical example of technological threats.
- Organizational threats – these include threats resulting from insufficient structural, procedural and organizational solutions.

The development of IT and the global market automatizes production and financial-accounting processes, enables global and fast communication and makes it possible to conclude agreements between contracting parties at a distance. However, we should not forget that running a business entity on the basis on information and communications is related to both benefits and risks. Information systems aim to collect, storage and make data available quickly. Their size and quality, and above all their origin, are of interest not only to special services and other institutions which are potential opponents, but also terrorist organizations and individual persons. Information systems can be threatened by everybody who has appropriate level of knowledge and skills [8].

4. Risk management as one of the most effective methods of increasing information security

Using information technologies to accomplish business tasks often carries some risk, sometimes of chance and unpredictable character. As a result, it is difficult to predict them or to repeat them in a controllable environment. What is more, they may be dependent on various so far unknown reasons. Bearing the company's good in mind, and, as a result economic profit, we may not allow the harmfulness of the abovementioned phenomena to influence the quality of business processes. In this sense risk is what we should try to limit, but first we have to evaluate this risk, its influence and character. The basis for creating and maintaining an information system is a well-targeted risk management process, whose fundamental task is precisely to limit it. However, it needs to be noted that the issue of risk analysis is not related only to information and communication. A number of other fields in case of which the influence of unpredictable events may have negative effects assume the need for risk analysis, e.g. the construction sector, the investment sector, the insurance sector and the aviation industry.

In all of the abovementioned sectors there is a need for the analysis of the influence of co-related and unknown factors on the occurrence of an unexpected event, whose effects may sometimes be even catastrophic. It is difficult to imagine that airplane manufactures will not conduct a thorough risk analysis in the implementation of new IT systems responsible for controlling a plane. Proper definition of threats is a basis for ensuring information security in an enterprise. The source of a threat can also be a person who is a threat or who creates a sense of a threat. The main risks related to information security in a company are defined as [3]:

- The risk of losing confidentiality – an event which may result in disclosing information processed by an information system to a non-authorized user.
- The risk of losing availability – an event which may result in the lack of access to an information system, program or information for authorized users at a particular time.
- The risk of losing integrity – an even which may result in an authorized modification or destruction of data processed by information systems.

The development of information technologies creates favourable conditions for criminal activities. New solutions on one hand support decision-making processes at various levels of organization management, on the other, are related to new qualitatively threats. Such threats may disturb personal, material, financial and information resources.

5. Conclusions

On the basis of own experience and research related to running a business activity in „X" company it needs to be noted that the awareness of the need for risk analysis is immense. Observation shows that to ensure the highest level of information security two risk assessment methods are used:

- The qualitative method – it evaluates risk as low, medium, high or critical.
- The quantitative method – it evaluates risk by means of particular measurement units, e.g. multiplier of probability as a measurement unit of contractual penalties.

In order to determine the probability of occurrence of events appropriate sources of information are used, e.g.:

- statistical data collected by a company itself – in this case experience of a company in a particular line of business is of key importance,
- statistical data collected by other organizations operating in a similar line of business. In this case, however, some caution is maintained,
- expert assessment – it merit is that easily available; nevertheless, it may be subjective,
- expert assessment corrected by various methods, e.g. Delphi, which enables to increase the probability and accuracy of analysis.

On the basis on a long experience, X company has created a very reliable base of indications which enable to evaluate business risk of its business activity in the outsourcing sector. Risk analysis methods in X company are used in various kinds of company activity. The company's own methodology, which is based on the highest standards in risk analysis is used both to evaluate the level of information security in information systems as well as to evaluate investment. X company has specified aims related to risk management, namely:

- ensuring an undisturbed accomplishment of tasks and business processes which result from the company's mission by improving the protection of resources which are used to send, storage and process information,
- making it possible for the management to take optimal decisions related to expenses, investment in infrastructure and protection.

This article is an attempt to evaluate the level of information security in X outsourcing company. Because of the character of this company, it is a very serious aspect since only the highest level of information security guarantees continuity and high quality of business processes implementation. Thanks to the analysis of the collected research material it was possible to draw conclusions.

Employees who are involved in the process of information processing in this company are aware of information security and are appropriately trained in this respect. The company has suitable training systems of employees as well as document management system which are computer-assisted. These systems are included in access protection which guarantees control of access.

The technical level of securities comply with high safety standards and is resistant to potential attack from the outside. The company has implemented a number of standards, related both to control of access to devices, facilities and software. There is high awareness of the need for risk analysis and risk management in the company. What is more, there are procedures which order the process of risk management in many areas and at many levels of organization. High awareness of risk management is observed both in case of specialists and engineers as well managers which is of key importance because of an efficient decision making process related to investment in this respect.

Critical infrastructure is diversified to protect the company against various threats which could have a negative influence of the continuity of business processes. What is more, critical infrastructure is included in the documenting process and cyclic reviews.

The level of information security in companies is getting more and more important along with technological development, which is caused by the need to ensure security of business processes. If, in reference to the thesis formulated in the introduction to this paper, we will point to two key areas related to information security, namely infrastructure and people, then in case of this company both of them operate effectively and comprise a secure system which enables us to be sure that information stored and processed in this company are secured.

Literature

1. Białas A., Information and service security in a modern institution and company. Warsaw 2007.
2. Borowiecki R., Kwieciński M., Monitoring the environment, transfer and security of information. In the direction of a company's integrity. Warsaw 2003.
3. Kopczewski M., The elements of critical infrastructure of a country (organization) as objects exposed to cyberterrorism attacks. A web script.
4. Koziej S., Introduction to the theory of security. Warsaw 2001.
5. Lidel K., Information security. Kraków 2008.
6. Łuczak J. (ed.), Management of information security. Poznań 2004.
7. Kuta M., The policy of information security in a company – practical aspects, [in:] Borowiecki R., Kwieciński M., Monitoring the environment, transfer and security of information. In the direction of a company's integrity. Warsaw 2003.
8. Żebrowski A., Kwiatkowski M., Information security in the Third Republic of Poland. Kraków 2000.

Prof. Marian KOPCZEWSKI, PhD, Eng.
The Director of Security Sciences Department
University of Security in Poznań
ul. Elizy Orzeszkowej 1
60-778 Poznań
e-mail: marian.kopczewski@interia.pl

Junior brigadier Marek TOBOLSKI PhD, Eng.
The office of Military Fire Protection in Bydgoszcz
ul. Warszawska 10
85-915 Bydgoszcz
e-mail: marektobolski@tlen.pl