SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2023
ORGANIZATION AND MANAGEMENT SERIES NO. 175

SYSTEMIC BUSINESS CONTINUITY MANAGEMENT IN THE PROCESS OF BUILDING THE ORGANIZATION'S RESILIENCE AND IMPROVING ITS SECURITY. EXPERIENCE OF THE ORGANIZATION IN POLAND

Aneta WYSOKIŃSKA-SENKUS[1*], Krystian LECHAŃSKI[2], Jakub MALINOWSKI[3]

[1] War Studies University, Warszawa; a.wysokinska-senkus@akademia.mil.pl, ORCID: 0000-0001-9021-6355
[2] War Studies University, Warszawa; krystianlechanski05@gmail.com, ORCID: 0000-0002-0186-6004
[3] War Studies University, Warszawa; j_malinowski@vp.pl, ORCID: 0000-0001-8610-350X
* Correspondence author

Aim: The article aimed to present the essence of the systemic approach to business continuity management (BCMS - Business Continuity Management System) and to determine the level of maturity of business continuity systems implemented in small and medium-sized enterprises about selected groups of external threats, corresponding to current economic, political and legal conditions.
Project/methodology/approach: The subject of this study is an analysis based on the available resources in the literature and the results of the conducted empirical study.
Findings: As a result of the literature study, it has been proven that organizations are exposed to many threats that affect business continuity to varying degrees. The fundamental element of organizational prevention at the operational level is the business continuity plan, which defines response mechanisms in the event of an incident or crisis that negatively affects the stability of implemented projects. The analysis of the research results indicated that the primary response mechanism established in modern organizations transfers the burden of the effects of the crisis to employees, as it is related to the performance of professional duties using remote communication methods and techniques.
Research limitations/implications: The primary research limitation was the difficulty in obtaining a representative research sample, which is why it was decided to limit the scope of the research and carry it out in enterprises belonging to high-tech industries. Bearing in mind that the scope of the study referred to conditions which, due to the increased uncertainty of the general (intermediate) environment, are subject to changes and improvement of modern management systems, it is recommended to conduct the research again in other economic sectors. Expanding the study's scope will allow the development of a catalogue of good practices, including a more comprehensive catalogue of threats to the continuity of modern business organizations.
Originality/value: The article presents previously untested mechanisms ensuring business continuity about current threats – blackout and energy lockdown. The analyses contained therein may be the basis for improving internal crisis response systems, especially in small and medium-sized enterprises.

Keywords: business continuity plan, operational risk, blackout, crisis, incident.
Paper category: research and review publication.

1. Introduction

In recent years, more and more attention in management has been devoted to business continuity and building organizational resilience. In reality, organizations have to deal with increasingly more significant and complex threats, such as natural disasters, cyberattacks, or pandemics, which result in severe financial and reputational losses. To ensure business continuity and minimize the effects of potential threats, more and more organizations are introducing a systemic approach to business continuity management (BCMS - Business Continuity Management System) and focusing their activities on building organizational resilience.

This article presents Polish organizations' experience in systemic business continuity management and building their resistance to threats. The paper will discuss the concepts and tools used within the BCMS and the methods of implementing the system in organizations in Poland. In addition, the results of research on the level of maturity of the organization in the context of improving the security of the organization will be presented.

In light of the growing number of threats and the growing sensitivity of the organization to potential losses, the topic of business continuity and building the organization's resilience is becoming increasingly important. Therefore, implementing a systemic approach to business continuity management, such as BCMS, becomes a critical element of activities to minimize risk and improve the organization's security.

2. Business continuity plan in the enterprise – theoretical basis

Consistent and uninterrupted implementation of current production and service processes shapes the operational continuity of the organization, the results of which directly affect the form and scope of relations established with the environment. Business continuity can be disrupted as a result of both internal and external factors. Therefore, modern organizations carry out many complementary activities to minimize uncertainty leading to business continuity interruption. The high turbulence of the environment, as well as the increased dynamics of changes observed in the right dimension, is the result of emerging crises of a global nature. It encourages entrepreneurs to build organizational prevention, especially at the organizational structure's lowest operational level.

