MILITARY UNIVERSITY OF LAND FORCES

Scientific Journal of the Military University of Land Forces
ISSN: 2544-7122 (print), 2545-0719 (online)
2019, Volume 51, Number 1(191), Pages 25-34
DOI: 10.5604/01.3001.0013.2396

Original article

Information security – its essence and threats

Estera Pietras

Faculty of Production Engineering and Materials Technology,
Institute of Metal Forming and Safety Engineering Czestochowa University of Technology, Poland,
e-mail: estera.pietras@wp.pl

INFORMATIONS

Article history:

Submited: 23 March 2018

Accepted: 21 October 2018

Published: 15 March 2019

ABSTRACT

Due to the exchange of information, organizations are encouraged to create an effective system of information flow that should be monitored on a regular basis in order to minimize the risk of emergence of threats. Due to modern technical solutions of security systems, it is much more possible and accessible than a few years ago. For this purpose, proper identification and classification of threats is necessary. This constitutes the starting point for considering the role and the essence of risk. The article highlights the aspects related to ensuring information security as a whole and data protection – the most important assets of business entities.

KEYWORDS

information security, information security threats

Introduction

The sense of security is a man's original and primary need. Its absence creates anxiety and a sense of threat to life, health, property loss, etc. The analysis of the literature of the subject indicates that the two above mentioned elements are closely related. The more threats exist, the lower the level of information security is at a workplace, and if the situation is opposite, the fear of losing important business information is significantly reduced. Thus, these two factors are two opposite poles of social phenomena. Awareness of security is interdependent with the threat or the lack of it. The sense of security is consequently very important. This would not be possible without certain information, owing to which one can gain meaningful knowledge about the impact of security on every person's life. Information plays a key role in the proper functioning of enterprises. Some information is less crucial and of smaller significance for a company, there is also that of strategic importance that can influence the development of an organization. Therefore, information security is a consequential issue. The understanding and treating security as a key area of social interests is reflected in decisions made in the face of threats. The development of information technology brings real risks of asset loss in an enterprise through so far unidentified threats. Proper identification of elements of social security threats provides the basis for identifying changes in the security system. The literature of the subject shows that a threat is a situation or condition that threatens someone or in which someone feels threatened [1]. In the era of the computer technology development where everyone should feel safe, leaks of inadequately protected information have become the reality through threats such as: espionage, computer crime, hacking into the computer system, eavesdropping, or the like. The article presents key concepts related to security of information stored in ICT systems and networks, as well as contains information regarding exemplary information threats that significantly reduce the reliability of ICT systems.

1. Information security

The literature of the subject provides many definitions according to the typology of a threat. The most common definition describes information as everything that the mind is able to process and accept to carry out activities, in particular business ones. These are assets that, like other important business assets, are essential to the business activity of an organization and adequate protection is therefore recommended for them. An organization processes information outside and inside. Examples of such processing include invoices, contracts, input information and agreements with contractors. Therefore, information is the wealth of a modern enterprise. In order for a company to succeed on the market, it is obliged to look for appropriate instruments of data protection. The answer to this need is information security management that gives the optimal level to information security in an organization, as well as accessibility for selected enterprises. In information systems, information security management involves a set of processes that go in one direction, which is to increase and maintain the existing level of security. This level can be reached by defining strategies and objectives within a given organization detecting and analyzing threats, detecting risks, introducing adequate security measures, controlling the process of introduction of protective measures, identifying incidents and their final elimination.

Increased awareness of the value of information and its security is reflected in the dynamic development of international standards for information security management systems [2]. The norms PN-ISO/IEC27001:2014 and PN-ISO/17799:2006 define “information security” as “preservation of confidentiality, integrity and accessibility of information”. In addition, the following security attributes are taken into consideration: authenticity, accountability, undeniability and reliability [3].

Each of these attributes should be prioritized and have the same value, as all of them are important for sufficient protection of information. The purpose of information security is to ensure the stable operation of the information system, confidentiality of data processing, protection against modification and cost reduction that can be generated attack of the information system. Proper identification of elements of security threat emerging in an enterprise constitutes the basis for introducing changes in the security management system and ensuring its adequate level in an organization. Figure 1 presents the main components of information security and areas where they can emerge.

