Research Article • 10.2478/ijcm-2023-0017 IJCM • 60(1) • 2024 • 17-26

Determinants of business management in the digital age

Joanna Antczak*

*Military University of Technology, Warsaw, Poland. E-mail: joanna.antczak@wat.edu.pl

Abstract ***Purpose.*** *The 21st century is an era of rapidly expanding digitization in which cyber security is a key global challenge. Digitization creates cyber security risks. One of the problems of cyber security are issues related to accessibility of an organization's systems. The subject of this article is the management of an enterprise in the digital age. Digital amenities simultaneously generate new development opportunities and dynamic progress for enterprises, which are also susceptible to the threats occurring in cyberspace. The analytical goal was to identify the determinants of enterprise management in the context of their operation in cyberspace, which is characterized by a lack of borders, dynamism, and anonymity, and represents one of the most expanding areas of threats in the modern world.*

Design/methodology/approach. *In achieving the goal, the starting point was to present the cyber security of the business entity as an area that has a decisive impact on the management of the company in the digital age. Then, in order to analyse the actual market situation, part of the survey research on cyber security in the business unit was presented. In May 2022, survey research using a questionnaire method by the author of this article with the use of a telephone interview was conducted on behalf of the IPC Research Institute Ltd. based in Wroclaw. The survey was conducted on a sample of 100 enterprises from various industries operating on the territory of the Republic of Poland. The following research methods and techniques were used in the article: survey methods, induction methods as a form of going from the particular to the general, analytical methods, deduction method as a form of generalization and inference, literature analysis.*

Findings. *Research has confirmed that the cyber security of the business unit is a key determinant in the digital age. The publication indicates the need to conduct and develop research on the determination, analysis, and presentation of mechanisms for managing the business unit in the area of cyber security as a security protection in the digital age.*

Originality/value. *The value of the article is the analysis of the author's survey conducted on a sample of 100 companies from various industries operating in the Republic of Poland, and the identification of cyber security as one of the main challenges in the digital age. The article is addressed to executives in order to make them aware of the need to conduct an ongoing analysis of the company's performance in cyberspace in order to locate weak areas of operations and adjust the strategy accordingly to the company's capabilities and goals.*

Keywords digital era, cyber security, business management.

INTRODUCTION

Modern management of an organizational unit requires taking into account various, often unpredictable, changes and, at the same time, adapting organizational structures and processes occurring in them to the requirements of the changing market (Liu et al., 2019; Zakrzewska-Bielawska, 2017; Czernek-Marszałek, Piotrowski, 2022; Bitkowska, Sobolewska, 2020; Cyfert, 2023). The extraordinarily rapid emergence of new technologies is outpacing the ability of both producers and consumers to prepare in advance for the changes to the regulatory mechanisms constituting their institutional environment. Thus, there is a phenomenon of blockage, caused by confinement in the “old” systemic framework that prevents economic agents, primarily enterprises, from opening up to new challenges. Chaotic and haphazard formulation of institutional conditions is increasingly difficult to fit into the implementation of complementary market functions of the state as a regulator of socio-economic phenomena, often demonstrating its weakness in supporting, as well as protecting, the interests of businesses forced by global market challenges to try to seek competitive advantages in the carriers of the digital era (Mączyńska, Okoń-Horodyńska, 2020 p. 9).

The enormous potential of the Internet has led to a change in the meaning of geographical boundaries by which geographic distance no longer plays such a role as in previous decades. Ownership of a computer and access to the Internet has made it possible to carry out most administrative, political, and business activities more efficiently without being present at the

†Corresponding author

Open Access. © 2023 Joanna Antczak, published by Sciendo
This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

workplace. Any person with a personal computer can become a sender of content. Nowadays, it is not unusual for messages to be downloaded, transmitted, and saved with a single movement of a computer mouse or a click of a key (Górka, 2017, p. 73).
The 21st century is an era of rapidly expanding digitization or the Internet of Things, in which cyber security is a key global challenge. Digitization creates cyber security risks, including issues related to the accessibility of an organization's systems.
Cyber security is both a civilization problem and a classic example of an issue that cannot be analyzed or solved within a single sector. To ensure digital security for the state, institutions, and citizens, it is necessary to have a dialogue and partnership of many actors. This applies to both strategy and operations. Considering the legal aspects, cyber security is on the one hand an issue of public law (e.g., protecting the secrets of a business entity in cyberspace), and on the other hand, an issue of private law (e.g., securing the personal data of employees or contractors). The EU and its member states need a coherent system of protection based on standards for entities affected by cyber security. Protection in the digital world cannot be provided in isolation from the world. Cyber security is also a general issue of stability.
The subject of this article is the management of the enterprise in the digital age. On the one hand, there are digital facilities generating new development opportunities and dynamic progress, and on the other hand they have their weaknesses, namely, the threats occurring in cyberspace.
The analytical goal was to identify the determinants of enterprise management in the context of their operation in cyberspace, which is characterized by dynamism, anonymity, and a lack of borders, and represents a growing area of danger in the modern world.
In achieving the goal, the starting point was to present the cyber security of the business unit as an area that decisively impacts the company's management. Then, in order to analyze the actual market situation, the author surveyed a sample of 100 enterprises from various industries operating in the Republic of Poland in May, 2022. These enterprises were interviewed over a telephone using a questionnaire about cyber security in the business unit. This research was conducted on behalf of the IPC Research Institute Ltd., based in Wroclaw.
The article uses the following research methods and techniques: surveys, induction to go from the particular to the general, analytical methods, deduction as a form of generalization and inference, and literature analysis.
The article demonstrates the necessity of conducting and developing research on the identification, analysis, and presentation of mechanisms for managing cyber security of business entities. The article is of a practical nature and may constitute a good basis for further discussion of the subject matter.

