European Research Studies Journal
Volume XXIII, Special Issue 3, 2020

pp. 274-286

Business Continuity in Relation to the Security of Organizations Against Threats Arising from the Declaration of a State of Epidemiological Emergency

Submitted 02/08/2020, 1st revision 11/09/2020, 2nd revision 23/10/2020, accepted 12/11/2020

Szymon Mitkow[1], Ewa Dębicka[2]

Abstract:

Purpose: *The purpose of the study is to determine how the development of business continuity plans will affect organizations' security in difficult to foresee crises. The study will be prepared on the example of the on-going pandemic caused by COVID-19.*
Design/Methodology/Approach: *In the research process, theoretical research methods were widely used, i.e., bibliographic query, critical analysis of the subject literature and statistical data, selection, and evaluation of source and empirical materials. Analysis and synthesis, gradual abstraction, comparison, and generalization made it possible to begin the phase of inference in the context of global changes in the economy's functioning and, in particular, organizations comprising that economy.*
Findings: *The research conducted made it possible to identify and describe the consequences of the COVID-19 pandemic and measures taken by organizations in the context of implementing and maintaining business continuity plans.*
Practical Implications: *The research's contribution is to show the general interrelationships between business continuity about the security of organizations against threats arising from the declaration of a state of epidemiological emergency.*
Originality/Value: *The uniqueness of the current situation is so important, interesting, and dynamic that it is worthwhile to pay attention to it and study it thoroughly. The paper constitutes a new contribution to research on crisis prevention, preparedness for action, response to a crisis, recovery of unavoidable consequences, and, most of all, ensuring the continued operation of organizations and improving their security.*

Keywords: *Organization security, continuity of operation, COVID-19.*

JEL codes: *L21, F64, M21.*

Paper type: *Research in Security Studies.*

[1]*Security, Logistics and Management Faculty – Military University of Technology in Warsaw, Poland. e-mail: szymon.mitkow@wat.edu.pl;*
[2]*Motor Transport Institute in Warsaw, Poland, e-mail: ewa.debicka@its.waw.pl*;

1. Introduction

Safety and security are often a subjective feeling that can be felt by anyone in a different way. However, regardless of the way we feel safe or secure, we can consider them in the following five dimensions (Williams, 2012):

- *in the military dimension* - related to the offensive and defensive military force of States and the mutual evaluation of intentions by States;
- *in the political dimension* - related to the institutional stability of States, systems of governance and ideologies that provide them with legitimacy;
- *in the economic dimension* - functioning around access to resources, financial assets and markets, the access necessary to maintain the expected level of prosperity and power of the State;
- *in the social dimension* - focused on the stability and development of traditional language and cultural patterns and religious and national identities and practices;
- *in the environmental dimension* - related to maintaining the local and global dimension of the biosphere as an indispensable base for all human activity.

Nowadays, another health dimension can be added to the above-mentioned dimensions, namely the dimension related to providing health protection as an essential condition of human existence. People's lives and livelihoods are now more in danger from the disease than from war, terrorism, or other conflicts. Investing in health is an investment in national security (Brundtland, 1999). Diseases, in particular such as SARS-CoV-2 and its consequences, have shown how they can shake the economic stability of countries and even the stability of the whole world. The first documented cases of the global COVID-19 pandemic, caused by the SARS-CoV-2 virus, were detected at the end of 2019. The emergence of this new, dangerous disease has brought serious problems to the functioning of many organizations that were not prepared for the restrictions, impositions, and prohibitions implemented. Thus, their security as organizations was exposed to various types of losses. Considering the current pandemic situation and the actions by governments and organizations themselves, the following questions arise:

- *What actions are taken by organisations in the era of SARS-CoV-2 to ensure them to operate?*
- *How does the creation of business continuity plans increase the security of organisations in crisis situations, which are difficult to predict?*

The study is based on the example of data concerning the organization's functioning during the ongoing pandemic caused by COVID-19 in Poland. Besides, an attempt has been made to anticipate future changes and global trends, as the current priorities and away, the organization's security is managed, have changed significantly. The paper consists of 4 points. In point No 2, the theoretical basis for the problem under consideration is presented. Points No 3 and 4 present an analysis of statistical data of research conducted in Poland. Point No 5 provides summaries and conclusions and future orientations of the research.