The Bael Agreement indicates that operational risk should be equated with a loss resulting from insufficient or inadequate internal processes, people, and systems, as well as from events external to the company (Basel Committee on Banking Supervision, 2006). The presented approach, developed by the Basel Committee, emphasizes the importance of the effects of unfavourable phenomena while indicating a broad spectrum of circumstances that may disrupt the course of activities and processes. The unique and often ambiguous nature of threats, especially those whose source is in the organization's environment, implies the need to protect critical processes that ensure the continuity of the organization's operation. Scenarios of incidents and crises are developed in business continuity plans, considering the effects, prospects, and value of resources at the organization's disposal.

Business Continuity Plans (BCP) are sets of tested and documented procedures for operational business continuity management, defining the organization and rules of conduct as part of activities constituting a planned response to an unexpected disruption with a destructive impact causing a crisis in the organization's operations (Gołąb, 2009). The presented approach indicates that the business continuity plan is a fundamental element of securing the enterprise against the effects of business disruptions. It also makes it possible to ensure a minimum level of process operation in the event of one of the attributes of a crisis, which include: the risk of incurring losses threatening the survival of the organization, loss of supervision over the occurring events, significant negative impact on the organization's resources, insufficient time to implement the undertaken actions (or taking a reaction), lack of reliable information (Krzakiewicz, 2008). The presence of some of the listed threats is a natural consequence of changes occurring simultaneously in the organization and its environment. However, the increased dynamics of changes significantly increase the organization's susceptibility to the occurrence of events, the effects of which significantly increase the uncertainty of operation and, consequently, limit its ability to self-regulate. It is worth noting at this point that modern enterprises have advanced, automated decision-making systems that facilitate the development of variants of action concerning threats originating within the organization.

External threats to the continuity of the organization's operations have a much wider spectrum of occurrence and impact, which is why it isn't easy to develop a universal response methodology. The critical criterion for building organizational prevention in this aspect is sensitivity to the time factor[1]. It is assumed that the ability to recognize the sources, scale, and effects of specific external threats increases exponentially, along with the acquisition of new experiences resulting from the organization's completed, current, and planned projects. Of course, some threats are repetitive, thanks to which the entrepreneur can adequately secure resources and means in advance, neutralizing the impact of specific incidents and risks. Most often, however, it is difficult to precisely determine both the time and the level of effects

[1] Every complex organization satisfies the conditions of the ergodic hypothesis, which states that if a system functions for a long enough time, it goes through all possible states, no matter how low the probability of a given state is (Grzesiowski, 2000).

of particular phenomena on the organization, which is why theoretically assumed scenarios of the development of phenomena are created, which in specific circumstances may be a source of the crisis.

Differences in the strength and course of crisis phenomena that have emerged between individual regions of the world, and even countries, lead to the thesis that despite the strong interconnection of economies in the global world, enterprises react differently to similar threats related to the crisis or, more broadly, to the risks resulting from changes in the environment (Romanowska, 2010). The phenomena resulting from the SARS-CoV-2 [2] coronavirus pandemic, which lasted for over three years and spread worldwide, and the armed conflict in Ukraine and Russia, which has been taking place since February 24, 2022, are gaining importance. The indicated conditions significantly contributed to expanding the catalogue of risks that should be included in business continuity plans. Concerning the pandemic, the threats directly impacted the continuity of operation of selected industries, as the legislator imposed a legal ban on the provision of certain services to some organizations (Goldstein, Flynn, 2022). The catalogue of risks has accordingly expanded due to the armed conflict between Russia and Ukraine. Although military operations are local, their effects directly affect the functioning of all industries, even those not involved in the course of the conflict. Russia, as the leading exporter of energy resources, uses political pressure on the countries of Eastern Europe that are militarily weaker and poorer in energy resources (Kułaga-Boczko, 2022). This situation is a source of threats related to the availability of energy resources, which, in the era of the development of modern societies, are the basis for the operation of all types of business organizations. The first of them is a blackout – loss of voltage in the NPS power grid over a large area as a result of a sequence of several random or intentional events, i.e. grid failures, shutdowns of power plants, extreme weather conditions, a terrorist event (NCMP, 2022). The second threat currently identified by government institutions dealing with the security of critical European infrastructure is the energy lockdown. Unlike blackout, this is a phenomenon implemented by state authorities, consisting of partial limitation of the availability of electricity, which is aimed at ensuring the continuity of operation of public benefit organizations and preventing failures of the power grid (Pinto, Fernandes, da Silva, Pereira, 2022).

