MANAGEMENT SCIENCES NAUKI O ZARZĄDZANIU

sciendo

Year 2019, Vol. 24, No. 4
ISSN 2080-6000
e-ISSN 2449-9803

SECURITY INFORMATION MANAGEMENT SYSTEMS

Kamil Andrzejewski

Wroclaw University of Economics and Business, Wroclaw, Poland
e-mail: kamil.andrzejewski@ue.wroc.pl

ORCID: 0000-0002-9337-3193

DOI: 10.15611/ms.2019.4.01
JEL Classification: H550, M130

Abstract: The article includes a literature outline of the scientific field of management sciences concerning issues of security management an organization. The article focuses on identifying literature in this area and describing the process in terms of the essence of management in the organization. The authors who were pioneers of the subject were indicated and the author 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 discusses opinions of other authors in the selection of the optimal strategy for managing security in an enterprise and shows how it financially a effects the company and its intangible market value.

Keywords: security management, information, company value, assessment of the stock market, new market value, startup, legal security, IT security, security context, development security management, ERP, fraud.

1. Introduction

Security information management systems are connected with communications management. This subject of great importance in the development of every small and large organization in the 20th and 21st century. Scientists have become very interested in this research problem since 1993. The basis guiding the research in publications in this area is to answer to the main article problem.

The main purpose in this article is how to build security information management and what process to use in a new startup enterprise and a company development during the period of growth?

Taking into account the current state of knowledge about the issue of operation Management. The following scientific goals of the article are included by the author. The main objective of the article is to improve the decision-making security in defined processes in the organization through the use of the process of management and exchange of information and support with information ERP IT systems.

Finding a solution in the human and technical aspect for the integration of information security management tools with management tools the author conducted research in the scope of processes, services and products of the organization. The author included a formulation of information and organizational conditions for which it is possible to implement a safe and low-cost implementation of security management in an organization working on the basis of defined HR, managerial processes and information security management standards as all organization system.

Security management information system 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. All information has attributes and a transmission validity schedule.

The area of security management information system is a unique trend of solutions developed

by experienced researchers. Implementation teams dealing with the development of research in this area were used. The above community includes researchers from various universities all around the world as well as development centres, for example Colorado Technical University, Queensland University Australia, and Saint Joseph Research. Period of building the implementation model of the solution, two hypotheses were made in the article.

H1: Field implementation of information security management mechanisms can be integrated with material and non-material growth of a new startup and a company undergoing information and IT development.

H2: Implementation of the method of introducing information security management in organizations which are managed based on ERP (Enterprise Resource Planning) processes and systems does not require major changes to existing business and IT processes in the startup and the operating organization.

Security information management has been the subject of research of scientists for twenty years in the field of protection of countries, cities, and employees, including work in an organization. However, since 1997, there has been a noticeable trend of very high dynamics in company development in the field of technologies that may be stolen 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 one`s organization may result from bankruptcy to serious legal and financial consequences.

Literature describes pragmatic and bibliographic security management where authors Xu and Dong analyse deeply methods of "security mechanism has limited the use of multicast. Key management for multicast is used for group members in one multicast session to generate, refresh and transfer keys which are used for encryption and authentication. In addition to the maintenance of keys, issues about scalability, reliability and robustness should be carefully considered" [Xu, Dong, Xu 2004, p. 141].

One must be aware of the importance of dynamics of technology and process development and their protection in terms of secure data flow and secrets in a group of employees, suppliers of all areas of the 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 of the company.

Organizational security should be considered in many dimensions. In this case, the authors describing the problem focus on the process of the thorough transformation of the organization in terms of the work of the board, human resources, production works, physical protection and IT.

Important aspects of a security information's system is also the model and type of business. This case is important for Busenitz and Barney "building on no rational decision making models from behavioral decision theory, we asserted that entrepreneurs are more susceptible to the use decision-making biases and heuristics than are managers in large organizations. To understand why entrepreneurs and managers in large organizations may vary in the extent to which they manifest biases and heuristics in their decision--making, it is important to understand the utility of no rational decision-making. Under conditions of environmental uncertainty and complexity, biases and heuristics can be an effective and efficient guide to decision-making. In such settings, more comprehensive and cautious decision-making is not possible, and biases and heuristics may provide an effective way to approximate the appropriate decisions large organizations. With entrepreneurial ventures in particular, the window of opportunity would often be gone by the time all the necessary information became available for more rational decision-making. Additionally, successfully starting a new business usually involves overcoming multiple hurdles. Using biases and heuristics as simplifying mechanisms for dealing with these multiple security management cases may be crucial. To face such hurdles from a strict econometric approach would not only postpone decisions, but would in all likelihood make them overwhelming. More specifically, overconfidence may be particularly beneficial in implementing a specific decision and persuading others to be enthusiastic about it as well" [Busenitz, Barney 1997, p. 9].

