Współczesna Gospodarka

Contemporary Economy
Electronic Scientific Journal
Współczesna Gospodarka (ug.edu.pl)

Vol. 15 Issue 2 (2022) 1-12
*ISSN*2082-677X
DOI 10.26881/wg.2022.2.01

IT SECURITY MANAGEMENT IN THE ERA OF THE FOURTH INDUSTRIAL REVOLUTION

Michał Igielski

Abstract

The purpose of this article is to attempt to identify and assess the determinants of IT security management at the organizational level. This is particularly important in the context of the main pillars of the Industrial Revolution 4.0, which include the integration of advanced information technology (IT), automation (OT), „Internet of Things" (IoT) and artificial intelligence (AI) systems. This impacts IT systems, which are becoming more sophisticated and complex all the time. This results in increased dependency - the more complex the IT system, the more complex the security must be. The more so that nowadays the functioning of the organization depends on the processing of various information, therefore IT security management includes a set of processes aimed at achieving and maintaining the established level of security. The article also presents the types of IT threats in relation to the use of systems supporting management. It also focuses on activities in the aspect of IT security of modern organizations.

Keywords: fourth industrial revolution, information infrastructure, information security management

JEL classification: D83, M15, M40, O33

Introduction

Currently, the world is in a transition phase from the third industrial revolution to the fourth, referred to as Industry 4.0. The pillars of Industry 4.0 are concepts such as the global megatrend, which includes the integration of advanced information technology (IT), automation (OT), the "Internet of Things" (IoT), and artificial intelligence (AI), which allows for global access to data. This integration enables widespread use of „machine intelligence" to autonomize analytics and manufacturing and service processes, among other things.

Such an increasing share of information technology in the daily life of entire societies, combined with their expectation of facilitation that speeds up the organization of daily life, means that virtually all organizations are compelled to use information technology to an ever greater extent. But we don't expect just improvements - we also expect to be assured that all the data we make available are properly protected against unauthorized access.

Thus, the potential of dynamic civilization changes makes it necessary to forecast new challenges and threats to IT infrastructure. Therefore, in-depth analysis, due to the potential of threats will have to be corrected by the progress of informatization, the existing development of a dynamic model of IT security system solution. At the same time it is necessary to remember about State Informatics Infrastructure which includes IT systems and networks important for effective functioning of each organization, taking into account their broadly understood security and economic interests.

1. IThe essence of the fourth industrial revolution

The life of the entire population of mankind consists of three main stages defined by waves of development of civilization. The first wave is the agrarian revolution associated with the acquisition of the ability to cultivate the land and the spread of a sedentary lifestyle. The second wave is the industrial revolution initiated by the invention of the steam engine, electricity, new means of transport and mass communication and the creation of mass production (Toffler, 2006). The invention of the computer, in turn, is considered the beginning of the third wave - the post-industrial revolution. This phenomenon is associated with the use of automated machinery and equipment, unrestricted access to information, and moving away from mass production to individualized production. The third wave of humanity's social and economic evolution is also treated as a continuation of the industrial revolution by creating automated production based on flexible production systems and smart factories with cyber-physical production systems where information is transmitted through the Internet. The changes occurring in industry in the wake of the third wave are also referred to as the third and fourth industrial revolutions - Industry 3.0 and Industry 4.0 (Stadnicka and all, 2017).

We should understand the fourth industrial revolution as a collective term for technologies and concepts of value chain organization (Hermann and all, 2015). So we can say that the essence of the fourth revolution is the cyber physical space created by hardware, software, network and of course people . It is the cyber physical space that became the foundation and the main difference between the previous revolutions. It has allowed for changes that humans have not yet experienced in any of the revolutions described earlier (Zembski, 2017). All of this assumes the existence of intelligent systems that are networked - vertically connected to other processes within the enterprise and horizontally connected to value-creating networks that can be managed in real time - from order entry to the coordination of disposal logistics (Götz & Gracel, 2017).

However, K. Schwab (2016) has a completely different perspective on this topic, who believes that the name referring to the three previous industrial revolutions is misleading, as the scope of this revolution is much more extensive. The main differences between the fourth and third revolutions are: worldwide widespread access to the Internet, a dramatic reduction in the cost of data storage, device mobility, smart sensors, renewable energy, and artificial intelligence.