The COVID-19 pandemic has affected research on business continuity management (BCM) by highlighting the need for BCM programs to adapt to reflect the altered environment (Goldstein, Flynn, 2022). The pandemic has also exposed systemic vulnerabilities at the economic level, highlighting the significance of BCM in protecting the interests of stakeholders (Corrales-Estrada, Gómez-Santos, Bernal-Torres, Rodriguez-López, 2021). In addition, there are few studies analysing the relationship between organizational sustainability capabilities, organizational resilience capabilities, and BCM to comprehend risk management[2].

[2] On March 11, 2020, the World Health Organization announced a state of pandemic, which is still formerly in force.

Future research is required to investigate the impact of the pandemic on BCM programs and to identify new trends and guidelines to consider when developing a BCM plan strategy. Another trend is the exploration of information systems security management topics of BCM, including definitions, terminology, trends, and guidelines common to this requirement born essentially from the IT industry (Charoenthammachoke, Leelawat, Tang, Kodaka, 2020). A preliminary systematic literature review explores the trend of BCM, the subject, and the relationship between BCM and associated study fields[3]. Other trends include the development of a holistic approach to BCM that provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities[4]. Furthermore, there is a notable emphasis on the implementation of proficient business continuity management within insurance firms that utilize contemporary e-commerce technologies (Labus, 2017).

3. System Business Continuity Management

The first works related to the concept of business continuity management appeared in the 1970s. One of the first classics to pioneer in this field was Dr David G. Backhurst, who published a number of articles on business continuity planning in the 1970s and 1980s. Another classic from the area was Dr Russell L. Ackoff, who developed the business continuity planning methodology in the 1970s.

In the 1980s and 1990s, the concept of business continuity management gained popularity, and one of the classics who contributed to its development was Dr Jay E. Heizer, who has published several articles and books on business continuity this decade. The work of Dr Robert L. Shannon should also be mentioned, who in 1992 published the book "Business Continuity Planning: A Step-by-Step Guide with Planning Forms".

Nowadays, there are many authors and scientists dealing with the subject of business continuity management.

Systemic management is an approach to management that focuses on a holistic approach to the organization, its processes, and its resources. Within the systemic approach, an organization is treated as a system composed of interrelated elements that work together to achieve specific goals. Systemic management requires an understanding of both internal and external processes that affect the organization and taking into account their impact on the efficiency and effectiveness of the organization.

The basic assumption of systemic management is that changes introduced in one area of the organization affect other areas. Therefore, it is important to take these dependencies into account in the organization management process and to monitor the impact of the introduced changes on the entire system.

Systemic management assumes the use of tools and methods that enable effective management of the entire system. This approach allows you to identify problems and their causes, and then take remedial action to prevent similar problems from arising in the future. Systemic management also includes continuous improvement of organizational processes, which increases the organization's efficiency and effectiveness.

As a result, systemic management can contribute to improving the quality of the organization's work and its financial results. The challenges related to managing an organization are very big today, and a systemic approach is an answer to many of these challenges.

In today's increasingly complex and dynamic business environments, organizations must ensure business continuity in order to survive and thrive in the market. To this end, many organizations use a systemic approach to business continuity management that aims to ensure optimal operational performance and minimize the risk of failure in the event of incidents or disasters.

The systemic approach to business continuity management assumes that the organization must be ready for incidents or disasters and have the ability to act quickly and effectively to restore normal functioning. The systemic approach to business continuity management includes a number of activities aimed at minimizing risk and increasing the organization's resilience to incidents.

The systemic approach to business continuity management is based on several key features. First, it is an integrated approach in which all organizational functions, processes, and resources are interrelated. Second, the systemic approach to business continuity management is customer-oriented, which means that the organization must be prepared for different situations to ensure business continuity and minimize the impact on customers. Third, the systemic approach to business continuity management is process-oriented, which means that an organization must have a thorough knowledge of its processes to be able to react quickly to incidents.

The issue of business continuity management is extremely important and is the current research of many authors.

According to David Lindstedt and Mark Armour, authors of the "Adaptive Business Continuity: A New Approach", business continuity management is a systematic and holistic process of identifying potential threats to an organization and determining what steps should be taken to minimize the impact of these threats on the organization in the event of their effects. Business continuity management is also the process of ensuring that the organization is able to operate without interruption, even in the event of unpredictable events (Lindstedt, Armour, 2018).

The Business Continuity Institute's (BCI's) Good Practice Guidelines define business continuity management as a "holistic process that identifies threats to an organization and the impacts to business operations that those threats if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand, and value-creating activities".

