Management and Production Engineering Review
Volume 13 • Number 3 • September 2022 • pp. 30–38
DOI: 10.24425/mper.2022.142380

Managerial Recommendations Concerning the Cybersecurity of Information and Knowledge Resources in Production Enterprises Implementing the Industry 4.0 Concept

Leszek PACHOLSKI

Poznan University of Technology, Faculty of Engineering Management, Poland

Received: 22 October 2021
Accepted: 10 June 2022

Abstract
The paper addresses a managerial problem related to ensuring cybersecurity of information and knowledge resources in production enterprises interested in the implementation of INDUSTRY 4.0 technologies. The material presented shows the results of experimental research of a qualitative nature, using two expert inventive methods: brain-netting and a fuzzy formula of inference. The experts' competences included the following three variants of the industrial application of the INDUSTRY 4.0 concept: (1) high production volumes achieved using a dedicated and fully robotic production line (2) the manufacture of short, personalized series of products through universal production cells, and (3) the manufacture of specialized unit products for individual customers. The Google Forms software was used to collect these expert opinions. The conclusions of the research carried out using the brain-netting method point to nine variants of the cybersecurity strategy of IT networks and knowledge base resources in manufacturing enterprises represented by the experts. The results of the research using the fuzzy formula of inference are numerically and situationally defined relations linking the above-mentioned nine strategies with five types of cyber-attacks. The summary record of these relations as the basis for managerial cybersecurity recommendations has a matrix form.

Keywords
Management, Cybersecurity, Information and knowledge resources, Industry 4.0.

Introduction

Car manufacturers, nowadays, operate in increasingly turbulent and unpredictable conditions both within the sector and in the business environment as a whole. The boundary between business and the environment is blurring, and various external factors are exerting an interactive and synergistic influence on the industry. The length of time from the appearance of required for a specific innovation to reach the market is becoming shorter and shorter. Moreover, the need to produce and deliver a high-quality product to the customer with efficiency and minimum expenditure (as well as, at the same time, continuously improving business so that it meets the challenges of sustainable development) requires commitment, fulfillment of all the functions of the company and the ability to use business opportunities (Trzcieliński, 2011). As a result, a whole range of modern concepts of production and enterprise management, including the Toyota Production System, Lean Production, Flow Manufacturing, World Class Manufacturing, and Agile Manufacturing, have become integrated in the automated and robotic world of production systems and enterprises (Pacholski, 1998; Pacholski & Kalkowska, 2019; Shrama & Kodali, 2008). This situation goes beyond the organizational and technological possibilities of:

- the industrialization of mechanical production processes (INDUSTRY 1.0),
- the concepts of production lines based on machines and electric generators (INDUSTRY 2.0),
- the current concept of the digitization of production processes based on software-controlled computers (INDUSTRY 3.0).

INDUSTRY 4.0 is, in a historical sense, the fourth stage of managerial, technological and organizational innovations in the field of industrial production and operation (use and service), and the improvement of technical creations, using the concept of unifying the

***Corresponding author**: Leszek Pacholski – Poznan University of Technology, Faculty of Engineering Management, ul. J. Rychlewskiego 2, 60-965 Poznan, Poland, phone: +48 61 665 34 10, e-mail: leszek.pacholski@put.poznan.pl*

real world of production machines with the virtual world of the internet and information technology [19] (Szczerbicki & Nguyen, 2021). This concept has ushered in a new era of high automation in production. Manufacturing processes have become part of the Internet of Things, where communication and collaboration between machines and humans take place in real time. Component functions of this cooperation ensure efficient management and include the supply chain and key elements of production, integrated planning and implementation, as well as the transparency and autonomy of logistics with intelligent storage. INDUSTRY 4.0 is not only "data digitization", but also a cyber-IT technological revolution creating new organizational, technological, economic, socio-cultural and political opportunities and benefits, which would not be possible without such solutions (Pacholski, 2020; Pacholski & Piotrowski, 2008). The virtual world of internet networks and information technologies connecting the real world of intelligent production and operational machines with intelligent information flow systems can, unfortunately, attract cybercrime (McClure et al., 2012; Shostack, 2014). The targets of such cyberattacks can be virtually all links of the Knowledge Base. This applies not only to the database itself, but also to its interfaces and modules (the knowledge accumulation subsystem and both the applicant and explanatory subsystems). Its input components (construction and operation, building and improvement of the base) and output components (use and servicing of the base as well as the utilization of used and useless resources) are also particularly vulnerable to cyberattack (Hadnagy, 2014; Shostack, 2014).