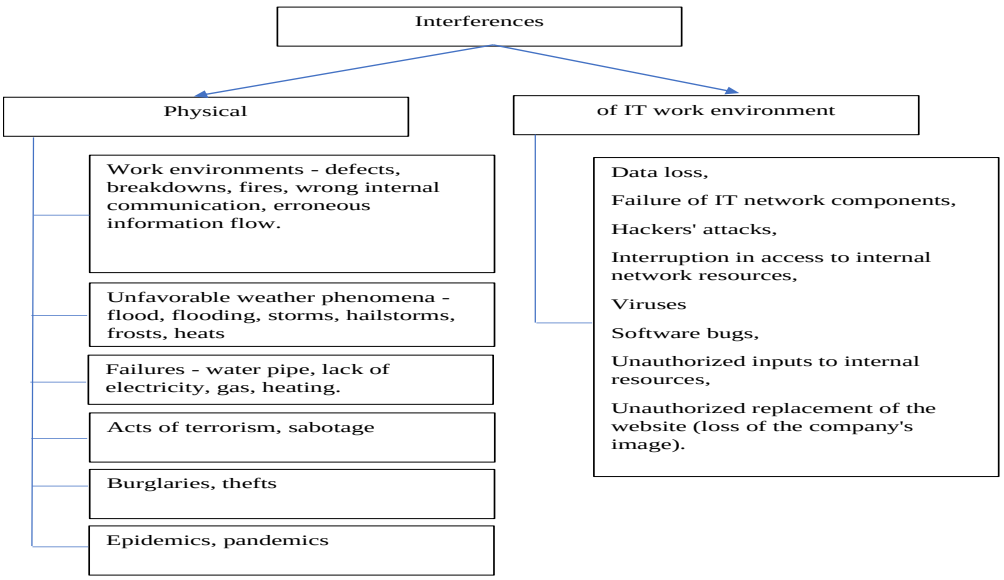
2. Theoretical Background

2.1 Threats to the Functioning of the Organisation

Ensuring safety and maintaining values are fundamental criteria for making strategic decisions in an organization. As a long-term goal of the organization's operation, continuity, and survival have always been the most important elements of effective organization management (Kaczmarek and Ćwiek, 2009).

Each organization is exposed to extraordinary events that may disrupt its functioning. The reason for the uncertainty in achieving the specified objectives is the threats, number, and scale of which affect an organization's safety and security. An organization's goal is to achieve a status of certainty and stability and obtain the minimum level of occurrence of a threat that may affect this status by its influence. The occurrence of threats, emergencies is the opposite of security. Therefore, each organization strives to influence its external environment and internal sphere to remove, neutralize, or dismiss threats and eliminate its own fears, concerns, anxiety, and uncertainty (Sikich, 2003). Each organization should have a list of threats, emergencies that will facilitate its rapid response in the event of a crisis. Figure 1 shows the list of the most frequently identified potential threats, which may more or less affect the continuity of the organization's operations.

Figure 1. *Examples of potential threats that may affect the continuity of the organisation's operations*

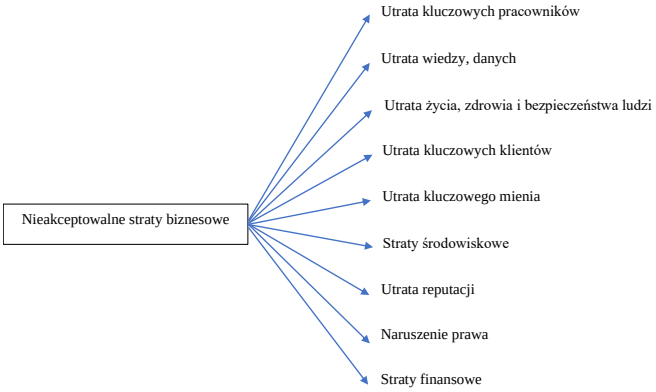


Source: *Own elaboration.*

By identifying the processes and activities whose interruption may have an impact on the functioning of the organization, we obtain a set of unacceptable business losses such as, among others, threats to the life, health, and security of those involved in the processes, loss of key customers, acting in contravention of applicable laws, etc. (Figure 2).