The definition of business continuity management according to ISO 22301 is a systemic approach to business continuity management that enables an organization to identify potential threats to business continuity, as well as prepare for and respond to such situations, enabling the organization to restore its critical business functions within a fixed time after a disruption or failure.

According to Herbane, B. (2010). BCM (business continuity management) is a holistic management process that identifies potential threats to an organization and the impacts on business operations that those threats if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.

Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Appoint that business continuity as a company's socio-technical ability to withstand and restore from intra- and extra-organizational contingencies. Business continuity management (BCM) refers to identifying potential threats to an organization and creating a framework for responding to them to ensure the continued operation of critical business functions. The article proposes an extension of existing BCM approaches for organizations to become more holistic and strategic in their planning.

Kawano, T., & Li, Y. (2017) refer that BCM stands for Business Continuity Management. It is a process that aims to identify potential risks and threats to an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities. The paper also discusses how Smart BCM (SBCM) can be used to integrate information and communication technology (ICT), new energies, and other advanced technologies into BCM in order to improve functionality, optimize operation, minimize damage in case of emergency, and shorten restoration time.

The ISO 22301 standard is an international standard for business continuity management in organizations. The ISO 22300 family of standards also includes other standards related to business continuity management that complement ISO 22301. Here are some of them:

- ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements.
- ISO 22300:2018 – Terminology and basics of the business continuity management system.
- ISO 22313:2020 – Practical guidelines for business continuity.
- ISO 22316:2017 – Anticipation and assessment of threats.
- ISO/IEC 27031:2011 – Business continuity management in information technology.
- ISO/PAS 22399:2007 – Guidelines for business continuity management.
- ISO/TS 22317:2015 – Guidelines for assessing the impact on business continuity.
- ISO/TS 22318:2015 – Business continuity management – mass incident management.

Among the Standards in the field of business continuity management in the organization, the following can also be indicated:

- BS 25999-2:2007 – Business continuity management – Specification.
- NFPA 1600:2019 – Standard for business continuity, crisis and emergency management.
- ISO/IEC 27031:2011 – Business continuity management in information technology.
- ISO/IEC 24762:2008 – Business continuity management in information technology – practical principles and guidelines.
- ISO/IEC 20000-1:2018 – IT service management systems – Requirements.
- ISO 28000:2007 – Supply chain security management – management system specification.
- ANSI/ASIS SPC.1-2009 – Risk and business continuity management – A systemic approach to the threat assessment model.
- ISO 31000:2018 – Risk management – Requirements.
- BS ISO 45001:2018 – Occupational health and safety management – Management system requirements.

Ensuring the continuity of an organization's operations, its resilience to all types of disruptions, and ensuring safety at the macro and microeconomic levels constitutes a source of competitive advantage. The ISO 22301 Security and Resilience - Business continuity management systems - Requirements standard outlines the benefits of implementing a business continuity management system and defines them in four perspectives: business, financial, stakeholders, and internal processes. The following benefits were listed under the financial perspective: supporting strategic objectives, contributing to competitive advantage, protecting and enhancing the organization's reputation and credibility, and increasing organizational resilience. Two benefits were identified from the financial perspective, including reducing exposure to legal and economic consequences and reducing direct and indirect costs of disruptions. From the stakeholders' view, the following benefits can be identified: protecting life, property, and the environment, identifying the expectations of interested parties and analyzing them, and ensuring confidence in the organization's ability to achieve success. The final perspective is the internal processes perspective. Under this criterion, the following benefits can be identified: increasing the organization's ability to maintain effectiveness during disruptions, demonstrating effective and efficient proactive risk monitoring, and eliminating weaknesses in operational activities (ISO 22301:2019).

4. The area and scope of business continuity plans in small and medium-sized enterprises – analysis of research results

In the literature on the subject, little content is devoted to the characteristics and description of systems ensuring business continuity in modern organizations. Therefore, to learn and present the mechanisms shaping business continuity systems established in business organizations, an empirical study was conducted, allowing for a more precise reference to the indicated issue.