Most definitions of security managements systems come from schools of business, however, the most adequate is quoted by Xu writing about information's systems cluster in business network that "along with a wide application of the network and information techniques, the level of informatization has been developed, however, management security solutions have also become severe. Based on the analysis of current security condition of (..) network and the key factors by which security disasters can be induced, a lightweight authentication protocol is proposed, ensuring that only legal users can access the digital systems information and network systems" [Xu 2014, p. 867].

Fehler described security as the subject of "process having a dynamic nature and state in which a given entity not only has 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" [Fehler 2010, p. 16]. 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 (fake 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" [Suchorzewska 2010].

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" [Liedel 2005, p. 19].

2. Security management communications process in the organization perspective

Long term security in the organization of a security management communication is the primary problem of many organizations in the world. The process of providing information in the field of security refers to its security, where there is no risk that the information will flow outside the enterprise and employees. Beskosty describes this as "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" [Beskosty 2017, s. 164].

The aim 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 as to what extent they are to define information security in an organization. Guidelines for maintaining standards in the scope of field research purposes include:

- "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" [Polski Komitet Normalizacyjny 2013, s. 10].

Most organizations face a challenge to check all information that may have a key impact on the final product or service. However, Bączek refers to information security in terms of the state's operation as an organization. In this case, one 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 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 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 other people" [Bączek 2006, p. 74].

In this case, the company is required to create accurate procedures for the provision of information, secret and classified data system, indicating 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.

During the past thirty years, the analysis of data generated from Location-Based Social Networks have aided in the identification of security management urban patterns. Understanding activity behaviour in urban areas for security systems and security management of the cites all around the world determines networks hubs for the protection citizens and tourists "as well as producing novel recommend systems that facilitate users choices. Recognizing crowd-mobility patterns in cities is very important for public safety, traffic management, disaster management, and urban planning, a framework for Recognizing the Crowd Mobility Patterns in Cities using location based social networks not only one data. The framework comprises four main components: data gathering, recurrent crowd-mobility patterns extraction, temporal func-tional regions detection, and visualization component" [Assem, Buda, O'Sullivan 2017, p. 671].

Other information is needed for the CEO and CFO, also the technology director, and production employees. However, information is most important when connected with security management. This always affects the content of information and communication and trust to become acquainted with who and how uses the knowledge and what is the purpose of this activity.

3. 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 all departments, and the 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, 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 the field of "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" [Ożarek 2013, s. 52].

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 form of e-mail, ERP systems, all information that is displayed on the screen of company computers and laptops, including movies, photos and presentation" [Suchorzewska 2010, p. 24].

However, knowledge about security management systems is about management and information systems as the "optimal solution for information security management is not always included in the PN-ISO-EIC-27001 standard" [*Information technology*… 2013, p. 13]. Management operations and coordinating information security processes in all cases require employees. All employees at an organization 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 requires 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 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" [Krawiec 2013, p. 31].

4. Human factor relations with information security management

Information security management is a new field on the borderlines 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.

Contrary 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 the 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 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. Conceivably, an employee – a human being is the most important relay factor responsible for secure data transfer inside and outside the company" [Ożarek 2013, p. 52].

Pankowska analyzes information management system focusing on organization as a traditional form of oral and written information transfer based on information systems. "This management is constantly based on trust between people working for the company. A human an employee is the most important relay factor responsible for 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" [Pańkowska 2004, p. 67]. 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 the company network in the scope of Internet use,
5. Conversations about organizations with people we don't know.

On the other hand, security information's is important for fast a growing country "Israel's information grown with Venture Capital Industry, its emergence and operation during the 90s, in which period the number of venture Funds increased from 2 to over 100. The context is the information transformation of Israel's high tech industry from the defense-dominated electronics industry of the 70s/80s to the 'Silicon Valley' model of the 90s characterized by large numbers of information companies. During this period the share of high tech information system manufacturing industry; and ICT's share in the Business Sector increased considerably attaining one of the highest levels worldwide. Given the importance information on Venture Capital, an analysis of the waves of new startups and companies should be done jointly with an analysis of the emergence and development information systems all companies" [Avnimelech, Teubal 2017, p. 33].

Management security articles 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.