The cost of data has fallen dramatically - the creation of the „cloud" means that data is theoretically available anywhere, and the proliferation of mobile computing, tablets and smartphones means that anyone can access data. Widespread trends have made information virtually free and available in real time. Which has significant implications for how they are collected and used. The web has made it possible to connect virtually all the media, machines and devices around us (Baldassari & Roux, 2018).

Nothing can surprise us anymore - what was once in the realm of dreams and fantasies, today is a common reality. Continuous development of artificial intelligence or machines that easily use prepared learning algorithms in order to optimize their decisions and eliminate related threats is only the beginning. The fourth industrial revolution is also about autonomous devices, even household ones, connected to each other by one common IT network. Finally, it's about chat bots, taking care of people and helping them with their daily chores.

This means that the new 5G-based economic model will dramatically affect every aspect of our lives. From things that seem mundane to us, such as increasing the majority and speed of data transfer in everyday life, through the widespread use of artificial intelligence and cloud computing to optimize production processes, to medicine or education.

On the other hand, describing in detail the Society 5.0, as a proposal of the concept of modern, future-oriented and human-centered society, in which the integration of cyberspace and the real world is to be realized by using the most modern technologies, such as: artificial intelligence, the Internet of things, robotics or big data, we should start, according to the author of the article, with a general description of the Society 4.0, in which (du Vall, 2019):

1. The creation, dissemination, use, and manipulation of information became essential to political, economic, social, and cultural activities.
2. There has been a transformation of the working class into a professional middle class.
3. There is the development of multiple networks (formal and informal).
4. There are considerable social divisions and inequalities - this is due to the fact that new technologies are changing the structure of employment in society, and this leads to a division between, on the one hand, "safe", well-paid and skilled workers and, on the other hand, the growing mass of unemployed (in addition, most members of society belong to the post-industrial working class, for whom work is not a source of identity).
5. There is an enduring link with the phenomenon of globalization, which is one of the most visible consequences of the information revolution.

Of course, it was the Japanese who first noticed that the society with the number five assigned was the next stage of evolution, creating a description of this new society that is available on the Prime Minister of Japan's website[1]: „it is a human-centered society in which economic progress containing solutions to social issues is balanced by a system that offers high integration of digital and real space”.

As we can see this is a new social challenge, not encountered before, which is not faced by Japan alone, but also by practically all countries in the world. That is why in 2015, the 2030 Agenda for Sustainable Development was adopted by the United Nations, which identifies 17 development directions that the entire international community should strive for.

As we can see, talking about the concept of Society 5.0, we have to remember that this social and economic change will not happen by itself this time - we have to create it. This is the time of great reforms, of which the role of precursor was taken by Japan, which has long been a leader in the permanent search for solutions to the accumulating social problems and the promotion of various innovative solutions. It is also no secret that the new transformation will permanently change most areas of social life, including the structure of employment. Thanks to this social and technological engineering, the problem that has been perceived so far as number four is to be overcome. This is because the information-based society we live in today has difficulty in effectively sharing the data we have and the knowledge we acquire. The Japanese conception calls this situation a limitation, without overcoming which we cannot hope to jump to a higher level of development. The problem is serious because most societies in the world are shrinking, demographics remain unfavorable, economics is still undergoing transformation, and

[1] The Government of Japan, [online], www.japan.go.jp

the world is not idle and creates new challenges on a global scale (just to mention the American and Chinese trade wars or climate problems) (Tomański, 2019).

2. Information infrastructure in the 21st century

In the twenty-first century, the issues relating to information infrastructure, mainly concern the designed integration and harmonization of information systems in an information-saturated environment with the dominant participation of artificial intelligence. Many times we come across concepts, based on research results, which concern harmonization of information systems in different relations in an organization. From the point of view of the security of such infrastructure, IT solutions that deal with the integration of distributed information systems and their security and the use of artificial intelligence for broader support of human decision-making processes are interesting. Further challenges for the IT infrastructure are EU projects that are an investment in the digitalization of the national and European economy, which contribute to:

- Smart growth in areas such as high quality data infrastructure, connectivity and security.
- Development of new trends: artificial intelligence and distributed ledger technologies (e.g. blockchain).
- The development of robotics and the use of big data.
- The use of advanced digital skills and their deployment, and the optimal use of digital capabilities and their interoperability.