With the above in mind, it should be stated that ensuring the cyber-security of information and knowledge resources in an enterprise implementing the INDUSTRY 4.0 concept is a serious managerial issue (Pacholski, 2020; Pacholski & Piotrowski, 2008; Szczerbicki E. & Nguyen N.T. (2021)). The material presented in this paper consists (in the sense of the type of research conducted) of a case study. Expert surveys, using brain-netting and a fuzzy formula of inference, were carried out on the car assembly line (the scope and object of research). The aim of the research was to examine the hierarchical structure of the recommended strategies and managerial programs ensuring the cybersecurity of information and knowledge resources in enterprises.

From Business Intelligence System to knowledge base

Modern cars are characterized by considerable design complexity and the use of various assembly technologies in their production. Car manufacturing is a complicated process, consisting of many phases and stages (Kalkowska, 2018; Kalkowska & Pacholski, 2017). The production processes of this branch of industry have so far been an exemplary technological, organizational and economic implementation challenge for the concepts of the Toyota Production System, Lean Production, Flow Manufacturing, World Class Manufacturing, and Agile Manufacturing. The implementation of these concepts in the automated and robotic world of production systems requires the new application of information technologies, going beyond the organizational and technological possibilities of the first three industrial revolutions. In terms of the IT systems of databases for data resources, information and knowledge, the INDUSTRY 4.0 concept requires a transition from solutions such as digital data processing to those based on a search of symbolically described knowledge resources. The diagram of a "classic" digital data processing system known as the Business Intelligence System consists of the following four steps:

- Data Sources – defining data sources located in the enterprise, for example: Enterprise Resource Planning systems (resource planning including: sales and finance- accounting – payroll); Customer Relationship Management – a system that automates and supports processes at the client-enterprise interface (marketing, sales, customer service, and management); Human Resource Management System; Learning Management System (training and skills); raw text files, spreadsheets and many other forms of data imaging.
- ETL processes (Extract, Transform and Load) – processes that include data extraction from an operational data source and data transformation – this stage may include data cleansing, filtering and the implementation of business rules, and loading data into the data warehouse.
- Data Warehouse – a type of database that is organized and optimized for a certain slice of reality (OLAP Cube – a data structure that allows you to quickly analyze data stored in a similar way to multivariate spreadsheets rather than as a traditional relational database).
- User Reports – on the basis of data from the warehouse, more complex analyses are carried out and lists are drawn up concerning, for example, predictions or the most probable ways to develop a distinguished phenomenon in the coming period, where the basis of this selection is, the current course of this phenomenon, and the current state of the system).

The general concept of the Knowledge Base as a recommendation for moving from database-type solu-

tions to solutions based on the search of knowledge resources, in accordance with the requirements of the knowledge-based economy and as a premise for the implementation of the INDUSTRY 4.0 concept, is shown in Figure 1.