CYBER SECURITY AS SECURITY IN THE DIGITAL AGE

The groundbreaking nature of transformations eliminating one order by another is triggered primarily by the digital transformation. This is because treating knowledge - the most precious commodity at humanity's disposal - as something available to everyone without any restrictions is a concept incompatible with the capitalist view of the world. Indeed, the mass digitization of information, and thus of human knowledge, does not merely facilitate access to information, but changes information itself, and above all the dynamics of increasing its quantity and the scope of use by collective subjects of information and communication techniques. Information, treated for centuries on a par with material goods, gradually becoming the most valuable commodity, may soon cease to be treated at all as something that can be bought and sold (Mączyńska, Okoń-Horodyńska, 2020, p. 12).
An important element of the development of information technology is ensuring security in cyberspace. Protection of data and information is vital for every network user (individuals, organizations, enterprises). The loss, destruction, theft, and leakage of data, including personal data and company secrets, can expose any network user to great moral damage, may damage the reputation, make the operation of the organization impossible, and generate huge financial costs (Kiełtyka, Smoląg, 2021, p. 12).
Progressive digitization has transformed the economy. Space and time have lost their absolute paradigm, and accessing information and processing data has become easier than ever before. It is not without reason that there is talk of the digital revolution rewriting culture, economics and, above all, consciousness. The world is no longer the way it was fifty years ago - business conditions can hardly be compared even to those of the late 20th century. Digitalization has drastically transformed every area of life, bringing about an irreversible convergence of the virtual and real world. The Internet of Things is emerging, which is a network of objects, processes, and people constantly connected to the Internet. Hyper-communication is occurring. Devices are continuously processing huge amounts of information, and some services are done in the computing cloud. Automation and robotization are becoming the norm. We have become accustomed to multichannel and omni-channel distribution of products. Twenty-four hours a day, consumers enjoy digital access to goods and services (Laszczak, 2019, p. 135).

Threats to both a specific business entity's interest and the stability of the state affect an organizational entity's security sphere. These threats are posed not only by criminals, but also - directly or indirectly - by foreign governments, and can take all the previously indicated forms of cyber threats, including those related to cyber-intelligence or cyber-terrorism (Banasiński, 2018, p. 305).

An analysis of the literature on the subject indicates a broad aspect of the problems that are associated with the digital age and, in particular, cyber security, which is an important issue for any business entity operating in the global market that is heavily dependent on information technology and is present on the Internet (Stoneburner, Goguen, 2022, p. 800–830; Bell, 2017, p. 536–539; Melaku, 2023; Raimundo Rosário, 2022; Kumar, Mallipeddi, 2022).

Every year, cyber attacks resulting from the implementation of new service delivery models generate increasing losses for the public and private sectors. Cost estimates include, among other things, loss of sensitive data and intellectual property, costs of service disruptions, and costs of lost operational benefits, including damage to an organization's image and reputation (elsa.org.pl, 2020).

Computerization and digitization bring new opportunities related to improving business efficiency and increasing competitiveness, but also make cyber security an increasingly central concern of organizational management.

Cyber security at a basic level can be understood as confidentiality, integrity, and availability (Figure 1).

