EasyChair Preprint

№ 1993

Company Security Information Management Systems

Kamil Andrzejewski

November 19, 2019

COMPANY SECURITY INFORMATION MANAGEMENT SYSTEMS

Kamil Andrzejewski[1]

Abstract: Article indicates the literature outline of the scientific field of management sciences depend issues of security management in the organization. The article focuses on identifying literature in this area and accurately describing the process in terms of the essence of management in the organization. Accurate authors who became pioneers of the subject were pointed out and also pointed to the important roles of the approach to information security management in the process of building and organizational development of the enterprise. At the end of the article, the author enters into discussions with other authors in the selection of the optimal strategy for managing security in an enterprise and shows how it effects for money at company and intangible market value.

Keywords: security management, information, company value, assessment of the stock market and market value of the organization, legal security, cyber security, security context.

INTRODUCTION

Security communications management is great importance in the development of every small and large organization in the 21st century. Scientists have become very interested in this research problem in the years 2012 to now. Security management has been the subject of research of scientists for twenty years in the field of protection of countries, cities, employees, including work in an organization. However, since 2012, there has been a noticeable trend in the very high dynamics company development in the field of technologies that may be theft of other market players. The safety management process is important in the field of management sciences and also in terms of the communication process of interest groups in the organization. The consequences of not having a security strategy in your organization may result from bankruptcy to serious legal and financial consequences. The cause and effect of erroneous security manager with management board on company. Must be aware of the importance of dynamics of technology and process development and their protection in terms of secure data

[1] Kamil Andrzejewski, PhD Candidate, Wroclaw University of Economy, e-mail: kamil.andrzejewski@ue.wroc.pl.

flow and secrets in a group of employees, suppliers of all area of company. The process of safety management in the field of management sciences is important if the organization refers to the prepared security strategy and the system of values company.

Organizational security should be considered in many dimensions. In this case, the authors describing the problem focus on the process of thorough transformation of the organization in terms of the work of the board, human resources, production works, physical protection and IT. The definition of security is many how they economics school of business, however, the most accurate is quoted by Fehler describing security as subject of " process having a dynamic nature and state in which a given entity not only high level access entry to company. Including the certainty that this access will not be worse in the future, and the disturbances appearing in this area will be effective dismissed or removed "[2] . The rapid development of information collection and storage processes in the organization has given a new field in the use of secure information among employees and suppliers. Not referring to unchecked information in the process of improving security (false news) results in the fact that "in every area of economic development, significant importance has been attached to the issue of information security and importance in the process of the organization cycle."[3].

According to Liedel, information security management is described as "constant control by practitioners against unwanted accidental or deliberate disclosure, modification, destruction, processing outside the organization"[4].

SECURITY MANAGEMENT COMMUNICATIONS PROCESS IN THE ORGANIZATION PERSPECTIVE

[2] W. Fehler, *Bezpieczeństwo przestrzeni publicznej.* [w:] *Bezpieczeństwo publiczne w przestrzeni miejskie,* red. naukowa: W. Fehler, Arte, Warszawa 2010, s. 16

[3] A. Suchorzewska, *Rozdział I. Społeczeństwo w dobie rozwoju sieci teleinformatycznych 6. Współczesne zagrożenia informacyjne,* [w:] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmu,* Oficyna 2010 LEX.

[4] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2005, s. 19.

Long term security at organization of safety communication is its primary problem of many organization in the world. The process of providing information in the field of security refers to its security where I have no risk that the information will flow outside the enterprise and employees. Beskosty describe this definitions it is "(…) information can be provided from many sources, including credible and unreliable. During its journey, it undergoes transformations and its value changes. Confidential information involves sharing only with those institutions and groups of people that are necessary for this process. The entity also has the right to refuse access to information to persons who do not have the rights and are not called to do so. Information from a reliable source is associated with its integrity over a period of time it has not been distorted and has not lost its value in the modification process"[5].

The participation of security departments within the administrative structures of the European Union is also important in this process. Procedures have been indicated to local national Standardization Committees of the member states to what extent they are to define information security in the organization. Guidelines for maintaining standards in the scope of:

- "availability of information - scope of authorizations and access;

- integrity - this applies to information processing methods

- confidentiality - scope and competence of people with or without access to information "[6].