Stakeholders of the Knowledge Base in the automotive sector are both constructors, users and service technicians, as well as the digitizing and cyber-physical devices using the services of this system. Component functions realized in the real time communication and cooperation between people and machines within the framework of the INDUSTRY 4.0 concept must ensure efficient management. These include: the supply chain and key elements of production; integrated real-time planning in order to better use production machines and increase their efficiency; digitization and automation of processes for optimal use of resources (human and hardware) and faster operational performance; control of product flow for better inventory management and optimization of logistics management; real-time quality control based on data analysis, and the implementation as well as transparency and autonomy of logistics with intelligent storage. These functions can provide excellent results both in terms of the flexibility, efficiency and cost reduction in all the afore mentioned processes, and in terms of customer service. The use of artificial intelligence, based on Big Data, System Integration, Additive Manufacturing, and Augmented Reality, enables the quick process of personalizing production. It also makes it possible to analyze and understand customer behavior, be "agile", take necessary actions to meet customer requirements and trends, and finally personalize products and services. Smart, digital products and services offer new functionality, reliability and capabilities that traditional products do not have. In addition to mechanical and electrical parts, each product combines: hardware, sensors, data memory, microprocessors, software and connectivity. All this constitutes a connected and flexible cyber-physical system, enabling agile adaptation to new challenges. The Knowledge Base system uses (in terms of creating a subsystem for collecting knowledge and managing its base) the methods of the symbolic representation of knowledge, as well as sub-symbolic methods and programs facilitating the implementation and management of the system. In the progressive, regressive and mixed inference module, it uses both classical bivalent logic and fuzzy logic (Atlam et al., 2019; Pacholski, 1998) and has the ability to solve problems that are not efficiently algorithmizable. It bases the solving of management problems on either strict mathematical and logical models of the analyzed problems and their implementation in the form of "intelligent" computer programs (evolutionary algorithms and fuzzy logic methods), or on the "self-learning" of "intelligent" computer programs based on models of neural networks and associative networks (neural networks, machine learning, and image recognition). Using Artificial Intelligence, it supports the hardware (digitizing and cyber-physical) processes of programmable multitasking manipulators, cobots and robots (Pacholski & Kalkowska, 2014). Finally, the Knowledge Base can perform some tasks of the knowledge-based economy

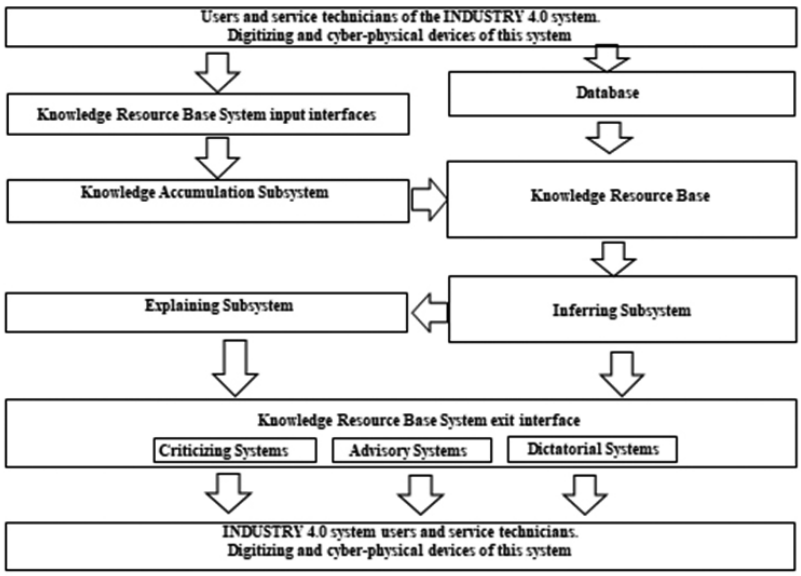

Fig. 1. Concept of the Knowledge Base [own study]

relating to professional decision-making and managerial activity. In car manufacturing companies interested in implementing the INDUSTRY 4.0 concept, such decisions and actions mainly cover the following issues:

- the intensive development and use of information and communication technologies in decision-making pertaining to industrial manufacturing processes,
- the intensive development and use of digitizing technologies and cyber-physical devices implementing production processes based on the methods of Artificial Intelligence,
- the globalization of manufacturing, competition, investment and labor markets,
- the turbulence and limited predictability of the environment,
- the constant change and uncertainty of the market, requiring creativity and innovation,
- the flexibility of operations and quick adaptation to new market conditions,
- a focus on the customer and an appreciation of their growing knowledge and requirements.

Cyberattacks and cybersecurity of knowledge resources

As previously mentioned, the stakeholders of the Knowledge Base, within the INDUSTRY 4.0 concept, are both constructors, users and service technicians, as well as the digitizing and cyber-physical devices of this system. Component functions realized in real time communication and cooperation between people and machines can, on the one hand, ensure efficient management, but on the other hand, can open up a number of possibilities for external interference (Brooks et al., 2018; Cappelli et al., 2012; Curran, 2020). It should also be added that the possibility of such interference is created by the storage of data and knowledge on a centralized Cloud Computing server. Despite this, this solution enables remote work and significantly improves its flexibility. However, in time-critical computing, users are now shifting to edge computing, which pushes data storage and processing closer to the point at which it is needed. Placing computing power as close as possible to the sensors recording data, information and knowledge reduces the amount of this information sent to the cloud, which effectively shortens the reaction time of the computer network.