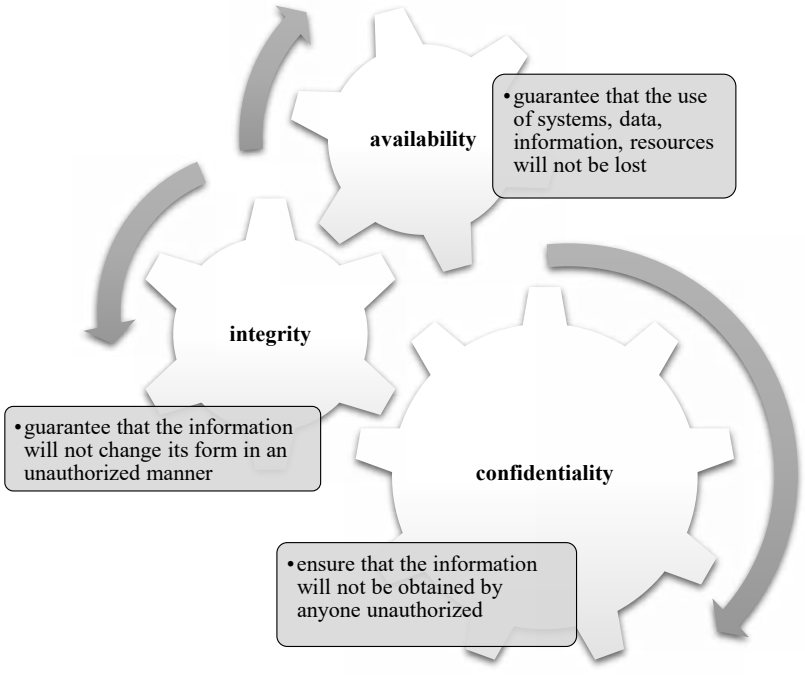


Figure 1. Cyber security basic level
Source: Own description based on Olejnik, Kurasiński (2022, p. 25).

Cyber security in the business area, for a business entity, refers specifically to:

- securing the organization's data, systems critical to the company's finances;
- operational issues in particular to the availability of systems or running backup systems;
- reliability and resilience, security and confidentiality of data;
- minimizing the risk of data leaks;
- continuity of company operations.

A key issue when considering cyber security is risk, such as the risk of losing business continuity, the risk of data leakage, or more generally, the occurrence of certain unwanted events. Risk is a phenomenon that is related to the probability of a certain event occurring that has consequences (Olejnik, Kurasiński, 2022, p. 30).

Cyber security is defined as the activity or process, ability, or capability whereby information and communication systems and the information contained therein are protected against damage, unauthorized use or modification, and exploitation. A cyber security breach is an event that compromises the confidentiality, integrity, or availability of an information system or security

policies or procedures. Phishing, denial of service, zero-day-exploits, ransomware, and unauthorized access to information systems are a few examples. Each of these breach types has potential economic and reputational consequences for the affected firm. Depending on the type of breach, economic costs might include those for detection, regulatory notification, customer redressal and compensation, litigation, loss of market value or investments, regulatory fines, extortion payments, and cost of lost business (Shaikh, Siponen, 2023, p. 2).

CYBER SECURITY IN ENTERPRISES IN THE LIGHT OF SURVEYS

This article presents a fragment of research conducted from 2020 to 2022 on 250 enterprises operating in Poland. The aim of the research was to analyze the architecture of cybersecurity in enterprises. The survey investigated cybersecurity in four thematic areas: cybersecurity (in general), financial outlays on cybersecurity, in the scope of the General Data Protection Regulation, and the impact of COVID-19 on cybersecurity.
The author conducted a survey study through telephone interviews with cyber security professionals on behalf of the Research Institute IPC Ltd., based in Wroclaw. The survey included yes-no questions and multiple-choice questions.
This article presents research on cybersecurity in general conducted among 100 enterprises operating in the Republic of Poland (Figure 2). The largest survey sample consisted of manufacturing (34%) and service (22%) enterprises.

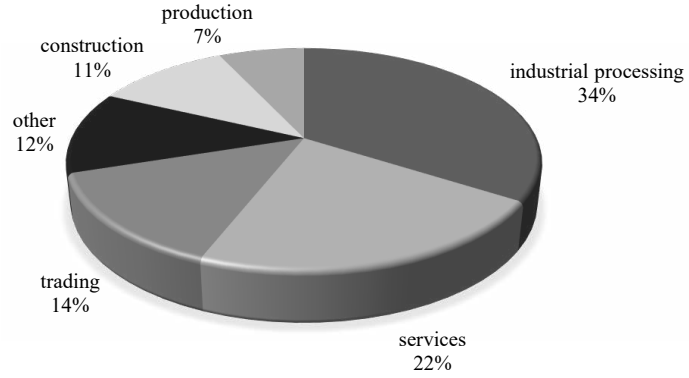


Figure 2. Industries of the surveyed companies
Source: own elaboration based on survey research.

When characterizing the surveyed companies by shareholding, 76% were held by domestic private investors, 11% by foreign investors, and 13% by the State Treasury. 50% of the surveyed companies possessed total assets valued less than or equal to EUR 2 million, 39% possessed assets valued between EUR 2 million andEUR 10 million, and 11% possessed assets valued between EUR 10 million and EUR 43 million. 31% of the companies had more than 250 employees, 21% had between 250 and 50 employees, 27% had between 50 and 10 employees, and 21% had fewer than 10 employees.
Figures 3 –15 illustrate the respondents' answers to the issues of setting up a cyber security system in a business unit.