The study's main subject was identifying mechanisms ensuring business continuity in small and medium-sized organizations belonging to high-tech industries. All organizations surveyed focus their activities on research and development in the field of technical sciences. The research problem was formulated in the form of a question: which areas, in the light of current economic conditions, pose the greatest challenge in the process of ensuring business continuity in enterprises operating in the field of high-tech technologies? The research was carried out using the diagnostic survey method, a survey technique, carried out with the use of an original research tool – a questionnaire. Bearing in mind the difficulty in recognizing the significance of the indicated threats by the respondents, resulting from the narrowed research area as well as the unusual nomenclature of threats, the definitions of "blackout" and "energy lockdown" were included in the questionnaire.

The survey was conducted in January and February 2022 among 43 people holding managerial or coordinating functions, representing 9 small and 5 medium-sized enterprises, respectively, operating in the Mazovia voivodeship. The respondents included 15 women (35%) and 28 men (65%). The respondents represented three age groups, respectively, in the range from 26 to 35 years (40%), in the range from 36 to 45 years (47%), and in the range from 46 to 55 years (13%).

The first part of the study focused on defining the scope of the business continuity assurance system in relations to threats originating in the environment of the surveyed enterprises. Fig. 1 presents a summary of respondents' opinions relating to the identified external threats to the organization.

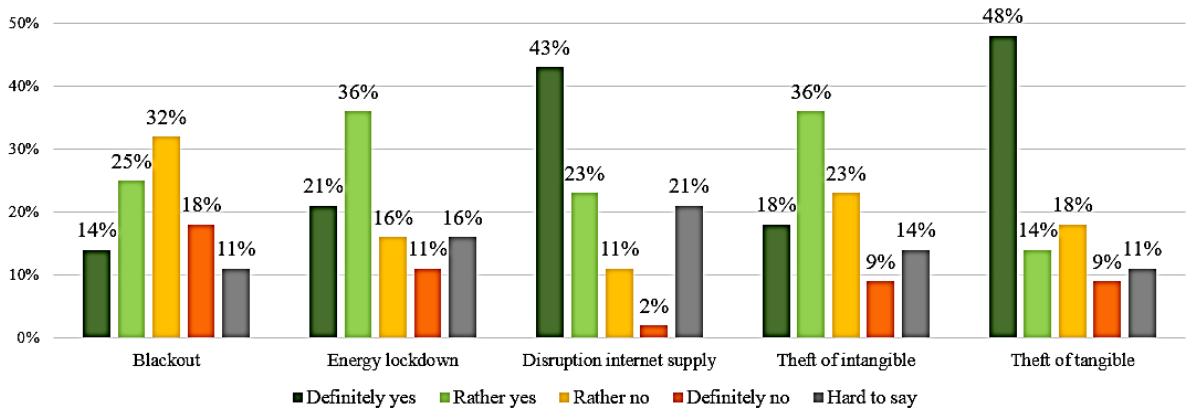

Figure 1. External threats articulated in business continuity plans indicated by respondents.
Source: own study.

Indications of the respondents illustrated in Fig. 1, clearly indicate that in modern organizations, in particular, areas are identified that affect the continuity of operations and shape the security of the organization in the objective dimension. This approach has its organizational justification, as it allows the entrepreneur to formulate general procedures for reacting in the event of an incident. However, it is insufficient when the risk materializes and the area of its occurrence is focused within a single key process responsible for ensuring the continuity of the organization's operation. It should be emphasized here that the respondents' indications do not take into account the links between individual threats. The occurrence of a blackout as well as an energy lockdown partially or completely limits the availability of the Internet and some intangible resources that can be used by means of automated electronic or computer systems. The indicated ambiguity may result from ignorance or non-occurrence of such events in the organization itself and in its environment. Nevertheless, shaping the safety culture in the company requires the creation of new attitudes and values with the participation of all members of the group. The aim of these activities is to persuade employees to eliminate excessive risks in the workplace (Krupa, 2017). Therefore, it is extremely important to systematically monitor the risk horizon and involve employees in the risk identification process.

The second element that was the subject of the study was the impact of identified threats on ensuring business continuity. Fig. 2 illustrates the opinions of respondents, outlining the degree of impact of specific threats on the interruption of business continuity.