As observation shows, the essence of such projects is an interactive information infrastructure as a basis for decision-making process on the basis of profiled information sources and contents, which, occurring in information silos and collections, give its users access to a coherent and common set of data. They also enable the management of a catalog of tasks in the IT infrastructure elements ensuring their integration, optimization of value generating processes and applied processes.

At this point, according to the author, it is also necessary to draw attention to the fact that nowadays the experience of social sciences boils down to the fact that many people see chaos, confusion and uncertainty in the world, including deep social inequalities, armed conflicts or mass migrations. All of this has very significant implications for IT infrastructure security. Nonetheless, one can observe today the striving towards integration progress of digital technical innovations. These innovations are delivering new products and services - changing processes, shaking up markets and ultimately changing our environment. Under these conditions, we can observe a disruption of the cyclical crisis that is growing. This trend is supported by a developmentally inadequate lack of regulation and alternating between nationalization and economic liberalization that deepens social divisions and access to capital (von Weizseker & Wijkman, 2018). Today, capital and its financial systems are focused on maximizing short-term profit - a source of conflict between private and public interest, which leads to an insufficient supply of money. Especially this supply is important in areas serving important social investment needs, which certainly include information infrastructure. In this situation, the security of this infrastructure will certainly be related, among other things, to the generic and qualitative planning of development investments as well as to the need for global investment analyses.

Therefore, the assumed economic criteria of profitability of innovative solutions and the so-called time targets will be of great importance for the security of IT infrastructure. Their importance also results from the necessity to design new procedures, based on IT technologies, in the area of target times and infrastructure changes that improve the efficiency of the organization's activities. The estimation of risks connected with the general security of the country is connected with its direct activity.

To sum up, nowadays the problem is to profile sources of information which, even if at the initial stage in information silos, give users access to a coherent and common set of data and their flow - this enables integration of certain business and technical management processes. Efficient circulation of up-to-date information allows organizational functioning to be put in order and provides a basis for increasing the quality of taken decisions, and thus increasing the effectiveness as a result of activities originating from the implementation of integrated IT software supporting this management. The aim of such activities is to support and optimize the value generating processes which include: teams designing, manufacturing, selling, providing services or serving and talking to customers (Senge, 2008).

Under the conditions of civilization development 4.0, organizations need to integrate available data to a much greater extent, analyze it and transform it into useful knowledge. In general, it should be said that the sets of information for decision-making, taking into account their entropy, should be as abundant and extensive as possible. The larger the information base is, the more the decisions generated from it are relevant to the current situation and represent higher utility and usefulness in the management process.

However, under these conditions, the problem of redundancy of information in the system (redundancy), which on the basis of quantitative and qualitative criterion, by assumption exceeds the minimum required to solve the problem, should also be taken into account. At the same time, due to the particular for the security of critical information infrastructure, its use in software is justified at least:

- Identified and precisely defined data, information in their collections and information silos, whose occurrence and reliability of transmission plays a key role during the technological process.
- Identification of redundant communication routes, which can be used interchangeably (a kind of hot reserve), which affects the system costs, but profiles the so-called backup route to the information.
- Recovery of data after its partial loss or damage or to detect e.g. damage (CRS checksum).
- Data compression, i.e. the possibility of verifying the information, which allows to detect possible errors originating from its use (checksums).

The experience of practice and science shows that artificial intelligence, learns from information and interacts with the outside world. Machine intelligence, on the other hand, using data from different silos, can recognize causal patterns, so it can preventively shut down a threatening element. The use of at least an actuation sensor in combination with a blocking sensor in a safety system is nothing more than the functional experience of events by machines and devices. Thus, machine learning becomes a collective consciousness - a „hive mind” in which each element learns and acts in a synchronized, collective manner - organizing the system's effectiveness according to set parameters. In addition, the system too can study the behavior of the user of such a system, analyzing its prediction in the decision-making process. Thus, it optimizes harmony and safety in an anomaly-free environment. In addition, machine learning models can assign a risk index to each employee, which determines their job competencies and verifies assumptions related to future competencies (Zuboff, 2020).