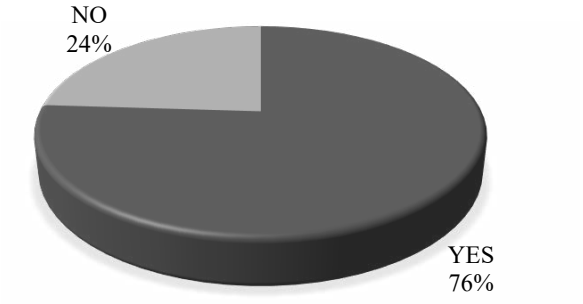


Figure 3. "Do you have a cyber security policy?"
Source: own elaboration based on survey research.

81% of the surveyed companies build common knowledge about cyber security threats and ways to prevent them. 76% of the surveyed companies have a cyber security policy that all employees can use.

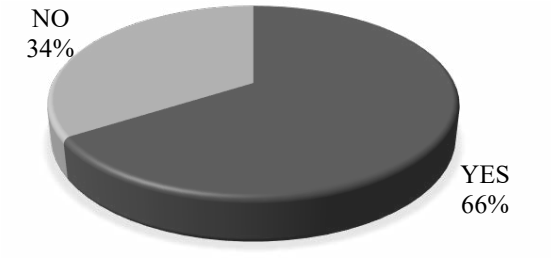


Figure 4. "Do you provide cyber security training?"
Source: own elaboration based on survey research.

Cyber security training is provided at 66% of surveyed companies. In 85% of the affirmative companies, the training is conducted by an external company.

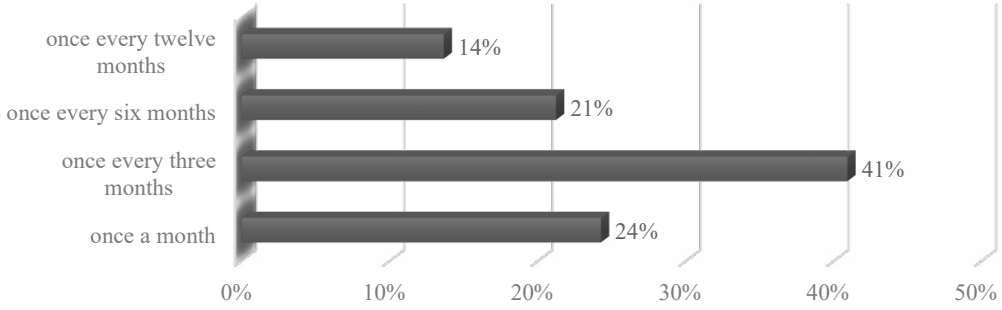


Figure 5. Cyber security training frequency
Source: own elaboration based on survey research.

Among the companies where cyber security training is conducted, in 41% the training takes place once a quarter, in 24% once a month, in 21% once every six months, and in 14% once a year.

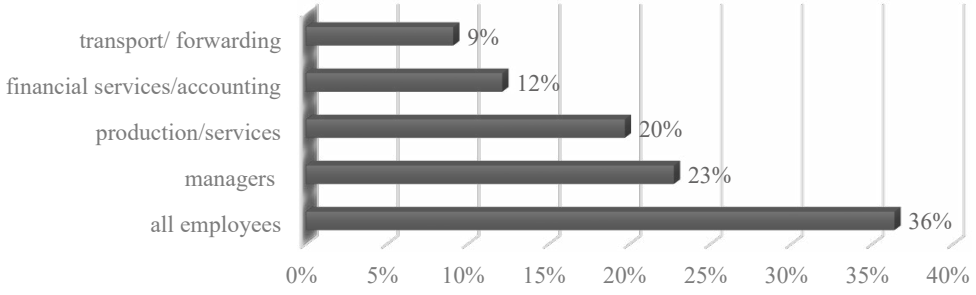


Figure 6. Employees trained in cyber security
Source: own elaboration based on survey research.

Among the companies that conduct cyber security training, 36% train all employees. Managers and production and service employees are trained at a similar rates in the surveyed companies (23% and 20%, respectively). Employees in financial and accounting departments are trained in 12% of the surveyed companies, which may be surprising, especially in recent years, when cyberattacks on financial services have intensified. Transportation and shipping employees are trained at 9% of surveyed companies.