Most of organization has a challenge to check all information that may have a key impact on the final product or service. Bączek refers to information security in terms of the state's operation as an organization. In this case, you can see frequent dependencies and the same problems in "internal and external issues based on true, reliable and timely information. The flow of data and the protection of information also

[5] M. Beskosty, *Zarządzanie bezpieczeństwem informacji,* „Studia nad Bezpieczeństwem" 2017, nr 2, s. 164.-

[6] Polski Komitet Normalizacyjny. „Technika informatyczna. *Praktyczne zasady zarządzania bezpieczeństwem informacji".* PN-ISO/IEC 17799, Warszawa 2013, s.10.

sensitive by law is protected by the country or state. Information about citizens, organizations and their activities has no right to violate established legal norms. Citizens they are also employee representatives (control offices, media, deputies) have some knowledge and information about the operation system at company. They work and have relations with another people"[7].

The security of information management aims to take into account the purpose of disclosing content and the effects of its use in the organization. The exact division of information management has an impact on the operational activity of the enterprise and results in making group decisions in the field of information protection against unauthorized use outside or transferring data to a competing organization. The information has attributes and transmission validity schedule.

In this case, the company is required to create accurate procedures for the provision of information, secret and classified data system, indication of persons who have the right to legitimately disclose or not disclose information. The competence procedure also applies to full information control and access to it within the scope of the entire organization. All information must be carefully processed and evaluated in terms of limited access to it in terms of the need to have this knowledge.

Other information is needed for CEO and CFO also technology director, production employee. However, information is most important connect with security management. Always affect the content of information and communication and trust become acquainted with who and how it uses knowledge and how it has a purpose in this activity.

INFORMATION SECURITY PROTECTION WITH PROCESS ORGANIZATION MANAGEMENT

The information management process is related to all areas of work in the organization. In this case, it is the security legal department, IT department, human resources, production, transport, which is significant throughout departments. Entire maintenance process by management and organization in the field of enterprise operation. Security management has its own plan to implement and maintain the process in terms of department evaluation, organization communication policy,

[7] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego,* Toruń 2006, s. 74.

control of accurate cost and risk accounting for the daily improvement of security processes. In his article, Ożarek presents what is the Information Security Management System (ISMS) known as "management subsystem that functions in well-functioning organizations. Showing the safety management process without taking into account the management processes that take place in other zones and activities is not only impossible and pointless in the perspective of the organization's operation. "[8]

Suchorzewska defines security communications management as a permanent process that carries out missions to protect organizations in the field of the growing threats to the organization in a constantly changing economic environment and technological change. "The right choice of information security management model takes into account all forms of information data, including signature notes, cache records, information in the form of e-mail, ERP systems. All information that is displayed on the screen of company computers and laptops, including movies, photos, presentation"[9] .

However, the “optimal solution for information security management is not always included in the PN -ISO-EIC-27001 standard”[10].

Management operations and coordinating information security processes in all cases requires employees. All employee at organization they have detailed planned risk assessments and many select support procedures that can be used in a given crisis situation and in the future. Krawiec indicates that "information security management is effective data protection depending on information security policy and business goals. Assessment of employee and management involvement knowledge of security requirements management of tangible and intangible risks during data outflows or virtual attacks. It is important to effectively promote safety requirements and recommendations among employees and the external environment in relation to the organization. The organization should ensure an appropriate amount

[8] G. Ożarek, *System Zarządzania Bezpieczeństwem Informacji – budowa i wdrożenie*, [w:] *Ochrona danych osobowych w praktyce*, Polski Komitet Normalizacyjny, Warszawa 2013, s. 52

[9] A. Suchorzewska, Rozdział V. Przestępstwo cyberterroryzmu w polskim systemie prawnym 4. Ochrona informacji utrzymywanych w systemach informatycznych a bezpieczeństwo informacyjne państwa 4.3. Zarządzanie bezpieczeństwem informacji, [w:] A. Suchorzewska, Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmu, Oficyna 2010, LEX, s.24..

[10] Information technology – Security techniques – Information security management systems – Requirements, ISO, Geneva, 2013, s.13.

of training information security, including the establishment of an effective process for managing each incident related to the security of the entity in the organization"[11].