3. IT security management

The use of information and information technology tools in business activities has developed the boundaries of communication, cooperation and enabled the acquisition of new markets for innovative goods. In technologically developed economic activities, information becomes a tool for fighting unfair competition and a basic element of competition strategy. Information, is a special element of business tactics, which also becomes sometimes more important than access to capital - this is due to its economic value (Schwab, 2016). However, the intangible nature of knowledge makes the ability to protect knowledge ownership increasingly difficult. Its fluidity and simultaneity, which means that today knowledge (including IT), is difficult to retain for exclusive possession - this makes it necessary to protect it from loss.

The development of civilization makes us realize that the modern economy requires organizations to build qualitatively new relations with the environment that allow integration into innovation networks. And yet we must remember that the coupling of cognitive optimism of advanced science with entrepreneurship has always been limited by barriers, which in the system of their study involving technology transfer and commercialization of knowledge, allows us to identify sources of threats to this process. Its ordered set of barriers are: structural, systemic, awareness, cultural and competence barriers (Barrat, 2013). Certainly, in the near future, human activities related to information technologies will be associated with a specific type of knowledge-based organizations. These will be organizations created as a result of the virtualization process, which will most likely result in new barriers and their opposites, i.e. the driving forces of knowledge transfer. Virtualization as it turns out allows companies, regardless of size, to become fully competitive in the ever-changing global marketplace. At the same time, it will become a characteristic feature that the occurring „adjustment" process consists of a very fast learning process, as a result of which the organization adapts to the new requirements of the environment. At the same time virtualization enables rapid changes in the organizational structure as well as in the production or service profile. Acquisition of knowledge takes place not only thanks to the possession of appropriate personnel, but also thanks to global information technology enabling e-learning, for example (Takeuchi, 2017).

This issue becomes crucial if we consider that in business transactions entities disclose to each other various types of information, which often have significant economic value because they decide, for example, about the position of a given entrepreneur on the innovative technology market and its competitiveness (Matusiak & Guliński, 2010). Sometimes, even before the conclusion of an agreement defining the principles of cooperation, certain trade secrets are disclosed between entrepreneurs, which relate to, for example, the production process or used and previously designed technology.

Summing up, we can say that in today's world economy, we observe a significant reevaluation of the principles of business management, which is related to the computerization of information processed in them and its security. There are threats related to the lack of information security, which in a broad sense is a certain state. This state, as a result of actions negatively valued, is exposed to the loss of assumed level of: confidentiality, integrity, availability, accountability, authenticity and reliability. To the essential features of this process, in the author's opinion, should be included, first of all, all kinds of threats (including those resulting from the management of their production or services) and the problem of clarifying the concept of information infrastructure or the enterprise itself having such infrastructure. The rationale for the relevance of these issues stems from the aforementioned specificity of information security system management in enterprises and from: national distinctiveness, specificity of information protection, specificity of construction and functioning of information security management system elements and specific features of management in crisis management engineering.

Information security is understood as the state of confidence (supported by appropriate analyses, thought process) of an individual, a social group, the whole society about the availability and quality of acquired, stored, used and transmitted information. The subject of information security is therefore indirectly (in the case of control systems) or directly a person, whose need (access to information) can be fulfilled in this case (Zaskórski & Szwarc, 2013).

However, according to the author, the most effective in the security management process of information infrastructure turns out to be the collection obtained from the links between management levels, which is derived from planning information, operational information and control information. Therefore, in the developmental evolutionary process of such infrastructure, the use in the management structure of an expert support system based on data collection and its analytical processing and effective use becomes important. In addition, in the structure of such a system, due to the knowledge bases, its functions will change. This is the result of global access to information - the processes of information exchange, the sources of collected data or the resulting control of appropriateness and readiness of resources for reporting when supporting the decision-making process are changing. Therefore, the architecture of such a system in its elements must take into account, among other things, editing of databases and knowledge or, in the case of banking, the rules engine, i.e. alarms and notifications shaped by security considerations and „nodes" to external databases regulated by information protection. Depending on the threats and needs, the subsystem support modules can be expected with high probability. An example of this can be scenario alternatives carried out with the help of artificial intelligence against identified threats or business continuity and contingency plans.

According to the author of the study, currently in Poland, due to the costs, at the stage of preliminary research, modernized and tailored to a specific situation IT applications can be based on existing backbone systems, but only those which meet the basic requirements for the scale of progress. This makes it possible to assess the extent of modernization changes needed. Moreover, such an action streamlines the implementation process and profiles the needs for detailed IT modules created on order. Bearing in mind the professional experience and beliefs adopted on this basis, which profile the cognitive system, we can state that the data collected in the IT system already today often become the basis for the introduction of comprehensive optimization of management processes. Moreover, with appropriate authorizations, access to information allows to analyze threats more easily and in many dimensions. In this way it becomes a basis for conscious shaping of security of maritime infrastructure, for example on the basis of matrix analysis.