Table 1. The definitions of attributes of information security and its properties according to PN-13335-1 [4]

Confidentiality	It guarantees that information is made available to authorized entities, in strictly defined situations and in a specific way. Any failure to comply with the confidentiality requirement may violate the privacy of other persons.
Integrity	Protection of the inviolability of information stored in the system.
Accountability	It is associated with an unambiguous assignment of a specific scope of action to one entity.
Data integrity	Assurance that data has not been replaced in an unauthorized way and that it is accurate and complete, thus everything valuable to an organization.
System integrity	Assurance that the system performs its functions in an inviolable manner.
Authenticity	Assurance that the identity of an entity or resource is corresponding to the declared one (this applies to users of processes and systems). Implementation of the undeniability principle guarantees that a sender cannot deny the fact of sending the information, while a recipient cannot deny that he/she received the information.
Reliability	It means permanent, consistent and intended behavior and effects.
Accessibility	It assumes the possibility of authorized use of data and information at a desired time, in an expected way.

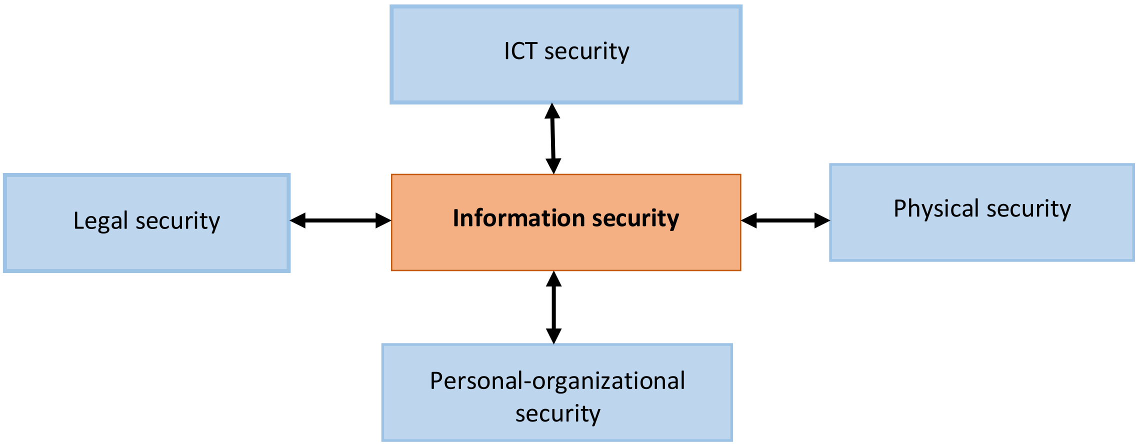

Fig. 1. The main components of information
Source: Own study based on [1].

The literature of the subject states that the value of information security is a set of activities, methods and systems, the main purpose of which is to secure collected and processed information in networks and ICT systems [5]. Therefore, according to the author, data security is reflected in the protection against destruction, disclosure and modification of data. The components of information security and their mutual relationships are thus crucial. The key elements include network, data and computer security.

Table 2. The characteristics of the components of information security [4]

Components of information security	
ICT security	It means the protection of computer systems, electronic data and data transmission, as well as the protection of information against destruction or intentional disclosure. It is the physical protection and access control (passwords and logins), which ensure such security.
Physical security	It includes an accurately conducted risk analysis in which threats will be identified, connected to adequate means of physical protection (safes, cards and gates), electronic protection (monitoring, fire alarm system and means of active protection (security staff and interventional employees), as well as protection of equipment and rooms against physical factors such as: theft, flood and fire.
Personal-organizational security	It includes procedures related to access to protected information by designating authorized person with access to rooms in the protected area. It is therefore vital to training and educating employees about the responsibility for data security in a company. Another important factor are procedures related to organizational activities in a company, for example, a cleaning lady's access to rooms located in the protection area.
Legal security	It means action compatible with legal regulations that concern proper security of information while it is being processed. Aspects of data security are identified with regulations regarding personal data or, for example, classified information. Organizations are obliged to process information and store it according to guidelines included in legal acts.