The exposure of today's enterprises to cyber risk is also related to the fact that the current number of connected IT devices in the world is over 20 billion. Therefore, more and more companies are faced every day with the increasing threat of cybercrime. Cybersecurity is rapidly becoming a growing concern for businesses around the world. Nowadays, managers and investors need clear parameters and benchmarks to assess whether a company and its IT operations are cyber-secure. However, these expectations clash with realities such as the fact that (Brooks et al., 2018; Copertari, 2021; Lee, 2021):

- the skills gap and the lack of qualified personnel in the field of cyber risk can cause a bottleneck in a company's cybersecurity,
- by the end of last year, there were two million vacancies in cybersecurity,
- 230,000 new malware programs are created every day,
- more than 4,000 cyber ransoms are demanded daily.

According to the World Economic Forum, the eventual removal of a single cloud provider could result in economic losses ranging from $50-120 bln. These are losses on a scale similar to those caused by Hurricane Katrina. However, instances of cyber-racketeering (the most recent example of which is the payment of over $4 mln dollars to Russian hackers by the US company Colonial Pipeline after a cyber-attack on its fuel transfer system), must be distinguished from the consequences of a lack of elementary leadership in managing the security of corporate information assets, or even countries. A textbook case is that of Alteryx, a company conducting marketing analysis. The company left an unsecured Knowledge Base on the internet, containing the confidential business information of approximately 123 million American households. The same category may also include the use by members of the highest state authorities in Poland (from October 2020 to June 2021) of instant messaging services, unprotected by the state security services, to send information relating to management of the country.

Cybersecurity theorists and practitioners (Curran, 2020; Hadnagy, 2014; Parkinson, 2017) have cataloged the following five types of cyberattacks:

- so-called Advanced Persistent Threats – this type of cyberattack uses many phases of the functioning of the IT network and the Knowledge Base of the enterprise in order to collect information on the communication and cooperation of the objects of this system, and then strikes at a specified time (A in Figure 2),
- Phishing – a type of fraud in which cyber criminals try to access the company's IT network via e-mail or other internet social engineering meth-

ods in order to obtain confidential information enabling access to this network and the Knowledge System (B in Figure 2),
- Internal Attacks – a form of cyberattack using confidential information, often from trusted users as well as employees and external contractors with specific, authorized access to the company's computer network (C in Figure 2),
- Distributed Denial of Service – DDoS (a cyberattack in which multiple sources attack a web server, website or other known network device of a company and overwhelm it with a flood of messages, packets and connection requests, causing a slowdown or failure in the Enterprise Knowledge Base a consequence of this cyberattack is the unavailability of the company's IT system for its users (D in Figure 2),
- Ransomware – a type of computer malware combined with a ransom note for its elimination; this software locks and encrypts devices on an enterprise's IT network to prevent users from accessing that computer network if the ransom demanded is not paid (E in Figure 2).

Managers and investors who need clear parameters and benchmarks to assess whether their companies' IT activities meet cybersecurity requirements are now employing various types of defense strategies (Atlam et al., 2019; Brooks et al., 2018; Cappelli et al., 2012; Shostack, 2014) based on the following four preventive measures:

- Organizing practical training in the field of cybersecurity for all company staff employed directly in the company's IT department, as well as those communicating and cooperating with this technology as part of, for example, implementation of the INDUSTRY 4.0 concept (W in Figure 2),
- Hiring other companies specializing in the delivery of cybersecurity services to professionally check the resilience of the enterprise's own IT systems – such companies then carry out simulated, phased cyberattacks to recognize the cybersecurity level of their client's systems (X in Figure 2),
- Introducing general or regional (for example, in all European Union countries) data protection regulations, which require the reporting of cybersecurity breaches (such projects improve the recognition of potential cyberattacks) (Y in Figure 2),
- Implementing an automated defense system against a cyberattack (such a system provides a wide range of defense tactics; it is used after checking the success of the automatic attack simulation; this type of simulation acts as a pseudo-hacker trying to "dig through" the cyber-security systems of the company's IT network 24 hours a day, 7 days a week; an automated defense system against cyberattack provides real-time feedback on such a case and allows the use of numerical simulations to estimate the distribution of aggregate losses as a result of such an attack). It is also possible to use this system to study extreme risk scenarios such as mass cyberattacks (the analysis of these scenarios can be used to develop a comprehensive assessment of the possibility of the spread of future cyberattacks). An automated cyberattack defense system also enables enterprises and government institutions to design appropriate responses in the event of a potential cyberattack (Z in Figure 2).