Moreover, it seems reasonable that in terms of basic research it becomes useful to build a rectangular cage matrix, in which such a picture of columns and rows best forms a coherent, transformable system. The matrix also allows profiling of data and information transfer channels for the so-called algorithmic machine language (software). However, under these conditions, it becomes further fundamental to solve problems related to:

- different objectives of competence groups, which are often in conflict with each other;
- low efficiency of communication between teams;
- poor coordination of activities that involve more than one team;
- difficulties in access to information.

Today, the identification of modern selected threats and challenges to the security of civilizational development in the 21st century, taking into account the information information infrastructure, the fourth level of development, can not omit the exploited areas of information warfare that form the basis of multigenerational conflicts (Sykulski, 2014).

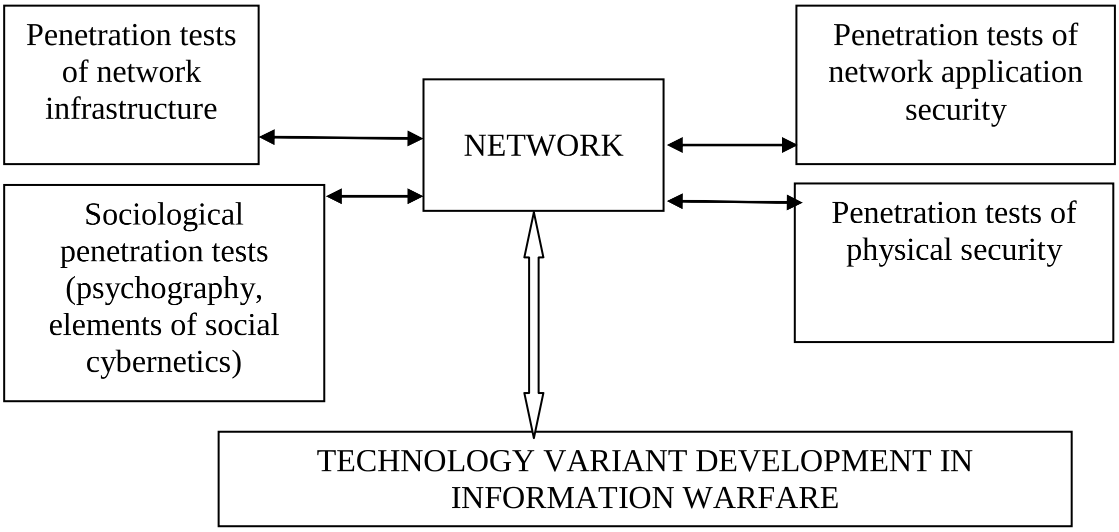
Penetration tests of network infrastructure
Sociological penetration tests (psychography, elements of social cybernetics)
NETWORK
Penetration tests of network application security
Penetration tests of physical security
TECHNOLOGY VARIANT DEVELOPMENT IN INFORMATION WARFARE

Figure 1. Elements of technology in information security management

Source: Own study.

Therefore, in response to innovations in information technology, new threats have emerged from the potential for hybrid warfare, network warfare, or cyber warfare that: (Sykulski, 2014):

– enable destabilization of globalization processes due to the development of computerized information and communication technologies;
– create sets of not fully explored ways of emergence of new methods of control over information resources.

Cyber warfare, is a serious challenge of the globalization era, which poses an increasing threat to the national interests of individual states. Functioning in a climate of information noise, or in other words, information smog, which results from the ubiquity of access to technology, humans are subjected to psychographic processes that violate their emotional integrity. Through the use of such mechanisms, we get information better tailored to us, which, due to individual and collective insecurity, weakens our perceptions. In turn, escaping the „information smog" we will fall into an „information bubble" which in turn narrows our perception. Thus, it neutralizes the human response to threats that are derived from the level of safety culture presented. Therefore, such action, creates a field for easy manipulation, which impedes the perceptual and logical reasoning, and through the planned transformation of social ties within this culture allows deformation of social consciousness towards the issues of security of information infrastructure.