According to the author, all components of information are significant but the key to proper enterprise protection against threats will be, however, personal security due to the crucial role of human and his/her behavior. Economic practice shows that the personnel may include persons who do not contribute to a company, do not follow instructions and orders, and as a result of the lack of sufficient knowledge usually choose the "shortcut". For the success of an enterprise on the market depends on the personnel and their active attitude towards needs and changes in the organization. The remaining components are only supporting. As indicated in the PWC report, "company employees were the source of 79% of the cases of detected incidents related to violation of information security, while 62% of cases involved hacker attacks".

2. Identification of threats

One cannot protect him- or herself against unknown and underestimated threats. It is therefore suggested to get to know the current, but also potential, dangers that may emerge in an organization. These threats can seriously jeopardize the results and prosperity on the market. An indispensable factor of the functioning of ICT systems in safe conditions is precise identification of threats. It is precisely the identification of threats that allows to determine the scale of complexity of the security problem analyzed as well as to indicate the main causes of the system failure. Identifying existing threats in an enterprise and indicating its supposed occurrence may concern accidental threats, but also those carried out in an intentional manner, for example, by human. Examples of such threats caused by human include, among others: theft, unauthorized disclosure, alteration, destruction and loss of data. There are no infallible people, thus it is only possible to reduce a human error to some degree. Just a few decades ago, ensuring the proper level of information security was not such a difficult task as it is nowadays.

The PN-I-02000:2002 norm provides the definition of a threat as: "a potential possibility of an ICT system violation". The literature of the subject indicates the following sources of threats:

- cultural,
- technological,
- ecological,
- economic,
- existential,
- political,
- informational [5].

The origin of a threat can have a natural or human character. Detection of danger is a very important aspect, as it gives an opportunity to counteract the undesirable consequences. The basis for detecting threats impacting the level of security will be the identification of changes occurring in the information security system [1].

According to areas of threat emergence, the following can be distinguished:

- Random threats – which include: accidents, natural disasters affecting the state of organization and the safe flow of information, for example, fire in a building where data carriers are located, atmospheric discharges, air pollution and failures to the power supply system.
- Traditional informational threats – which include: sabotage or diversionary activity as well as economic espionage aimed at gaining information.
- Technological threats – which include: collecting, processing, transferring and storing information in ICT networks and systems of an organization, for example, computer crime [1].

The next criterion for the division of informational threats is the source of their occurrence. Hence one can distinguish the following:

1. Internal threats emerging in an enterprise, inside an organization using a computer system. This group includes:
   - damage or loss of data, or a total lack of possibilities to process them due to an error or accident,
   - damage or loss of data caused by intentional activity of unauthorized persons, an error or accident,
   - erroneous operation on the part of a data base administrator or an operational system administrator,
   - incorrect configuration of the system, faulty hardware and software.

2. External threats arising outside the company. They include damage or loss of data and interference by third parties. They can lead to the lack of possibilities to operate a system or network.
3. Physical threats are often a result of a catastrophe, malfunction or occurrence of an undesired event impacting the information security of a given organization [6].

Threats connected to information security are mainly caused by rapid development of technology. It has forced organizations to comply with information security solutions. However, it should be borne in mind that this continual development of technology will not eliminate old threats, but it can make them easier to neutralize. In contrast, technological development will condition the emergence of new threats. The distribution of threats is shown graphically in Figure 2.