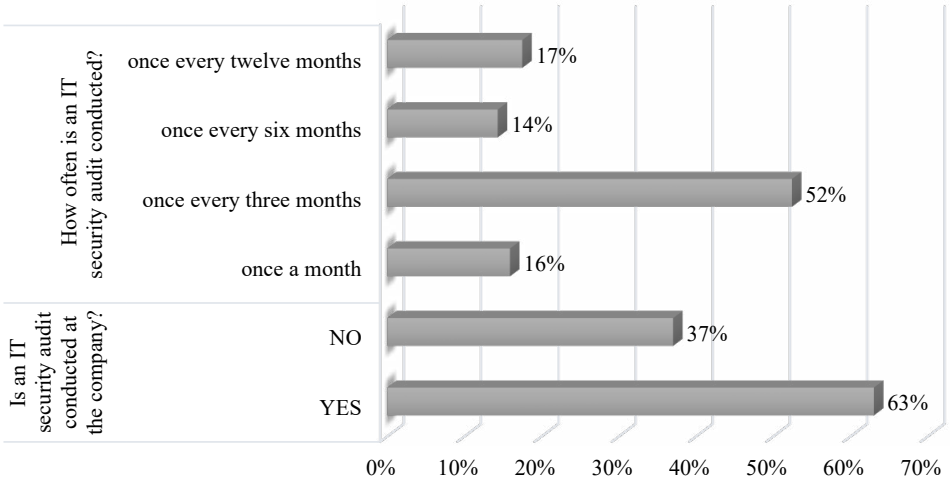


Figure 7. IT security audit
Source: own elaboration based on survey research.

IT security audits are conducted at 63% of the surveyed companies. Among these companies,52% perform it once a quarter, 17% once a year,16% once a month, and 14% once every six months.

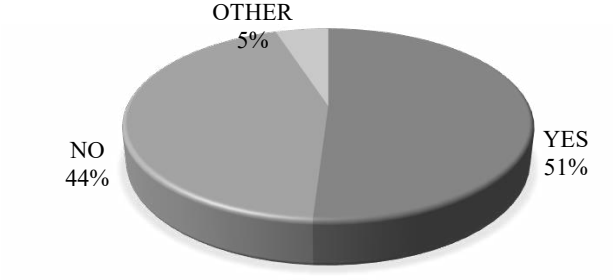


Figure 8. "Do you have a cyber security department?"
Source: own elaboration based on survey research.

51% of the companies surveyed had a separate unit for cyber security, while 44% of the companies did not. Three respondents indicated that they use external companies and two reported that they cede cyber security tasks to the IT department. In 41% of the affirmative companies the cyber security department is a separate and independent organizational unit, in 36% it is dispersed in different business units, and in 23% there is a mixed model. 61% of cyber security departments have 10 or fewer employees, 14% have between 10 and 20 employees, and 20% have more than 30 employees.

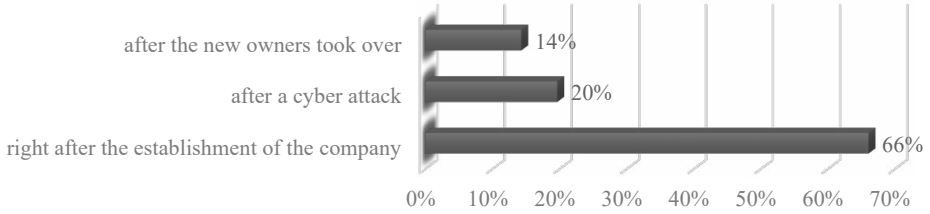


Figure 9. The timing of the creation of the cyber security department
Source: own elaboration based on survey research.

Among companies with a cyber security cell, 66% of departments were established at the time of the company's inception while 20% were created due to a cyber attack and to ensure security.

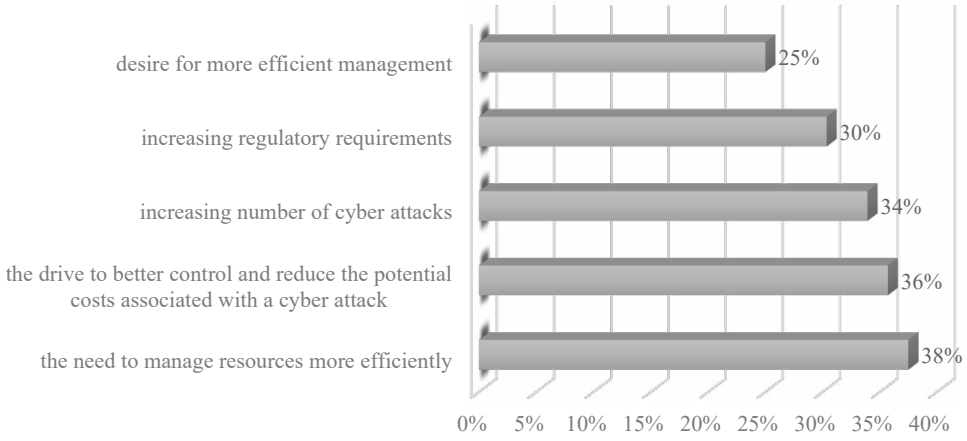


Figure 10. The purpose of creating a cyber security department
Source: own elaboration based on survey research.