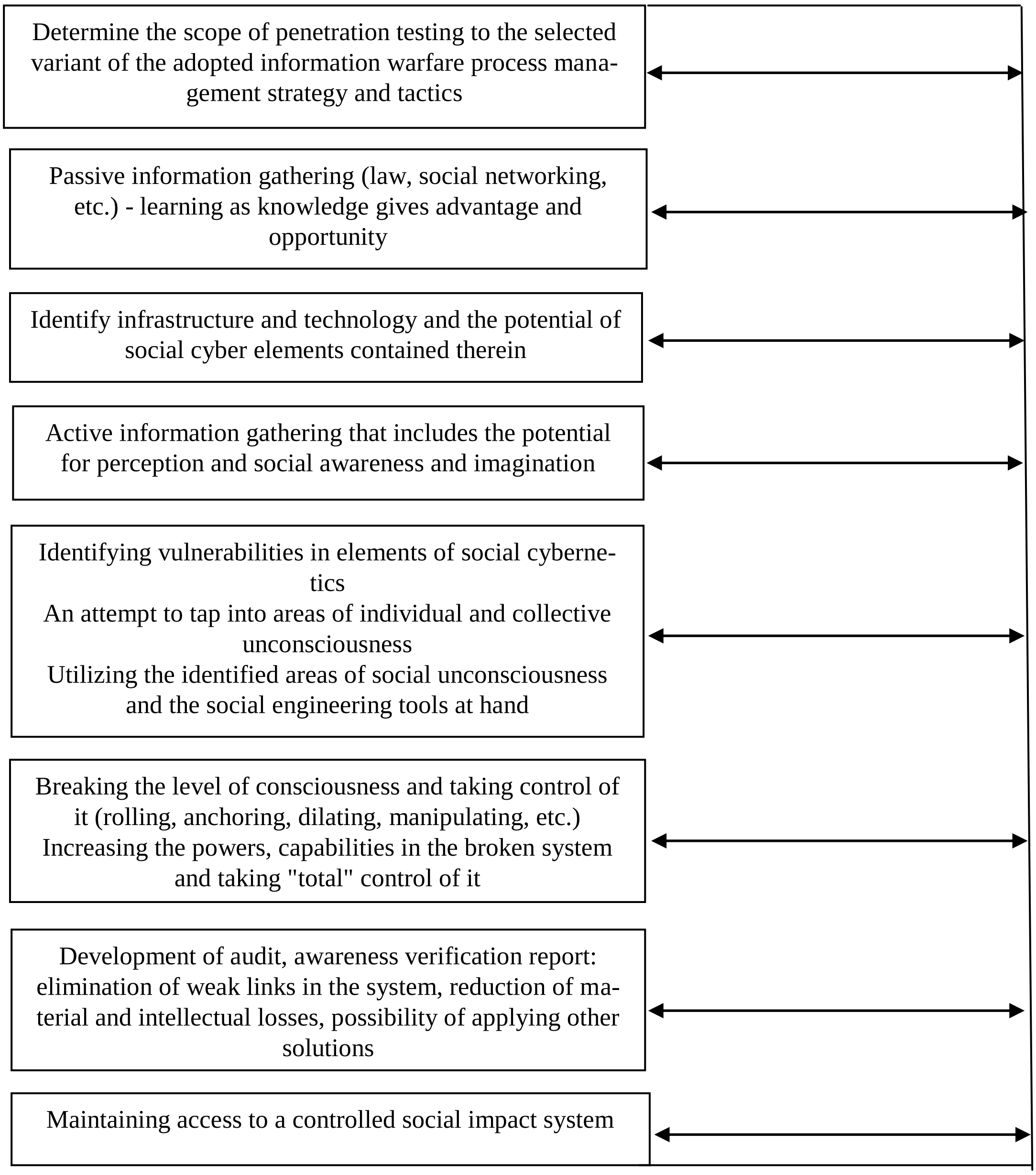
Determine the scope of penetration testing to the selected variant of the adopted information warfare process management strategy and tactics
Passive information gathering (law, social networking, etc.) - learning as knowledge gives advantage and opportunity
Identify infrastructure and technology and the potential of social cyber elements contained therein
Active information gathering that includes the potential for perception and social awareness and imagination
Identifying vulnerabilities in elements of social cybernetics
An attempt to tap into areas of individual and collective unconsciousness
Utilizing the identified areas of social unconsciousness and the social engineering tools at hand
Breaking the level of consciousness and taking control of it (rolling, anchoring, dilating, manipulating, etc.)
Increasing the powers, capabilities in the broken system and taking "total" control of it
Development of audit, awareness verification report: elimination of weak links in the system, reduction of material and intellectual losses, possibility of applying other solutions
Maintaining access to a controlled social impact system

Figure 2. Example variant of technology management in information war

Suurce: Own study.