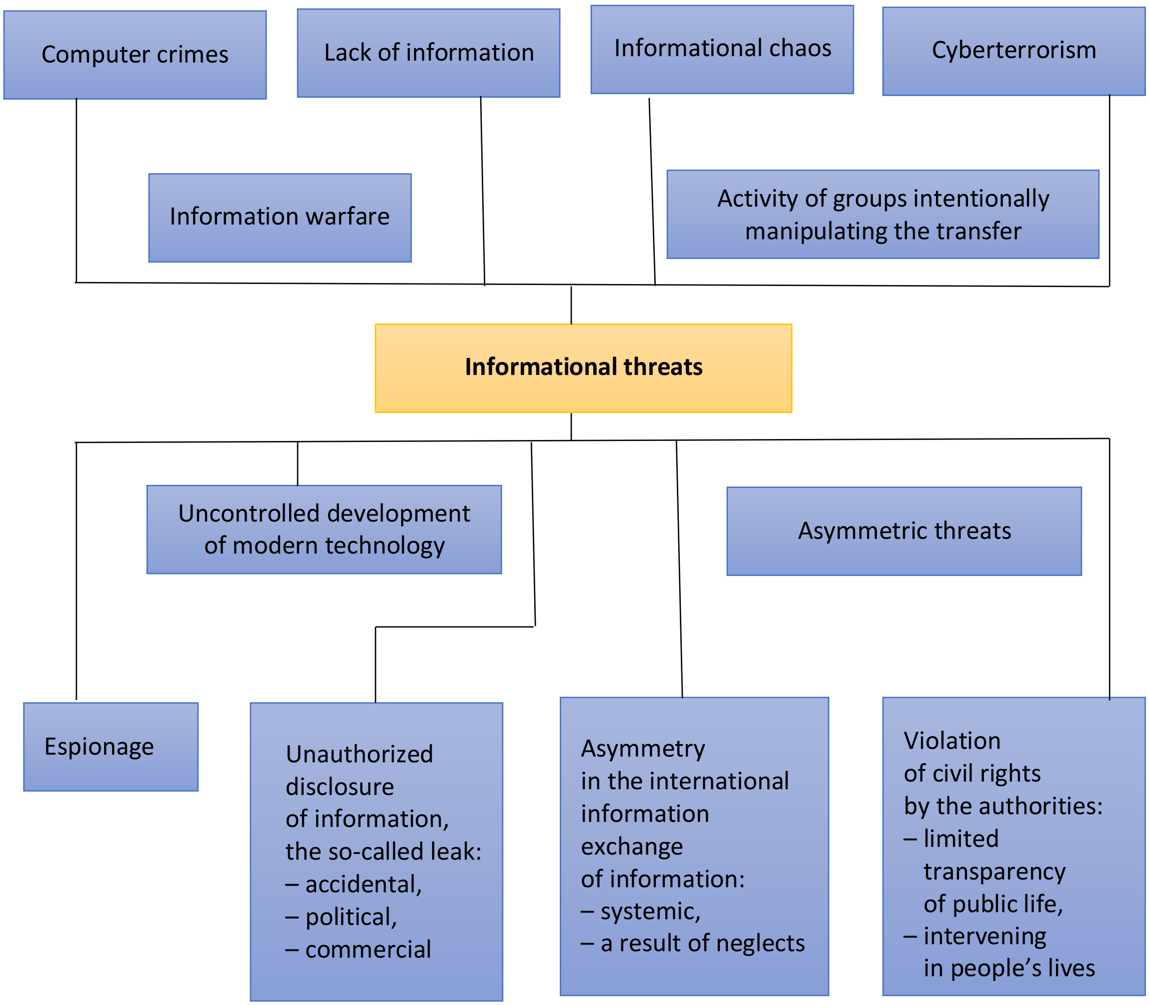
Computer crimes
Lack of information
Informational chaos
Cyberterrorism
Information warfare
Activity of groups intentionally manipulating the transfer
Informational threats
Uncontrolled development of modern technology
Asymmetric threats
Espionage
Unauthorized disclosure of information, the so-called leak:
– accidental,
– political,
– commercial
Asymmetry in the international information exchange of information:
– systemic,
– a result of neglects
Violation of civil rights by the authorities:
– limited transparency of public life,
– intervening in people's lives

Fig. 2. The distribution of informational threats in a developing company
Source: Own study based on [1].

ICT security plays a significant role in the proper prospering of an enterprise. Besides security, it generates numerous dangers associated with information phishing. The development of ICT has given human a range of opportunities for deliberate action to disclose information. The security of ICT systems and networks includes a number of initiatives that prevent unauthorized persons from accessing valuable information by intercepting radio signals or analyzing traffic in radio networks. Informatization of bank systems, electronic transfer of money and computerized accounting systems already exist in every enterprise. Today, integrated systems combine the accounting-financial department with a warehouse, production or cadres [7]. The security of communication systems consists of: transmission systems and security of means that impede and aim at physical protection of communication systems [8].