38% of companies established a cyber security department to manage resources more efficiently, 36% did so to better control and reduce potential costs associated with a cyber attack, 34% did so to counter the increasing number of cyber attacks, 30% did so to fulfil legal requirements, and 25% did so out of the desire to manage more efficiently.

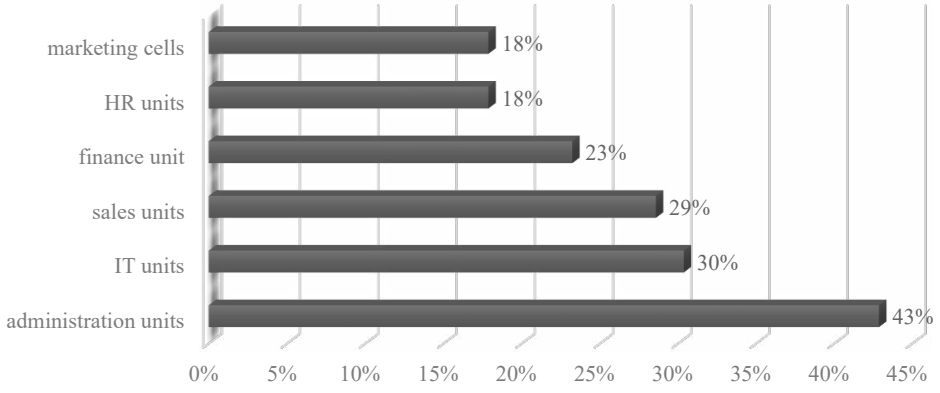


Figure 11. Major partners of the cyber security department
Source: own elaboration based on survey research.

The main partners of the cybersecurity department are the administration unit (43%), then the IT unit (30%), the sales unit (29%), the finance unit (23%), the HR unit (18%), and the marketing unit (18%).

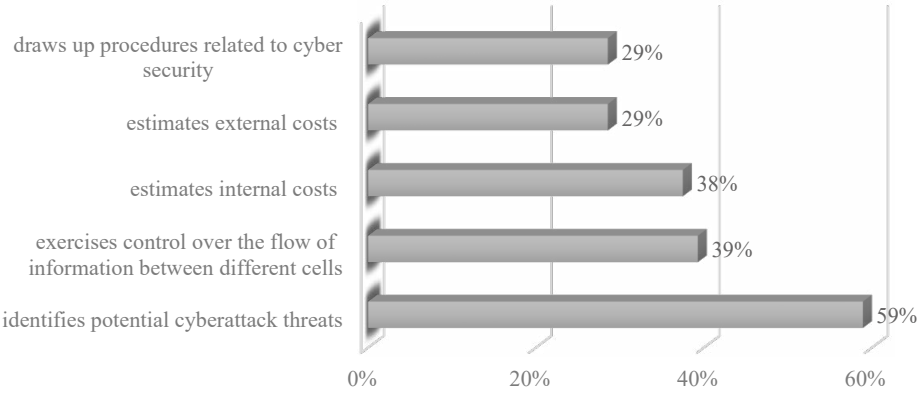


Figure 12. Tasks performed by the cyber security department
Source: own elaboration based on survey research.

The main tasks of the cyber security department that respondents indicated include:

- at 59%, identifying potential cyberattack threats;
- at 39%, exercising control over the flow of information between the various units;
- at 38%, estimating internal costs;
- at 29%, drafting cyber security procedures;
- and at 29%, estimating external costs.

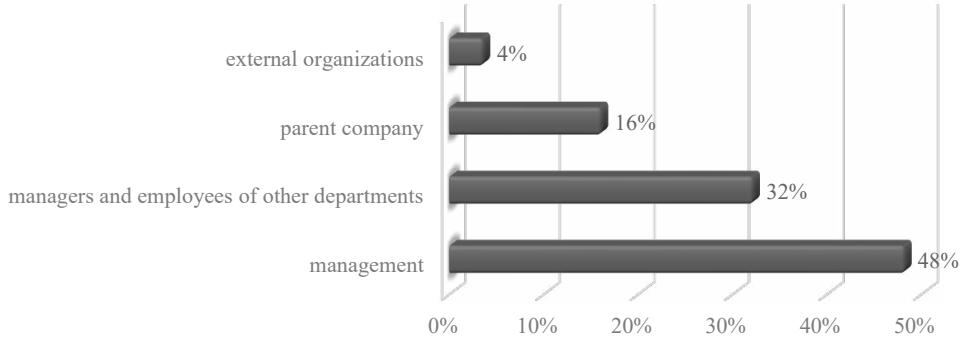


Figure 13. Recipients of reports produced by the cyber security department
Source: own elaboration based on survey research.