IT security management must be consistent and form an integral whole with other management systems of the organization. It is also strongly connected with risk analysis in order to continuously improve its integrated mechanisms of continuous analysis, which are to guarantee systematic counteraction to threats.

The basic task is to define areas of potential risk and consider what is at risk and to what extent. Then the definitions and principles of information systems security management should be defined. To do this, it seems right to recommend the following tasks to be performed (Tvrdíková, 2011):

- developing an information technology security program,
- defining roles and responsibilities in the organization,
- configuration management of information systems,

- change management,
- informing employees about information system security features,
- selecting and implementing appropriate security.

In summary, when talking about IT security management, we can focus on two integral parts that make up the whole. The first part is to make all employees aware of and involved in IT security activities - including improving their competence. Another thing, equally important, is the selection and implementation of technical elements (hardware / software) that are optimal for the organization. However, in order to talk about security assessment, we must pay attention to the weakest links in our solution - whether they are stable - because it is them that our enemies will want to „hit”. Most often, in today's economic reality, the weakest link is the user - employee, client, contractor. That is why the first element mentioned above is so important. So what if we create the most modern and secure system, when it is the user who „lets in” an unauthorized third party. Therefore, IT security is related to organizational, social and technical safeguards, which will never be 100% secure anyway.

Conclusion

The problem of IT security management in modern organizations is certainly determined by many factors. However, the starting point for all, the author's task, is undoubtedly to create and implement a policy / strategy for security management in this very area. Importantly, all resulting policies must be clear and very precise, as there can be no discrepancies in their understanding among internal stakeholders, i.e. employees.

Very often human error is at the root of the most serious threat to IT security of any organization. It is statistically the main reason for inefficiency, or loss of time and money in organizations. There is nothing surprising in this, because making mistakes has always been in the nature of man and very often they result not from intentional actions, but from lack of caution, experience, stress or even exhaustion. To this group, some authors also include the so-called factors difficult to predict, which are primarily events associated with various natural disasters. In such situations we can never be sure how a person will react, whether it will not be an "impulse" for him to make a mistake (Olszak & Ziemba, 2017).

Definitely, however, the most relevant from the point of view of the author and the topic of this paper, are the intentional threats, associated with hostile actions of third parties. The average person thinks that they are mostly related to the operation of malware - the so-called viruses, or the action of people who break into IT systems in order to seize data - the so-called hackers. Unfortunately, this is only the tip of the iceberg, and the cyber war, which is most often known from the media and which consists of attacks on the enemy's information systems, has become more real than ever before in history.

To sum up, the purpose of this paper is certainly not an attempt to create or expose a selected, particular solution / model of IT security management. Nor did the author intend to present rankings or evaluate potential methods and techniques to provide such security. In organizations of the 21st century, information technologies, which are designed to support, simplify their key manufacturing or service processes, are increasingly complex and developed. They also support the creation of distributed - virtual organizations, whose efficiency is determined by the high level of IT sophistication. Hence these mechanisms are particularly endangered and require equally developed defense mechanisms with advanced technologies. Therefore, in the author's opinion, it is also important to pay attention to the problems with which the organizations have not been in contact so far and whose elimination can be the basis for survival in such a turbulent economic environment - in the era of the fourth industrial revolution. In this regard, it seems unquestionable that ensuring IT security of the organization in the XXI century appears to be one of its key resources.

References

Barrat J. (2013). *Our Final Invention: Artificial Intelligence and the End of the Human Era.* New York: Thomas Dunne Books.

du Vall M. (2019). *A super intelligent, people-centred society, or the idea of a Society 5.0 words a few.* „Państwo i Społeczeństwo", No 2, pp. 11-31.

Götz M., Gracel J. (2017). *The Fourth-Generation Industry (Industry 4.0) – Challenges to Research in the International Context*. „Kwartalnik Naukowy Uczelni Vistula", No 51, pp. 217-235.