According to the map of historical events from the PwC Report, in 2016 as many as 96% of Polish medium and large companies noted more than 50 incidents related to violation of information security or IT systems. For 64% the number of such events was greater than 500. As indicated by the report, "the most commonly used method of cyber-attacks was a phishing attack (39%), intended to mislead a user and persuade him or her to performed the intended operation. The use of IT systems was on the second place (35%) and the use of an external data carrier on the third (23%). Among the most severe effects of cyber-attacks, the respondents indicated: exposure to legal risk and financial losses as well as loss of customers and theft of intellectual property. At the same time, as much as 55% of companies are not aware of the kinds of effects of cyber-attacks on data in their business organizations" [9].

More than half of attackers are commercial companies, thus new requirements emerge for organizations that focus on information protection [10]. The literature of the subject distinguishes the following attacks:

1. Active – the so-called active influence on the system, direct or indirect modification of data flow.
2. Passive – lack of active influence on the system (eavesdropping, observing and analyzing network movement).
3. Unauthorized access to classified information that is stored and processed.
4. Unauthorized impact on the system, which can lead to changes in the functioning of ICT networks [1].

Fast communication and technological development have made it possible to sign agreements between entrepreneurs from around the world. Nonetheless, it should be borne in mind that it has consequences in the form of threats and attacks from each side.

When analyzing individual threats such as: fraud, computer forgery, computer sabotage, destruction of data and computer programs, hacking into computer systems, attacks on computer systems and computer eavesdropping, we are dealing with the most dangerous threats affecting the level of information security. Most of the time, factors causing these threats are intentional or result from personnel's unawareness. Threats are formed on different grounds in an enterprise. It should be noted that the cause of this situation could be a result of the lack of sufficient knowledge about information systems security or inexperience on the part of employees. The author of the article pays attention especially to some of computer threats.

Table 3. Selected computer threats

Name of the threat	Description of the threat
Destruction of data and computer programs	Placing a segment of self-replicating code, i.e. virus or executable program, the so-called Worm, in programs. Besides system intrusions, computer viruses, i.e. programs that have the ability of self-replicating and copying from one computer to another without the user's knowledge, are the most common threat. Taking into account various user mistakes and program errors, it can be concluded that almost every system can be threatened by different types of viruses which include, for example: a logic bomb and a time bomb.
Computer forgery	In the first version, it is used for falsifying paper documents, a printer, a computer and software. Due to properly selected equipment, one can easily falsify original documents while maintaining the characteristic traits of a print. The second version is concerned with electronic files that are stored in computer memory or on data carriers. Electronic documents are even more susceptible to change than traditional ones.
Computer fraud	They are directly associated with data manipulation based on entering incorrect information into a data base which allows to modify storage statuses, illegally grant a concession or falsify an annual balance sheet. Manipulation that relies on operating in publically accessible electronic devices uses, for instance, terminals. Manipulation of programs is based on transforming commands or writing new ones that in turn cause a program to perform operations by itself, which the user does not have an influence on. This type of manipulation is difficult to detect [7].
Attacks on computer systems	It is an easy way to gain information, fully controlled via the Internet. The most frequently used computer attacks include: 1. Viruses that can even disable thousands of computers. 2. Viruses that are asleep in a computer and act like hackers, whose attack does not have to be controlled. While using email or popular websites, it infects the system by installing itself on other computers. Logic bomb that can often remain inactive but presence of some files can activate it.

Source: Own study based on [7].

In the 21st century, hackers do not need as much equipment as before to break into the information system. Even the more and more complicated information systems have vulnerabilities, which in turn allow unauthorized persons to gain access to information.