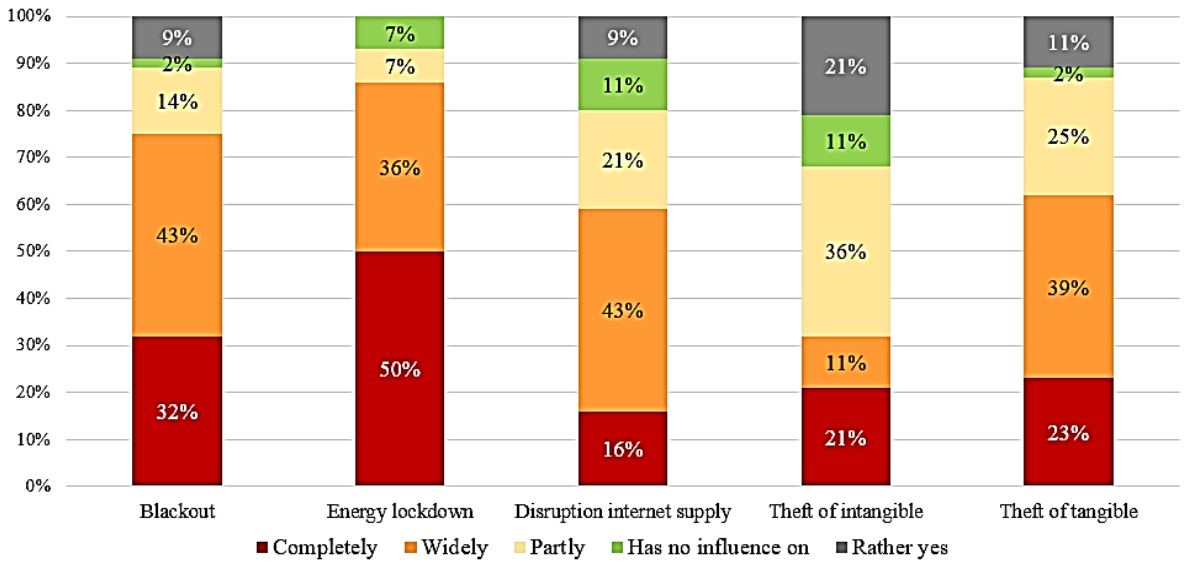

Figure 2. Opinion of respondents regarding the level of impact of specific threats on the ability to ensure business continuity.

Source: own study.

Research results presented in Fig. 2 reveal a kind of contradiction in the approach of the surveyed organizations to business continuity management. In the first part of the survey, 39% of respondents indicated that they listed blackout as a threat in their business continuity plans. In the second part of the study, as many as 75% of respondents indicated that blackout contributes to interrupting business continuity. The indicated difference shows irrefutably that entrepreneurs similarly use identical or mismatched mechanisms both to identify operational risk and during business continuity management. Within the framework of the risk management concept, the effects are analysed statically, while within the framework of business continuity in dynamic terms. This means that the effects are analysed over time along with the change in the severity of the threat or the duration of the crisis situation (Zapłata, 2012). At the same time, as many as 86% of respondents indicated that the energy lockdown affects the interruption of business continuity, and only 32% of respondents indicated that the theft of intangible resources affects the interruption of business continuity. Referring to the indicated differences in the approach to business continuity management, it should be emphasized that the unquestionable basis for the efficient and uninterrupted functioning of an organization is the implementation of (Zawiła–Niedźwiecki, Gołąb, 2010):

- solutions, preventing the emergence and development of continuity threats,
- mechanisms, for removing the effects of disruptions as quickly as possible,
- systems, enabling continuation of operations in critical conditions.

The aim of the third part of the study was to determine the response mechanisms indicated in the business continuity plans in the event of specific threats. Fig. 3 presents the indications of the respondents, shaping the context and scope of actions in the event of an incident leading to the interruption of business continuity.