Hermann M., Pentek T., Otto, B. (2015*). Design Principles for Industrie 4.0 Scenarios: A Literature Review.* „Working Paper", No 1, pp. 3-16.

Matusiak K.B., Guliński J. (2010). *System of technology transfer and commercialization of knowledge in Poland - driving forces and barriers*. Warszawa: Polska Agencja Rozwoju Przedsiębiorczości.

Olszak C.M., Ziemba E. (eds.). *Strategies and models of electronic economy*. Warszawa: PWN.

Senge P. (2008). *Fifth discipline.* Gdańsk: Wolters Kluwer.

Stadnicka D., Zielecki W., Sęp J. (2017). *Concept Industry 4.0 - evaluation of implementation possibilities on the example of a selected company,* [In:] R. Knosala (ed.), *Innovation in management and production engineering* (pp. 472-483). Opole: Polskie Towarzystwo Zarządzania Produkcją.

Schwab K. (2016). *The Fourth Industrial Revolution.* Cologny: The World Economic Forum.

Sykulski L. (20014). *Koncepcja Radykalnego Podmiotu i Czwarta Teoria Polityczna Aleksandra Dugina w kontekście bezpieczeństwa Polski i Unii Europejskiej*. „Przegląd Geopolityczny", No 8, pp. 237–238.

Takeuchi H. (2017). *Knowledge creation in an organization*. Warszawa: Poltext.

Toffler A. (2006) *Third wave*. Warszawa: PIW.

Tomański R. (2019). *The Japanese man of the new era, Society 5.0*. Pozyskano z: https://sektor3-0.pl/blog/japonski-czlowiek-nowej-ery-czyli-spoleczenstwo-5 (31.05.2022)

Tvrdíková M. (2011). *Selected aspects of information systems security management.* „Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu", No 32, pp. 107-117.

von Weizseker E., Wijkman A. (2018). *Capitalism, short-sightedness, population and the destruction of the planet.* Warszawa: Wydawnictwo Instytutu Badań Stosowanych Politechniki Warszawskiej.

Zaskórski P., Szwarc K. (2013). *Security of information resources as a determinant of information management technologies*. „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", No 9(7), pp. 37-52.

Zembski S. (2017). *Practical opportunities to use problematic learning in terms of adaptation to Industry 4.0 requirements.* „Quality production improvement", No 1, pp. 29-42.

Zuboff. S. (2020). *The age of surveillance capitalism, the struggle for the future at the new frontier of power.* Poznań ZYSK i S-ka.

https://www.japan.go.jp/latest/index.html (25.05.2022).

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMATYCZNYM W DOBIE CZWARTEJ REWOLUCJI PRZEMYSŁOWEJ

Streszczenie

Celem artykułu jest próba określenia i ocena uwarunkowań zarządzania bezpieczeństwem informatycznym na poziomie organizacji. Jest to szczególnie ważne w kontekście głównych filarów rewolucji przemysłowej 4.0, które obejmują integrację zaawansowanych systemów informatyki (IT), automatyki (OT), „Internetu Rzeczy" (IoT) oraz sztucznej inteligencji (AI). Wpływa to na systemy informatyczne, które cały czas stają się coraz bardziej rozbudowane i skomplikowane. Powoduje to wzrost zależności – im bardziej złożony system informatyczny tym bardziej złożone muszą być zabezpieczenia. Tym bardziej, że obecnie funkcjonowanie organizacji uzależnione jest od przetwarzania różnych informacji, dlatego też zarządzanie bezpieczeństwem informatycznym obejmuje zespół procesów zmierzających do osiągnięcia i utrzymania ustalonego poziomu bezpieczeństwa. W artykule przedstawiono także rodzaje zagrożeń informatycznych w odniesieniu do wykorzystania systemów wspomagających zarządzanie. Skoncentrowano się także na działaniach w aspekcie bezpieczeństwa informatycznego współczesnych organizacji.

Słowa kluczowe: czwarta rewolucja przemysłowa, infrastruktura informatyczna, zarządzanie bezpieczeństwem informatycznym

Klasyfikacja JEL: D83, M15, M40, O33

Michał Igielski
Gdynia Maritime University
Morska 81-87, 81-225 Gdynia
m.igielski@wznj.umg.edu.pl