The main recipient of reports produced by the cyber security department is the management board at 48%, followed by managers and employees of other departments (32%).

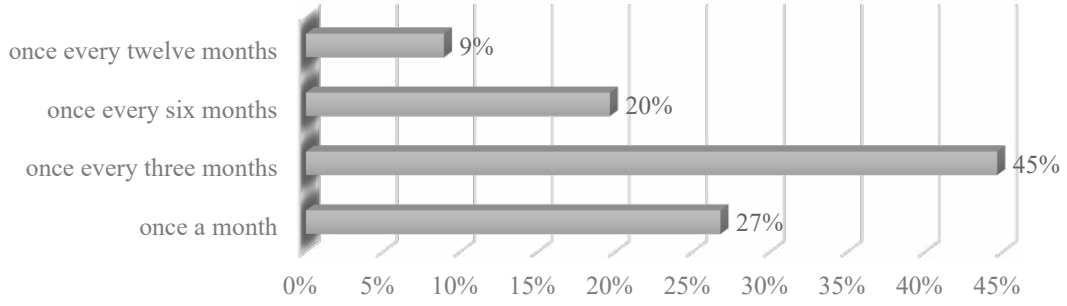


Figure 14. Frequency of reports produced by the cyber security department
Source: own elaboration based on survey research.

In 45% of companies, the cybersecurity department reports quarterly. In 79%, the cybersecurity department creates reports in electronic form, and in 21%, in paper form.

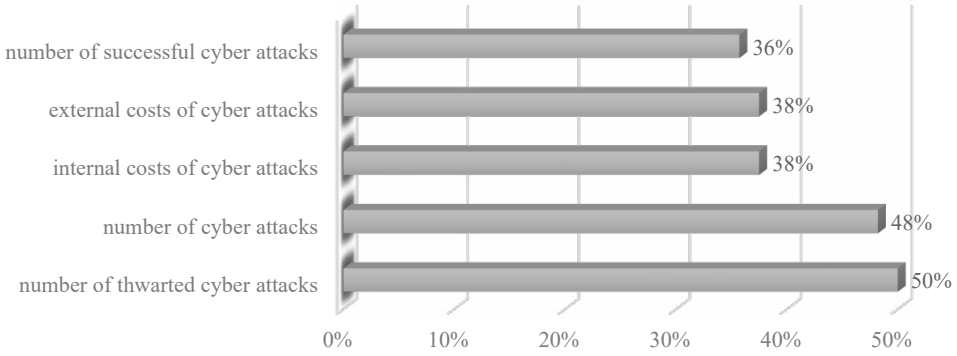


Figure 15. The content of the reports produced by the cyber security department
Source: own elaboration based on survey research.

In companies where the cyber security department produces reports, they include:

- at 50%, the number of cyber attacks thwarted;
- at 48%, the number of cyber attacks;
- at 38%, each of the internal costs of cyber attacks;
- at 38%, the external costs of cyber attacks;
- and at 36%, the number of successful cyber attacks.

6% of surveyed companies said they had been the target of a cyber attack. The main reasons were hacking, failure, and leakage. As for the recency of the attack, two respondents answered that it had occurred within the past three months, two that it had occurred within the past six months, and the rest answered that it was within the last 3 to five years.

The material collected in the course of the research and the conducted analysis show that the determinants of enterprise management in the context of their operation in cyberspace include:

1. Building a culture of security in cyberspace.
2. Creation and implementation of cybersecurity policy.
3. Defining the resources that should be protected.
4. Defining threats related to data storage and their processing, risk assessment, and at the same time identifying opportunities.
5. Simulate a cyberattack to identify bottlenecks.
6. Defining procedures to restore the efficiency and functionality of systems after a hacker attack.

CONCLUSIONS

The changing digital environment in which business entities operate, with its associated facilitations and threats, is forcing management to make decisions on strengthening activities in the area of information security. The basis for ensuring cyber security in the operation of the company is the implementation of appropriate safeguards, policies, and procedures defining how to act in the event of a cyber attack and how to improve employee awareness of existing threats (Antczak, 2020, p. 126). The dynamic development of the digital era in particular, by accelerating the exchange of information and changing the form of document circulation, affects the management of the business unit, which increasingly faces a great test of its competence in conducting business in cyberspace. Cyber security of a business entity has a decisive impact on company management in the digital age.