HUMAN FACTOR RELATIONS WITH INFORMATION SECURITY MANAGEMENT

Information security management is a new field on the borderline of IT, law and management, dealing with defining security aspects for an organization and its ICT systems, its achievement and maintenance. It is subject to the same general rules as any other field of management - it has its purpose, plans, policies, control and evaluation instruments, cost and loss accounting of the enterprise. Other side is the position of Ożarek, in which the author states that the Information Security Management System (ISMS) is one of many management subsystems functioning in modern, well-managed organizations. The management of a given organizational unit only through the prism of information security, without taking into account management processes taking place in other areas of its activity, is not only impossible but also pointless. These systems are mutually complementary and only this way of treatment ensures their effectiveness and efficiency. At this point, it should be noted that this approach to the ISMS is also preferred by the procedures set out in PN-ISO / IEC 27001. The information security management process allows you to succeed in strategy and achieve business goals. "Information managed by organizations is in oral and written form transmitted electronically in an IT system. This process based on trust between people working for the company and management staff. Conceived employee - a human being is the most important relay factor responsible for secure data transfer inside and outside the company "[12].

Pankowska analyzes information management system focus on organization traditional form of oral and written information transfer based on information systems. "In this management is constantly based on trust between people working for the company. Human - employee is the most important relay factor responsible for

[11] J. Krawiec, Bezpieczeństwo danych – podejście systemowe, [w:] Ochrona danych osobowych w praktyce, Polski Komitet Normalizacyjny, Warszawa 2013, s. 31

[12] Ożarek G., System Zarządzania Bezpieczeństwem Informacji – budowa i wdrożenie, [w:] Ochrona danych osobowych w praktyce, Polski Komitet Normalizacyjny Warszawa 2013, s.52

secure data transfer inside and outside the company. Man is one of the weakest and most important links of information security in an economic entity "[13] The impact of the human factor on the security of information management can be divided into five categories, where employees or managers of the organization play a key role:

1. Data theft by computers and laptops, using networks, external drives, taking pictures of the monitor with a mobile phone,

2. Opening and browsing unknown e-mails and websites,

3. Installing the application on a mobile phone and a company computer,

4. Not using in the company network in the scope of Internet use,

5. Conversations about organizations with people we don't know.

Management security article and literature indicates a relationship about the close cooperation between IT departments and an employee of the security department in controlling organization processes at all levels of organization management. Authors Margol, Dymora, Mazurek pointed to the value of the managing each element. Dynamic process of security and safety by protecting data backups, providing certain information via an external website of the organization. Failure to comply with the principles and rules of security management can lead to downtime in the organization's work, high cost in terms of finance in the process of recovering information. "Consequences affecting organizations directly may be the loss of trust by customers and everyone from all external environment in the company"[14].

STRATEGY PLAN FOR INFORMATION SECURITY MANAGEMENT

Information security planning involves the division of threats and consequences by location and source. In an organization, strategic information security risk planning appears inside and outside the organization. Nowak indicates

---

[13] Pańkowska M. , *Zabezpieczenie wiedzy w organizacjach, Warszawa 2004, s.67.*
gospodarczych, [w:] Prace Naukowe Akademii Ekonomicznej we Wrocławiu, Nr 1011.

[14] Margol P., Dymora P. Mazurek M. (2017), *Strategie archiwizacji i odtwarzania baz danych*, Zeszyty Naukowe Politechniki Rzeszowskiej, z. 36(3), październik-grudzień, s. 31.

that "the internal threat includes the risk of loss, damage or lack of access to data, which by definition is associated with an error of activity or intentional scrupulous conspiracy of dishonest users. External threats include data loss and damage by intentional third party actions on the network and information system acting to the detriment of the organization. The inability to service occurs due to a breakdown or catastrophe and other unknown events that affect the enterprise's information system and its entire system of operation"[15] .

Bączek indicates the sources of threats in the area of information security against unauthorized entities. In the organization's operation, the author refers to "random threats, including natural disasters that affect the information security status of the enterprise (e.g. building fire - storage of information carriers and paper versions of the organization). Traditional information threats including espionage, private investigators and sabotage activities aimed at obtaining information or offensive misinformation. Activities related to the IT department, including the process of maintaining IT networks in the field of computer crimes and cyber terrorism, information struggle. Threats directly related to the rights of employees and citizens in the field of social groups, including the sale of information about entities, violation of privacy and unlawful interference by special services"[16].