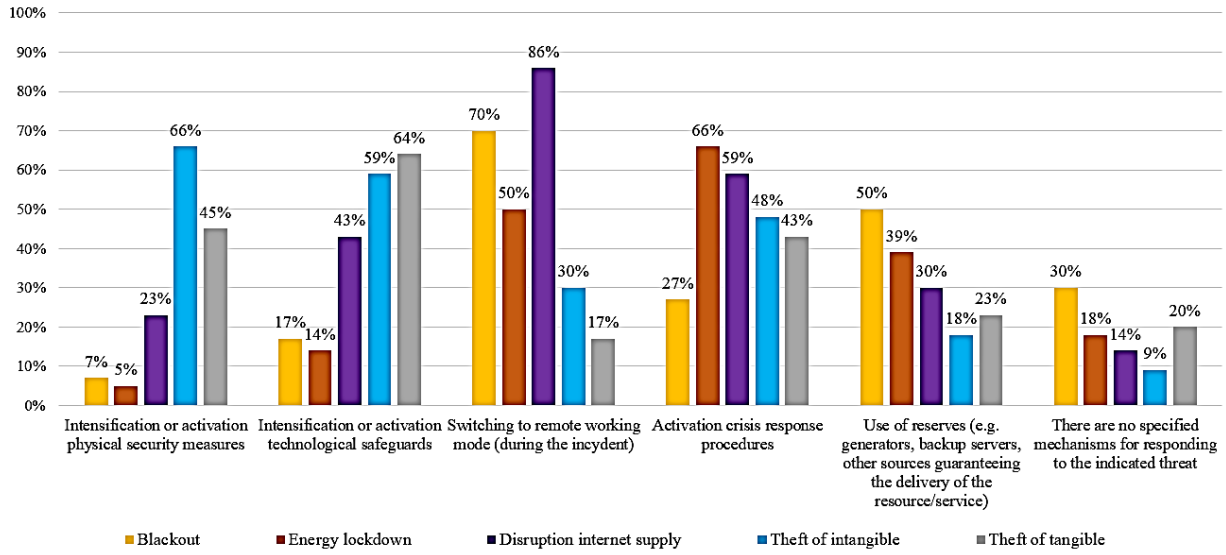

Figure 3. Response mechanisms articulated in business continuity plans and response systems in contemporary organization.

Source: own study.

Percentage of respondents' opinions illustrated in Fig. 3, indicates that the most frequently indicated mechanism, established in business continuity plans, is the change of the working mode, ensuring the possibility of performing part or all of the work remotely. The instrument was adequately indicated most often in relation to the interruption of Internet supplies – 86% of responses, as well as in the event of a blackout – i.e. 70% of responses. However, it should be emphasized here that changing the form of performing current tasks is possible to a limited extent and does not contribute directly to eliminating the source of the threat. Therefore, an important aspect that constructs the methodology of the organization's operation in a crisis is to indicate several complementary response mechanisms (Zawiła-Niedźwiecki, Gołąb, 2010). Another, most frequently presented instrument, allowing for active resolution of disruptions, was the launch of crisis response procedures. This mechanism was most often indicated in relation to the energy lockdown and the interruption of Internet supplies. The literature on the subject indicates that detailed crisis response procedures in organizations that take into account many scenarios of the development of threats allow you to accurately and purposefully identify the methods, ways and resources necessary to restore the efficiency of the organization to the level before the occurrence of the incident. The authors of the study pay special attention to the percentage of 30% of respondents who indicates that the business continuity plans established in their organizations did not specify mechanisms for responding to the occurrence of a blackout.

Failure to isolate response mechanisms in the fact of threats whose occurrence is highly probable indicates the immaturity of business continuity assurance systems. The catalogue of risks, threats and weaknesses of the organization that affect or potentially affect the interruption of the ongoing processes should be constantly monitored and supplemented. Especially in a situation of increased uncertainty resulting from dynamic changes in the environment.

The lack of an adequate reaction to changes is most often associated with the materialization of losses both in the financial and image perspective, because the effects of interrupting the continuity of the company's operations are directly observed at the level of relationship management.

5. Summary

In the article, the authors focused on presenting the experience of organizations in Poland in the field of business continuity management. The authors point to the importance of a systemic approach to business continuity management, which allows to increase the organization's resistance to various types of threats and crises.

The article presents issues related to the definition and objectives of business continuity management, as well as various approaches and methods used in the business continuity management process. Then, the experiences and practices of organizations in Poland in the field of business continuity management were discussed, including examples of actions taken to increase the organization's resistance to various types of threats.

The authors emphasize the importance of effective business continuity management for improving the organization's security and for increasing its competitiveness on the market. They also indicate the need for continuous improvement of business continuity management processes and the need to take into account the changing market conditions and business environment.

In conclusion, the article shows how important it is to effectively manage business continuity in organizations, and what benefits such an approach can bring. The experiences of organizations in Poland presented in the article are a valuable source of knowledge for other enterprises that want to take action to increase their resistance to various types of threats.

References

1. Basel Committee on Banking Supervision. (2006). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*, BIS. https://www.bis.org/publ/bcbs18.htm, 5.02.2023.
2. Burtles J. (2014). *Crisis Management: A Guide to Incident Management, Continuity Management't and Disaster Recovery*. Rothstein Publishing.