Conclusion

Nowadays, enterprises conducting business activity are exposed to information theft. Information has become an asset of prosperous organizations that can determine their success on the market. It is important to realize that even if a particular enterprise does not use business intelligence tools, competitors may conduct such activities. Threats should be expected from both outside and inside of an organization, bearing in mind that the human factor is the weakest element in information protection, as it is attacked from all sides by various methods and practical activities aimed at provoking specific behaviors and social attitudes. According to the author, it is the leaks and errors in the proper training of employees that cause threats resulting from the human factor. It should be noted that new technologies are in possession of both entrepreneurs and persons who want to steal and modify information. It is the employer's responsibility to educate organization's employees about the value of information as well as the consequences posed by loss of that information. The multifaceted nature of this problem is shown by identification of potential information security threats. To sum up, only a sound risk analysis and complying with guidelines can reduce the loss of valuable information and data. Thus, it is unacceptable to ignore any threats, even those underestimated, in an organization. One cannot fully protect him- or herself from the phenomenon of attack techniques or use any classification because new attack methods appear every now and then. This indicates the broad scope of the issue. According to the author of the article, it seems necessary to identify and evaluate threats, both current and potential, not yet identified ones.

Acknowledgement

No acknowledgement and potential founding was reported by the author.

Conflict of interests

The author declared no conflict of interests.

Author contributions

The author contributed to the interpretation of results and writing of the paper. The author read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.

ORCID

Estera Pietras – The author declared that she has no ORCID ID's

References

1. Wrzosek M, Nowak A. *Identyfikacja zagrozen determinujacych zmiany w systemie bezpieczenstwa spoleczenstwa informacyjnego*. Warszawa: Akademia Obrony Narodowej; 2009.
2. Janczak J, Nowak A. *Bezpieczenstwo informacyjne. Wybrane problemy*. Warszawa: Akademia Obrony Narodowej; 2012.
3. PN-ISO/IEC 27001:2014, *Technika informatyczna – Techniki bezpieczenstwa – Systemy zarzadzania bezpieczenstwem informacji – Wymagania*. Warszawa: PKN; 2014.
4. Nowak A, Scheffs W. *Zarzadzanie bezpieczenstwem informacyjnym*. Warszawa: Akademia Obrony Narodowej; 2010.
5. Baczek P. *Zagrozenia informacyjne a bezpieczenstwo panstwa polskiego*. Torun: Wydawnictwo Adam Marszalek; 2006.
6. Zebrowski A, Kwiatkowski M. *Bezpieczenstwo informacji III Rzeczypospolitej*. Krakow: Oficyna Wydawnicza Abrys; 2000.

7. Fischer B. *Przestepstwa komputerowe i ochrona informacji*. Krakow: Kantor Wydawniczy Zakamycze 2000.
8. Prauzner T. *Technologia informacyjna. Wybrane problemy spoleczne*. Edukacja, Technika, Informatyka. 2012;3(pt2):39-44.
9. PwC Polska, [online]. Available at: www.pwc.pl [Accessed: 2 October 2017].
10. *Raport CP2007*, [online]. Available at: www.cert.gov.pl [Accessed: 10 October 2017].

Biographical note

Estera Pietras – M.Sc. Eng., Czestochowa University of Technology, Faculty of Production Engineering and Mater als Technology, Institute of Metal Forming and Safety Engineering. Participant in conferences and information security trainings. The main areas of her interest include security engineering and information security management.

Istota i zagrożenia bezpieczeństwa informacji

STRESZCZENIE Z uwagi na fakt wymiany informacji organizacje zachęcane są do utworzenia skutecznego systemu bezpiecznego przepływu informacji, który powinien być na bieżąco sprawdzany, aby zminimalizować ryzyko pojawienia się zagrożeń. Dzięki nowoczesnym rozwiązaniom technicznych systemów zabezpieczeń jest to dużo bardziej możliwe i dostępne niż jeszcze kilka lat temu. W tym celu niezbędna jest właściwa identyfikacja i klasyfikacja zagrożeń. Stanowi to punkt wyjścia do rozważań dotyczących roli i istoty ryzyka. Artykuł zwraca uwagę na aspekty związane z zapewnieniem bezpieczeństwa informacji jako całości i ochrony danych – najważniejszego dobra jednostek gospodarczych.

SŁOWA KLUCZOWE bezpieczeństwo informacji, zagrożenia bezpieczeństwa informacji

How to cite this paper

Pietras E. *Information security – its essence and threats*. Scientific Journal of the Military University of Land Forces. 2019;51;1(191):25-34.

DOI: http://dx.doi.org/10.5604/01.3001.0013.2396