Żebrowski describe safety management how is process. He describe planning information security threats on based on the fact that man is the greatest threat in the organization's operation. Deliberate action to the detriment of a person's enterprise within or around an organization may lead to its direct or indirect lost money or value of company. Person can strategically intentionally threaten information security by hacking into the system, stealing documents, obtaining access codes to safes, bank accounts or internal networks (intranets) in the organization. "Man as a rational being can use hacking into computer systems to obtain information about the organization in various ways. At this point, it is the man who can intentionally initiate failures and errors. Not sleep spy vigilance allows you to decode access passwords, attack on company mail, as well as upload dangerous computer applications for economic intelligence purposes. Many managers uses administrative and department of IT to circumvent security and capture information based on one or more perpetrators"[17].

---

[15] Nowak E., Nowak M., Zarys teorii bezpieczeństwa narodowego, Warszawa 2011, s11.

[16] Bączek P., Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Toruń 2006, s.45

[17] Żebrowski A., Kwiatkowski M., Bezpieczeństwo informacji III Rzeczypospolitej, Kraków 2000, s.63.

LEGAL LAW REGULATIONS SAFETY MANAGEMENT FOR PRIVATE COMPANY OPERATIONS

Legal aspects of safety management as well as law regulations constitute the field of activity in the European Union in this respect. Ensuring optimal measures to protect enterprises in the form of directives and ordinances of EU institutions concern the regulation of the principles of information exchange between organizations and the state, and also indicate how to respond to cyber-attacks in the process of managing the organization in the field of national entities in the aspect of European Union member states. In 2011 and 2012, Directive 2012/17 / EU was adopted, which thoroughly described and indicated the central, commercial and company registers in the EU Member States, thus replacing the old non-functional directives of 1989 and 2005. Two years later in 2013, announced Directive 2013/40 / EU dedicated to counteracting any attacks on information systems, thus it replaced the document of the European Union General Council of 2005. The third article of the directive defines the type and groups of computer crimes. In 2016, "Regulation 2016/679 / EU regarding personal data of the GDPR, as amended from former legal provisions of 1995, was announced and established"[18].

Directive 2016/679 / EU related to the protection and processing of personal data by the bodies of the European Union and the EU Council document of 2008 was repealed. In 2016, Directive 2016/1148 / EU was adopted, which specified the conditions for securing ICT networks and systems in the European Union. In Poland, a team was established in 2017 for IT security in cyberspace across the country and cooperation between members of the European Union. In 2008, members of the permanent Program Council of the European Union established the Government Emergency Response Team (CERT), which provides cyber security in public finance units and cooperates with commercial banks in the EU Member States European

[18] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679/UE z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz. Urz. UE L 119 z 27.04.2016

Union. In 2015, a government team was created in Poland, which created a document called "Methodology of managing cyberspace risk in government information security management systems"[19].

Between gap year 2016 and 2017 government of Poland make plan with experts about cyber security strategy from 2017 to 2022. National Program for Cyber Security Policy of Poland in 2017-2022 are created and begin planning change from communications between government (tax, security systems) and small and large company who based in the country. In January 2015, tax company system payment in Poland are required to send to the Tax Offices. Tax sending and returns in electronic form of all declarations from a private organization, including VAT on services and goods. In 2016, a law in Poland related to "digital web system of business entities that carry out public tasks and a new provision in the field of providing information"[20] is in force in the National Court Register in the form of an e-application and e-declaration. In 2017, “under the Tax Ordinance Act, an obligation was made available to tax audit bodies to provide special individual number and form audit register company files (JPK)”[21], which have data regarding the accounts and accounting books of the organization - enterprises in electronic form.

SUMMARY

Information security management is a great challenge for any organization. In each case, the most important is the human factor - the appropriate use of IT techniques and new technologies in the field of data protection and security in the process. The article includes a literature review in the field of information security management and is the starting point for conducting surveys in this area. The literature review security management process it is at opinion from author starting point for creating and describing processes and methods. In the field of collaboration

[19] Pobrano dnia 3 sierpnia 2019 roku: https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09

[20] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. z 2013 r., poz. 235 ze zm.

[21] Ustawa z 29 września 1994 roku o rachunkowości, Dz. U. z 2018 r., poz. 62.
Ustawa z dnia 10 września 2015 r. o zmianie ustawy – Ordynacja podatkowa, Dz. U. z 2015 r., poz. 1649 ze zm

between research and development of management security in every process of the organization efficient operation. The literature indicates that managing not only IT security but also information security is the most important problem of modern enterprises.