Research method

A study of managerial recommendations on the cybersecurity of the knowledge base in a company introducing the requirements of the INDUSTRY 4.0 concept was carried out on the basis of a case study using two expert inventive methods: brain-netting and fuzzy inference formula. Seven managers employed in managerial positions in car manufacturing companies were appointed as experts. The competences of these experts included the following three variants of the industrial implementation of the tool technologies of the INDUSTRY 4.0 concept (Pacholski & Kalkowska, 2019):

- high volumes of car production (with a cost level lower than the competition) by dedicated and fully robotic production lines with common picking modules, using digital tool technologies of the INDUSTRY 4.0 concept,
- the manufacture of short, personalized series of cars (the so-called "mass individualization" of production processes), through highly individualized, robotic, universal production cells (having the value of frequent changeovers), using the digital tool technologies of the INDUSTRY 4.0 concept,
- the manual production of cars with the highest unit value, manufactured for individual clients, by top-class specialists using the digital tool technologies of the INDUSTRY 4.0 concept in order to improve the organization of production processes and increase the "ergonomics" of human work.

The Google Forms software was used to collect these expert opinions. The starting point for the research carried out using the brain-netting method consisted of the four aforementioned types of practical preventive measures (W, X, Y, Z) for the cybersecurity of the IT networks and knowledge base resources in the manufacturing companies represented by the

experts: practical training in the field of cybersecurity for all staff employed directly in the company's IT department, as well as those communicating and cooperating with this technology, was given the symbol W; hiring other companies specializing in the delivery of cybersecurity services to carry out simulated cyberattacks in order to check the resilience of an enterprise's IT systems was given the symbol X; the symbol Y was given to projects involving the implementation of general, for example European, regulations on the protection of computer data based on reported cases of cybersecurity violations; and the fourth symbol Z, was given to the implementation of an automated defense system against cyberattack, providing a wide range of defense tactics, after prior checking of the resilience of the company's own IT systems to automatic attack simulation.

Possible variants of these combinations of preventive cybersecurity measures were analyzed using the brain-netting method. These combinations together with the four source ones (W, X, Y, Z) form a set (Fig. 2) of nine types (1, 2, 3, ..., 7, 8, 9) of the main managerial recommendations on the cybersecurity of information and knowledge resources in production enterprises implementing the industry 4.0 concept. The rejected combinations (one "binary" and two "triples") refer to projects containing the term XZ which experts found redundant These redundant combinations in Table 1 are marked with the symbol #.

In order to examine the binding relations (based on a fuzzy inference formula) between the nine variants of cybersecurity strategy and the five types (A, B, C, D, E) of cyberattacks on IT networks and knowledge base resources in the manufacturing companies represented by the experts, five levels of expert assessment of the strength of these relations were adopted. Thus, the matrix constituting the analytical basis of managerial cybersecurity recommendations covers 45 individual situations.

Table 1
Course of analysis and five resulting combinations (5, 6, 7, 8, 9) of additional (in relation to four source) preventive cybersecurity measures (own study)

	WX	XY	WZ	YZ	WY	XZ
W	*		*		*	*
X	*	*				
Y		*		*	*	
Z			*	*		*
	5	5	6	6	6	#

	WXY	WXZ	WYZ	XYZ
W	*	*	*	
X	*	*		*
Y	*		*	*
Z		*	*	*
	8	#	9	#

As part of the fuzzy formula of inference, the probabilities of the high (h), medium (m) and low (l) strength of the relationship (Atlam et al., 2019; Pacholski, 1998) are marked with the symbols: pa_i^h, pa_i^m and pa_i^l. The seven aforementioned experts were entrusted with the task of determining the above probabilities. The probability boundary conditions were defined as follows:

$$\begin{aligned} &pa_i^h + pa_i^m + pa_i^l = 1 \qquad \text{and} \\ &pa_i^h \geq 0; \quad pa_i^m \geq 0; \quad pa_i^l \geq 0, \quad \text{where} \quad i \in 1, n \end{aligned} \tag{1}$$

Subsequently, a five-level linguistic scale of expert assessments was proposed. Moreover, the linguistic variable z was introduced to describe the strength of the analyzed relations and the fuzzy scale presented below (Table 2).