3. Charoenthammachoke, K., Leelawat, N., Tang, J., Kodaka, A. (2020). Business continuity management: A preliminary systematic literature review based on ScienceDirect database. *Journal of Disaster Research, 15(5),* 546-555.
4. Corrales-Estrada, A.M., Gómez-Santos, L.L., Bernal-Torres, C.A., Rodriguez-López, J.E. (2021). Sustainability and resilience organizational capabilities to enhance business continuity management: A literature review. *Sustainability, 13(15),* 8196.
5. Drescher D. (2018). *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Apress.
6. Gołąb, P. (2009). *Zarządzanie ryzykiem ciągłości działania w firmach ubezpieczeniowych*. Warszawa: Polska Izba Ubezpieczeń.
7. Goldstein, M., Flynn, S. (2022). Business continuity management lessons learned from COVID-19. *Journal of Business Continuity & Emergency Planning, 15(4),* 360-380.
8. Grzesiowski, M. (2000). Zarządzanie przez kryzysy. In: K. Perechuda, K. (ed.), *Zarzadzanie Przedsiębiorstwem Przyszłości* (p. 203). Warszawa: Agencja Wydawnicza PLACET.
9. Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History, 52(6),* 978-1002.
10. Kawano, T., Li, Y. (2017). A Study on Smart Business Continuity Management for Near Future Cities. *Journal of Asian Architecture and Building Engineering, 16(1),* 1-8. doi: 10.3130/jaabe.16.1.
11. Kerzner, H. (2017). *Project Management Metrics, KPIs, and Dashboards: A Guide to Measuring and Monitoring Project Performance*. Wiley.
12. Krupa, W.L. (2017). Zarządzanie ochroną pracy. In: A. Kowerski (ed.), *Meritum bezpieczeństwo i higiena pracy*. Warszawa: Wolters Kluwer.
13. Krzakiewicz, K. (2008). Podstawowe problemy zarządzania antykryzysowego. In: R. Krupski (ed.), *Zarządzanie strategiczne. Podstawowe problemy*. Wałbrzych: WWSZiP.
14. Kułaga-Boczko, A. (2022). Szok cenowy na europejskim rynku gazowym w 2021 roku – dominacja Rosji i wpływ innych zjawisk globalnych. In: A. Daniluk, P. Stawarz, A. Wierzbicki (eds.), *Numer Jubileuszowy Dedykowany Profesorowi Józefowi Tymanowskiemu.* Warszawa.
15. Labus, M. (2017). *E-business Continuity Management in Insurance Sector*. 7th International Conference on Information Society and Technology ICIST 2017. https://www.eventiotic.com/eventiotic/files/Papers/URL/f773e45b-4654-47dc-9e82-040ba4e459c6.pdf, 5.05.2023.
16. Lindstedt, D., Armour, M. (2018). *Adaptive Business Continuity: A New Approach*. Rothstein Publishing.
17. Niemimaa, M., Järveläinen, J., Heikkilä, M., Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. *International Journal of Information Management, 49,* 208-216.

18. Nuczyński, A., Jabłoński, S., Kobryń, A. (2017). *Zarządzanie ciągłością działania w organizacjach*. Warszawa: PWN.
19. Pinto, D., Fernandes, A., da Silva, M.M., Pereira, R. (2022). Maturity models for business continuity–A systematic literature review. *Maturity models for business continuity – A systematic literature review, 1*, 123-136.
20. Romanowska, M. (2010). Przełomy strategiczne w przedsiębiorstwie. *Studia i Prace Kolegium Zarządzania i Finansów, z. 98.* Szkoła Główna Handlowa, pp. 7-15.
21. Rządowe Centrum Bezpieczeństwa (2021). *Krajowy plan zarządzania kryzysowego 2021/2022, część A*. Warszawa, p. 27. https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego, 5.02.2023.
22. Zapłata, S. (2012). Systemowe zarządzanie ciągłością działania BS 25999 w działalności usługowej. *Zeszyty Naukowe Uniwersytetu Szczecińskiego, nr 722.* Szczecin, p. 248.
23. Zawiła-Niedźwiecki, J., Gołąb, P. (2010). Zapewnianie ciągłości działania jako ograniczanie ryzyka operacyjnego. In: P. Gołąb, L. Gąsiorkiewicz, J. Monkiewicz (eds.), *Zarządzanie ryzykiem działalności organizacji*. Warszawa: CH Beck.