Safety management and literature review in this area shows that management security areas rely mainly on the human factor and relationships between employees, customers and the enterprise environment. In many cases, the organization's lack of knowledge about security management is noticeable. Literature in this topic indicates that activities in this area must rely on regular employee training, fairly significant funding for the security department, as well as indicate in the organization on the transfer of knowledge in the field of the importance of information security management. The knowledge and training of employees and managers will significantly help the organization in the area of responsible approach to information security management in the unstable external world and in the area of network activities. Information security management has great material and immaterial value in the functioning of an organization. Identifying, describing and strategy of actions in the event of danger are key in the aspect of building the entire security system in the enterprise. Information protection consists in searching for the source of its future escape as well as minimizing the level of future consequences of the occurrence.

Definitely, every information needs to be checked, but not every aspect of this information is protected in the same way — however, we have to provide a schedule for its evaluation. With every small piece of information stolen, there may be an information avalanche of events that will plunge organizations into the future. Verification of security information depends on the level of its nature and significance of its occurrence. Knowledge of all information security management in-depth scientific ground will allow to create a new field of management sciences that will develop over the next years.

Management security operations is not only on the field of IT but also humanity will allow for the elimination of adverse events and projects, thereby increasing trust of the organization environment and constantly raising on the market value.

BIBLIOGRAPHY

Bączek P., Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Toruń 2006.

Beskosty M., Zarządzanie bezpieczeństwem informacji, „Studia nad Bezpieczeństwem" 2017, nr 2.

Fehler W., Bezpieczeństwo przestrzeni publicznej. [w:] Bezpieczeństwo publiczne

gospodarczych, Prace Naukowe Akademii Ekonomicznej we Wrocławiu 2012, Nr 1011.

Information technology – Security techniques – Information security management systems – Requirements, ISO, Geneva, 2013.

Krawiec J., Bezpieczeństwo danych – podejście systemowe, [w:] Ochrona danych osobowych w praktyce, Polski Komitet Normalizacyjny, Warszawa 2013.

Liedel K., Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego, Toruń 2005.

Margol P., Dymora P. Mazurek M., Strategie archiwizacji i odtwarzania baz danych, Zeszyty Naukowe Politechniki Rzeszowskiej, z. 36(3), październik 2017.

Nowak E., Nowak M., Zarys teorii bezpieczeństwa narodowego, Warszawa 2011.

Ożarek G., System Zarządzania Bezpieczeństwem Informacji – budowa i wdrożenie, [w:] Ochrona danych osobowych w praktyce, Polski Komitet Normalizacyjny Warszawa 2013.

Pańkowska M., Zabezpieczenie wiedzy w organizacjach, Warszawa 2004.

Polski Komitet Normalizacyjny. „Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji". PN-ISO/IEC 17799, Warszawa 2013.

Suchorzewska A., Rozdział V. Przestępstwo cyberterroryzmu w polskim systemie prawnym 4. Ochrona informacji utrzymywanych w systemach informatycznych a bezpieczeństwo informacyjne państwa 4.3. Zarządzanie bezpieczeństwem informacji, [w:] A. Suchorzewska, Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmu, Oficyna LEX, Warszawa 2010.

Żebrowski A., Kwiatkowski M., Bezpieczeństwo informacji III Rzeczypospolitej, Kraków 2000.

OFFICIAL LAW ACT AND REGULATIONS DOCUMENTS

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148/UE z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej, Dz. Urz. UE L 119 z 19.07.2016.

Dyrektywa Parlamentu Europejskiego i Rady 2012/17/UE z dnia 13 czerwca 2012 r. zmieniająca dyrektywę Rady 89/666/EWG i dyrektywy Parlamentu Europejskiego 2005/56/WE i 2009/101/WE w zakresie integracji rejestrów centralnych, rejestrów handlowych i rejestrów spółek, Dz. Urz. U.E. L 156 z 13.06.2012.

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dz. Urz. UE L 218 z 14.08.2013.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680/UE z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady,2008/977/WSiSW, Dz. Urz UE L 119 z 29.04.2016.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679/UE z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz. Urz. UE L 119 z 27.04.2016.

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. z 2012 r., poz. 526.

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. z 2012 r., poz. 526.

Ustawa z 29 września 1994 roku o rachunkowości, Dz. U. z 2018 r., poz. 62.

Ustawa z dnia 10 września 2015 r. o zmianie ustawy – Ordynacja podatkowa, Dz. U. z 2015 r., poz. 1649 ze zm.

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. z 2013 r., poz. 235 ze zm.

ONLINE DOCUMENTS

https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09