Table 2
Recommended fuzzy scale for linguistic variable z (Pacholski, 1998)

#	Assessment by seven experts	Scale
1	no relationship	$0 < z < 0.333$
2	strength of relationship is low	$0.167 \leq z < 0.5$
3	indirect relationship	$0.333 \leq z < 0.667$
4	strength of relationship significant	$0.5 \leq z < 0.833$
5	dominant relationship	$0.667 \leq z \leq 1$

The notation d_j was further introduced as the result of the assessment by expert j-th, where: ($d_j \in 1, 2, 3, 4, 5$). According to the fuzzy sets theory (Atlam et al., 2019; Kalkowska, 2018; Pacholski, 1998), membership in set N was expressed by the membership function for the interval $[0, 1]$ of the form: $\mu N(x)$. Each result of seven DJ expert assessments was assigned to five fuzzy sets.

For example, the first set was:
$N_1 = \{(\beta 1, \mu N(\beta 1)),\ (\beta 2, \mu N(\beta 2)),\ (\beta 3, \mu N(\beta 3))\}$, while the fifth was:
$N_5 = \{(\beta 5, \mu N(\beta 5)),\ (\beta 6, \mu N(\beta 6)),\ (\beta 7, \mu N(\beta 7))\}$ for each of the seven expert assessments.

Then, a standardized set of fuzzy relationships (Table 3) of the scale of relationships was taken into account, linking nine variants of cybersecurity strategies

with five types (A, B, C, D, E) of cyberattacks on IT networks and knowledge base resources in manufacturing companies represented by the experts:

- (0, 0.333) – insignificant relationship,
- (0.333, 0.667) – the relationship is moderately significant,
- (0.667, 1.0) – a very important relationship.

Table 3
Normalized fuzzy set for three variants of relationship (low, medium and very significant) linking nine variants of cybersecurity strategy with five types (A, B, C, D, E) of cyberattacks on IT networks and knowledge base resources in manufacturing companies represented by experts (Kalkowska, 2018; Pacholski, 2020)

Type of relationship	Fuzzy set				
	N_1	N_2	N_3	N_4	N_5
Insignificant relationship Moderately significant Very important relationship	0; 0.5	0; 0.0	0; 0.0	0; 0.0	0; 0.0
	0.167; 1.0	0.167; 0.5	0.167; 0.0	0.167; 0.0	0.167; 0.0
	0.333; 0.5	0.333; 1.0	0.333; 0.5	0.333; 0.0	0.333; 0.0
	0.5; 0.0	0.5; 0.5	0.5; 1.0	0.5; 0.5	0.5; 0.0
	0.333; 0.0	0.333; 0.0	0.333; 0.5	0.333; 1.0	0.333; 0.5
	0.167; 0.0	0.167; 0.0	0.167; 0.0	0.167; 0.5	0.167; 1.0
	1.0; 0.0	1.0; 0.0	1.0; 0.0	1.0; 0.0	1.0; 0.5

Finally, fsf was introduced as an element of the fuzzy set s and msf as a membership function for the corresponding element of fuzzy sets presented in Table 2 and the probabilities of the generalized evaluation of the seven experts were calculated (in two steps) as follows:

- Calculation of the average P_i probability score (where: $i = 1, 2, 3$), reflecting the frequency of the selection made by the experts:

$$P_1 = \sum_{f=1}^{3} f_{1f} m_{1f}; \qquad P_2 = \sum_{f=3}^{5} f_{2f} m_{2f}; \qquad P_3 = \sum_{f=5}^{7} f_{3f} m_{3f} \tag{2}$$

- Calculation of p_i (where: $i = 1, 2, 3$) corresponds to the probability of the significance of the relationship:

$$p_i = \frac{P_i}{\sum_{i=1}^{3} P_i} \tag{3}$$

Research results and recommendations

The results of the research, based on the fuzzy formula of inference and relating to the relationships linking nine variants of cybersecurity strategies with five types (A, B, C, D, E) of cyberattacks on IT networks and knowledge base resources in manufacturing companies represented by the experts, are shown in matrix form (Figure 2).