Margol, Dymora, Mazurek pointed to the value of the managing each element of 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 environments in the company" [Margol, Dymora, Mazurek 2017, p. 31].

5. 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 states 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" [Nowak, Nowak 2011, p. 11].

Drago, Estrin and Wooden described from 1990 till 1993 long research for company based in Australia regarding security management and the aim of model of business. It was a good knowledge model for information's and security companies "down under". The author, "using survey data from 565 private sector employees in Australia tests how perform--related incentives influence worker attitudes. It is concluded that job satisfaction is related to incentives based on individual or small group performance, while organizational commitment is more strongly related to company-level incentives (gains-sharing). Tests for the bundling of incentives and participatory management and for the interactive effects of incentives, participatory management security are insignificant in this data set" [Drago, Estrin, Wooden 1993].

Information security planning systems are similar to the "potential of cultural theory as a tool for identifying patterns in the stakeholders perception of risk. It is effect on information system is linked with risk management. Design of information methodology approach to risk management involves a number of human activities which are based on the way the various stakeholders perceive risk associated with information assets. Cultural theory claims that risk perception within social groups and structures is predictable according to group and individual worldviews; implications of cultural theory on information system with risk management as a means for security experts to manage stakeholders perceptions" [Tsohou et al. 2018, p. 198].

Firstly, security described by 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 (for all information the example is building firestorage 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" [Bączek 2006, p. 45]. A key research problem information security management systems is problems still facing is that of commonsense reasoning research. The fact of a child having once touched a hot-plate can extrapolate that anything glowing red is potentially dangerous, this ability to generalize an experience is very difficult for programmers to build into information's and computer systems. Because every generalization is context dependent and thus variable in nature to information's multicast of information.

Hu define management security system as a tree of "multicast is used to deliver packets to a group of users. To prevent users outside the group from eavesdropping. Group information key is maintained to encrypt the group to communication, and the group key is changed (rekeying) when a new member joins the group or an existing member leaves the group. Costs could be as high as n for a group with members. The hierarchical key-tree approach is widely used to achieve logarithmic rekeying costs. However, the key tree has to be kept balanced in order to keep logarithmic rekeying costs". Hu proposed the height-balanced tree and found that it has the best performance among the balancing strategies tested of security informations systems" [Lu 2005, p. 214].

Żebrowski describe security management ass long term process. He describes 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 loss of money or value of a company. A person can strategically intentionally threaten information security by hacking into the system, stealing documents, obtaining access codes to safes, bank accounts or internal networks (intranet) 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 person who can intentionally initiate failures and errors. Non-stop spy vigilance allows 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" [Żebrowski, Kwiatkowski 2000, p. 63].

6. Legal regulations safety management for private company operations

Legal aspects of safety management as well as laws and 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" [Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679/UE].

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. 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"[1].

Between the year 2016 and 2017 government of Poland planned with experts their cyber security strategy from 2017 to 2022. The National Program for Cyber Security Policy of Poland in 2017--2022 was created and began planning change for communications between government (tax, security systems) and small and large companies based in the country. In January 2015, company tax system payment in Poland were required to be sent to the Tax Offices as tax 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" [Ustawa z dnia 17 lutego 2005 r.] 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)" [Ustawa z 29 września 1994 r.; Ustawa z dnia 10 września 2015 r.], which have data regarding the accounts and accounting books of the organization – enterprises in electronic form.

7. Summary

Information security management is a great challenge for any organization. In each case, the most important is the human factor of 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. In the literature review security management process is, in the opinion of this author, the starting point for creating and describing processes and methods. In the field of collaboration 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.

Security management features are as follows: access control framework, image filters, provenance tracking system, and repository maintenance services for company. An important new trend for management systems is the protection and the management all system of "Cloud Computing providing an optimal infrastructure to utilize and share both computational and data resources whilst allowing a pay-per-use model, useful to cost-effectively manage hardware investment or to maximize its utilization. It offers transitory access to scalable amounts of computational resources, something that is particularly important due to the time and financial constraints of many user communities. The growing number of communities that are adopting large public cloud resources such as Amazon Web Services, SAP ERP, Microsoft proves the success and hence usefulness of the Cloud Computing paradigm. Nonetheless, the typical use cases for public clouds involve non-business critical applications, particularly where issues around security of utilization of applications or deposited data within shared public services are binding requisite" [Wallom, Turilli, Martin 2011, p. 247]. The future of information security management is mutual trust with information electronics system hardware and Artificial Intelligence departments and knowledge companies.

Security 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.

The literature in this topic indicates that activities in this area must rely on regular employee training, significant funding for the security department, as well as indications 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 the 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 occurrence.