A survey of companies shows that there is a common understanding of cyber- security threats and how to prevent them. 81% of surveyed companies have a cyber security policy used by all employees. Cyber security training is provided at 66% of the surveyed companies. 60% of the surveyed companies declared that there is an ISO/IEC 27001 standard implemented. The implementation of the ISO/27000 family of standards, together with the standards integrated with them, makes it possible to account for both the various requirements and the expectations of stakeholders in a coherent information security management system, including cyber security. The requirements of the ISO standards are general in nature and are intended to be applied

to all entities regardless of type, size, or nature of the organizational unit. The main reason for implementing a system based on the PN-ISO/IEC 27001 standard in an organization is to ensure the highest possible level of information security.
Research indicates that there is a need to define, examine, analyze, and present cybersecurity management mechanisms in business entities. This position is primarily due to the spread of knowledge on this subject, in particular during the period of increased incidents in cyberspace. Cyber risk poses a significant threat to the continuity, reputation, and finances of companies in all industries. Employees at all levels should be systematically trained on the risks of a cyberattack. Well-secured systems and security procedures may affect the competitive advantage of an enterprise.
The article is of practical nature and is the basis for a discussion on the identification of determinants of business management related to cyber security challenges.

REFERENCES

Antczak, J. (2021). Zarządzanie przedsiębiorstwem w cyberprzestrzeni. ASzWoj.

Banasiński, C. (Ed.). (2018) *Cyberbezpieczeństwo zarys wykładu*. Wolters Kluwer.

Bell, S. (2017). Cybersecurity is not just a 'big business' issue. *Governance Directions*, 69, 536–539.

Bitkowska, A., Sobolewska, O. (2020). Zarządzanie procesowe z wykorzystaniem wiedzy w polskich przedsiębiorstwach. *Przegląd Organizacji*, 1, 21–29.

Cremer, F., Sheehan, B., Fortmann, M., et al. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance. Issues and Practice*, 47, 698–736.

Cyfert, Sz. (2023). Podejście procesowe w środowisku VUCA. Rola zwinności i dynamicznych zdolności. In B. Ziebicki, A. Wodecka-Hyjek (Eds.), *Doskonalenie organizacji koncepcje, metody, rozwiązania*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie.

Czernek-Marszałek, K., Piotrowski, P. (2022). Cyfryzacja w przedsiębiorstwach turystycznych w warunkach COVID-19. Pozytywne i negatywne konsekwencje. *Przegląd Organizacji*, 4, 3–12.

Dennig, P.J., Lewis, T.G. (2017). Exponential laws of computing growth. *Communications of the ACM,60*(1), 54–65.

Ghelani, D. (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology, 3*(6), 12–19.

Górka, M. *(2017). Technologia informacyjna w obszarze cyberbezpieczeństwa Państwa i społeczeństwa. Systemy Wspomagania w Inżynierii Produkcji, 6*(5), 73–89. https://elsa.org.pl (Access: 20.05.2022).

Kiełtyka, L., Smoląg, K. (Eds.). (2021). *Wybrane uwarunkowania i determinanty rozwoju współczesnych przedsiębiorstw*. TNOiK Dom Organizatora, Toruń.

Kleer, J. (2016). Cywilizacje i ich przesilenia. *Studia Ekonomiczne INE PAN*, (1), 1–4.

Kumar, S., Mallipeddi, R.R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management, 31*(12), 4488–4500.

Laszczak, M. (2019), Zarządzanie bezpieczeństwem w erze cyfrowej. *Bezpieczeństwo. Teoria i Praktyka*, (4), 135–150.

Liu, H., Ning, H., Mu, Q., Zheng, Y., Zeng, J., Yang, L.T., Huang, R., Ma, J. (2019). A Review of the Smart World. *Future Generation Computer Systems, 96*, 678–691.

Mączyńska, E., Okoń-Horodyńska, E. (2020). Przedsiębiorstwo i jego otoczenie w obliczu czwartej rewolucji przemysłowej − wyzwania, szanse i zagrożenia. *Przegląd Organizacji*, Nr (1), 9–21.

Melaku, H.M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks, 11*(6), 101.

Olejnik, Ł., Kurasiński, A. (2022). *Filozofia cyberbezpieczeństwa Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*. PWN.

Raimundo, R.J., Rosário, A.T. (2022). Cybersecurity in the Internet of Things in Industrial Management. *Applied Science, 12*(3), 1598.

Shaikh, F.A., Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to Cybersecurity. *Computers & Security, 124*, 102974.

Stoneburner, G., Goguen, A., Feringa, A. (2002). Risk management guide for information technology systems. *NIST Special Publication*, 800–830.

Zakrzewska-Bielawska, A. (2017). Ambidexterity jako zdolność dynamiczna w odpowiedzi na niepewność otoczenia. *Studia Oeconomica Posnaniensia, 5*(9), 174–190.