	A	B	C	D	E	cybersecurity
W	0.500	0.583	0.500	0.500	0.500	0.517 IV
X	0.714	0.714	0.714	0.583	0.583	0.662 III
Y	0.583	0.500	0.583	0.500	0.500	0.533 IV
Z	0.833	0.833	0.714	0.714	0.583	0.735 II
WX +XY	0.833	0.714	0.714	0.583	0.583	0.685 III
WZ +YZ	0.833	0.833	0.833	0.714	0.714	0.785 II
WY	0.583	0.583	0.583	0.500	0.500	0.550 IV
WXY	0.833	0.833	0.714	0.714	0.714	0.762 II
WYZ	0.833	0.833	0.833	0.833	0.833	0.833 I

Fig. 2. Decision-making matrix of managerial recommendations regarding cybersecurity of information and knowledge resources in manufacturing companies introducing INDUSTRY 4.0 concept [own study]

This matrix may constitute the decision-making basis for managerial recommendations regarding the cybersecurity of information and knowledge resources in manufacturing companies introducing the INDUSTRY 4.0 concept.

- The strongest recommendation (Variant I in Figure 2) of cybersecurity of information and knowledge resources in production companies introducing the INDUSTRY 4.0 concept is the integration of a professional, automated system with a wide spectrum of defense tactics (checking the resilience of the company's IT resources to the automatic simulation of a cyberattack by a pseudo-hacker trying to "dig" through these resources for 24 hours a day, 7 days a week) with the simultaneous implementation of practical training (covering all employees of the company) according to applicable regional data protection regulations and the identification of potential cyberattacks.
- The second group (Variant II in Figure 2) of relatively strong recommendations includes the following three variants: the first consists of two-stage support for the implementation of a professional, automated system with a wide range of defense

tactics, first through the simultaneous implementation of training, and then the application of pertinent regional regulations on data protection and the recognition of potential cyberattacks. The second option is similar to the strongest recommendation mentioned above, but its basis is not the implementation of a professional, automated system with a wide range of defense tactics, but the regular hiring of companies specializing in the delivery of cybersecurity services for the one-time verification of the resilience of the company's own IT systems already in operation by carrying out a series of simulated, staged cyberattacks recognizing the client's cybersecurity level. The third option, on the other hand, consists of the implementation of a professional, automated system with a wide range of defense tactics without support in the form of applicable cybersecurity standards and training for the company's employees.

- Conditionally (Variant III in Figure 2), it is also possible to recommend (but with weaker argumentation) two solutions based on the hiring of companies specializing in the delivery of cybersecurity services for a one-time verification of the resilience of the company's own IT systems already in operation by conducting a series of simulated, staged cyberattacks recognizing the client's cybersecurity level. In the first variant, (more recommended), conducting a series of simulated reconnaissance cyberattacks is first supported by the simultaneous implementation of training of the employees of the client's enterprise, knowledge of the applicable regional data protection regulations, and then identification of potential cyberattacks. In contrast, the second option includes the service of checking the resilience of the client's own IT systems already in operation by conducting a series of simulated, stage cyberattacks in order to recognize the level of cybersecurity.
- The remaining three recommendations (option IV in Figure 2) out of the nine analyzed in this research (covering only employee training and standardization projects) concern stimulating the company's interest in the issue of the cybersecurity of its own IT systems. However, they do not provide defense against any of the five cyberattacks mentioned in this article.

Acknowledgments

The implementation of the proposed approach is a difficult undertaking. It presents four categories of challenges: economic, organizational and technological, social, and political. The economic challenges are investment-related and concern the difficulty in assessing the cost-effectiveness of cybersecurity projects. Implementation of the proposed solutions also means adapting the traditional business model of the enterprise to the new reality of threats from potential cyberattacks. The organizational and technological challenges correspond to the reliability and stability of production (or service) and the enterprise's IT systems, as well as the employees' lack of knowledge and experience relating to a transition to the fourth industrial revolution. Societal challenges consist of privacy concerns, aversion to radical reengineering and new forms of surveillance. People's concerns also relate to the risk of losing tasks to robotic work processes and those supervised by IT systems. Political challenges relate to the lack of formal regulations in terms of standards for the certification of projects in the field of cybersecurity, and to unclear legal issues relating to cybercrime.