All information must to be checked, but not every aspect of this information is protected in the same way – however, we one has to provide a schedule for its evaluation. With every small piece of information stolen, there may be an information avalanche of events that will sink organizations in the future.

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

The verification of security information depends on the level of its nature and significance of its occurrence. In depth knowledge of information security management will allow to create a new field of management sciences that will develop over the next years. Management security information operations is not only in field of IT but also in business to business and customer relations. Will allow for the elimination of adverse events and projects, thereby increasing trust of the organization environment and constantly raising on the market value.

The article, including the proposed objectives and hypotheses is a stage in the process of future research activities. The author presented a new approach to managing communication security as an organization's operating system and pointed out defined processes in functioning organizations.

The author, as part of an implementation doctorate thesis (grant research doctorate from Ministry of Science and Higher Education in Poland) to new build prototype solution and carry out simulation and survey research till 2021 to show the likely benefits for the organization.

Future research may be focus on measurable results of implementing organization security process management information system to startup and existing organization.

The author of the article is developing doctorate research to build to a prototype for the implementation of the information security management platform in the organization. The author is conducting research with the support of a team and Supervising Professor, on the existence of potential benefits and threats in the area of information security management over a period of time.

Bibliography

Assem H., Buda T., O'Sullivan D., 2017, *RCMC: Recognizing crowd-mobility patterns in cities based on location based social networks data*, ACM Transactions on Intelligent Systems and Technology, volume 8, issue 5, 2017.

Avnimelech G., Teubal M., 2017, *Venture capital start-up co-evolution and the emergence & development of Israel's new high tech cluster: Part 1: Macro-background and industry analysis*, Economics of Innovation and New Technology, 13(1).

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

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

Busenitz L., Barney J., 1997, *Differences between entrepreneurs and managers in large organizations: Biases and heuristics in strategic decision-making*, Journal of Business Venturing, 12(1).

Drago R., Estrin S., Wooden M., 1993, *Pay for perform mance incentives and work attitudes*, Australian Journal of Management, volume 17, issue 2, December.

Fehler W., 2012, *Bezpieczeństwo przestrzeni publicznej*, Prace Naukowe Akademii Ekonomicznej we Wrocławiu, no. 1011.

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

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

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

Lu H., 2005, *A novel high-order tree for secure multicast key management*, IEEE Transactions on Computers, 54(2).

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

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

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

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

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

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

Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., 2018, *Formulating information system risk management strategies through cultural theory*, Information Management & Computer Security, 14(3).

Wallom D., Turilli M., Martin A., 2011, *My Trusted Cloud: Trusted cloud infrastructure for security-critical computation and data management*, IEEE International Conference on Cloud Computing Technology and Science.

Xu M., Dong H., Xu K., 2004, *Survey of research on key management for multicast, Ruan Jian Xue Bao*, Journal of Software, volume15, issue 1, January.

Xu Q., Research on the security problems existinged in information management of libraries World Automation Congress Proceedings, 6936178, 2014.

Żebrowski A., Kwiatkowski M., 2000, *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków.

Official legal law acts 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, DzU z 2018 r., poz. 62.

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

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, DzU 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.

ZARZĄDZANIE PROCESEM BEZPIECZEŃSTWA INFORMACJI

Streszczenie: Artykuł zawiera zarys literatury naukowej z zakresu nauk o zarządzaniu dotyczący zagadnień zarządzania procesem bezpieczeństwa informacji w organizacji. Artykuł koncentruje się na identyfikacji literatury w tym obszarze i opisaniu tego procesu pod względem istoty zarządzania w organizacji. Wskazano autorów z całego świata, którzy są pionierami zarządzania procesem bezpieczeństwa jako unikalnego tematu rozwoju organizacji. Autor wskazał nowe trendy podejścia do zarządzania bezpieczeństwem informacji w procesie budowania i rozwoju modelu biznesu przedsiębiorstwa. Na końcu artykułu autor, opierając się na literaturze, dokonuje wyboru optymalnej strategii zarządzania bezpieczeństwem w przedsiębiorstwie. Autor pokazuje, w jaki sposób bezpieczeństwo zarządzania wpływa finansowo na organizację i jej wartość rynkową.

Słowa kluczowe: zarządzanie bezpieczeństwem, informacja w organizacji, ocena rynku akcji, nowa wartość rynkowa, startup, bezpieczeństwo prawne, bezpieczeństwo IT, kontekst bezpieczeństwa, zarządzanie bezpieczeństwem ERP, oszustwa.