References

Atlam H.F., Walters R.J., Wills G.B., and Daniel J. (2019), Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT, *Mobile Networks and Applications*, Vol. 26, pp. 2545–2557.

Brooks Ch.J., Grow Ch., Graig Ph., and Shirt D. (2018), *Cybersecurity.* Essentials, Wiley.

Cappelli D.M., Moore A.P., and Trzeciak R. (2012), *The CERT Guide to Insider Treats*, Addison-Wesley Professional.

Copertari L.F. (2021), Comprehensive project risk management methodology, *Advances in Social Sciences Research Journal*, No. 1, Vol. 8, pp. 94–115.

Curran K. (2020), Cyber security and the remote workforce, *Computer Fraud & Security*, ELSEVIER, No. 6, Vol. 2020, pp. 11–12.

Hadnagy Ch. (2014), *Social Engineering: The Science of Human Hacking*, Wiley.

Kalkowska J. (2018), *Pro-exploitation Approach in the Processes of Creating Public Transport Vehicles*, Publishing House of the Poznan University of Technology, (in Polish).

Kalkowska J. and Pacholski L. (2017), Simulation technologies in agile reconfiguration of assembly production process, *Organization Review*, No. 2, pp. 49–55 (in Polish).

Lee I. (2021), Cybersecurity: risk management framework and investment cost analysis, *Business Horizons*, No. 4, Vol. 16, pp. 66–71.

McClure S., Kurtz G., and Scambray J. (2012), *Hacking Exposed 7: Network Security Secrets and Solutions*, McGrow Hill.

Murino T., Naviglio G., Romano E., Guerra L., Revetria R., Mosca R., and Cassettari L.C. (2012), World Class Manufacturing Implementation Model, *Applied Mathematics in Electrical and Computer Engineering*, Cambridge, Harvard, pp. 371–376.

Pacholski L. (1998), Fuzzy Logic Application in Ergonomic Renewal of Multiagent Manufacturing Systems, *Cybernetics and Systems: An International Journal*, Vol. 29, pp. 715–728.

Pacholski L. (2020), *Managerial Premises for the Implementation of the Industry 4.0 Concept on the Car Assembly Technology Line*, [in:] Sustainable Economic Development and Advancing Education Excellence in the Era of Global Pandemic, Proceedings of the 36th International Business Information Management Association Conference (IBIMA), pp. 4189–4199.

Pacholski L. and Kalkowska J. (2019), *Prospectives of Ergonomics and Organization Paradigms' Changes of Machines Manufacturing Processes*, [in:] Pacholski L., Kalkowska J., Kielbasa P., [eds.] Ergonomics in the Face of the Challenges of Mass and Globalization in Production, Cracow University of Technology and Polish Academy of Arts and Sciences Editorial Board, pp. 5–52, (in Polish).

Pacholski L. and Piotrowski K. (2008), Political Ergonomics, Macroergonomic Battles, *Human Factors and Ergonomics in Manufacturing*, No. 5, Vol. 185, Wiley-Blackwell, pp. 515–524.

Parkinson S. (2017), Use of access control to minimise ransomware impact, *Network Security*, No. 7, Vol. 2017, pp. 5–8.

Shostack A. (2014), *Threat Modeling. Designing for Security*, Wiley.

Shrama M. and Kodali R. (2008), Development of a Framework for Manufacturing Excellence, *Measuring Business Excellence*, No. 4, Vol. 12, pp. 50–66.

Szczerbicki E. and Nguyen N.T., Cognitive Systems, Concepts, Processes, and Techniques for the Age of Industry 4.0, *An International Journal Cybernetics and Systems*, No. 5, Vol. 52, pp 293–295.

Trzcieliński S. (2011), *Agile Enterprise*, Publishing House of the Poznan University of Technology (in Polish).