Figure 2. *Types of losses in the organisation as a result of an adverse situation*

Zakłócenia	**Disturbances / Disruptions**
Fizyczne	**Physical**
Środowiska pracy - usterki, wypowiedzenia umów najmu, użytkowania, leasingowe, awarie, pożary, niewłaściwa komunikacja wewnętrzna, błędny przepływ informacji.	Disturbances to the working environment - malfunctions, termination of rental, use, lease agreements, breakdowns, fires, inappropriate internal communication, incorrect information flow.
Niekorzystne zjawiska pogodowe - powódź, podtopienie, wichury, gradobicia, mrozy, upały.	Adverse weather conditions - flooding, flooding, gusts, storms, hailstorms, frosts, heat.
Awarie - wodociągowe, brak prądu, gazu, ogrzewania.	Breakdowns - water supply, lack of electricity, gas and heating.
Akty terroryzmu, sabotażu.	Acts of terrorism, sabotage.
Włamania, kradzieże.	Burglaries, thefts.
Epidemie, pandemie.	Epidemics, pandemics.
Informatycznego środowiska pracy	**Disturbances / Disruptions with the IT work environment**
Utrata danych,	Loss of data,
Awaria komponentów sieci IT,	Failure of IT network components,
Ataki hakerów,	Hacker attacks,
Przerwa w dostępie do zasobów sieci wewnętrznej,	Interruption of access to internal network resources,
Wirusy,	Viruses,
Błędy oprogramowania,	Bugs in software
Nieautoryzowane wejścia do wewnętrznych zasobów,	Unauthorised intrusions into internal resources,
Nieautoryzowana podmiana strony www (utrata wizerunku firmy).	Unauthorised replacement of the website (loss of company image).



Nieakceptowalne straty biznesowe	**Unacceptable business losses**
Utrata kluczowych pracowników	Loss of key personnel
Utrata wiedzy, danych	Loss of knowledge, data
Utrata życia, zdrowia i bezpieczeństwa ludzi	Loss of human life, health and security
Utrata kluczowych klientów	Loss of key customers
Utrata kluczowego mienia	Loss of key assets / property
Straty środowiskowe	Environmental losses
Utrata reputacji	Loss of reputation
Naruszenie prawa	Infringement of the law
Straty finansowe	Financial losses

Source: *Own elaboration.*

A crisis occurs when organizations do not have a ready-made way to deal with a situation that would match the phenomenon's scale. The procedures developed so far can be used in known and repeatable situations, in stable situations where the risk of interference is minimal or absent. Organizations cannot rely on best practices; they have to make decisions and manage information flow in a completely new, untested reality. 26% of the organizations surveyed, when analyzing their own actions and the effects of recently experienced crises, believe they could have done more to identify potential crisis scenarios better to better prepare for them (Deloitte Database, 2020).

The SARS-CoV-2 pandemic has posed new challenges for the whole world. Overnight, many organizations experienced a drop-in revenue, which affected their ability to continue business operations. The actions taken in many countries by governments and the global and European agendas should bring relief, at least for some of them. It should be remembered that there is no proven strategy for the nature of the crisis caused by the SARS-CoV-2, which such a crisis the economy currently is facing. Its global scale means that each organization has to face the challenges it faces and may still face in this difficult time period.

In addition to the already experienced economic and financial problem, one of the key organizational challenges has been to ensure business continuity in the new reality. Organizations were forced to face this by using (or modifying) a previously prepared plan or improvising. According to Deloitte's research, 86% of

organizations believe that they are sufficiently or very well prepared for a crisis, but most of them have not had the opportunity to test this belief.

2.2 Business Continuity Management

*Business Continuity Plans (*BCPs) and (*Business Continuity Management* (BCM) are important elements in the functioning of organisations. BCM is defined as the process, by which an organisation can recover from disturbances caused by e.g. storms and hurricanes, earthquakes, fires, floods, lack of access to media (e.g. electricity, water), acts of terror, epidemics, system failures or disruption of supply chains (Hiles, 2007). Business Continuity Management should include: measures to identify and mitigate risks, treated as an extension of the overall risk assessment process, mitigation of effects of devastating incidents and ensuring that the information required for business processes is readily available (PN-ISO/IEC 17799, 2007). The management process shall include the following stages (Good Practice Guidelines, BCM, 2008):

- understanding the essence of the business (activity),
- defining a Business Continuity Strategy,
- developing organisational solutions: preventive and corrective, developing BCM responses,
- implementation of specific solutions (Business Continuity Plans, audits, adapting the organisation to new operating conditions, etc.),
- building a culture of business continuity.

The management characteristics of BCM are presented in Table 1.

Table 1. *BCM management characteristics*

Description	**Business continuity management**
Main method	BIA – Business Impact Analysis
Key parameters	The size of the effects of the event and the time of its occurrence and duration
Type of event	Events having a significant impact on the organisation's activities
Severity and size of events	Strategy designed to manage events that may affect the disruption of the organisation's business continuity (regardless of severity of an event)
Scope	Focusing mainly on events having a potential or real impact on the functioning of the organisation in all areas of its activity
Strength and mode of impact	Mainly sudden and rapid events

Source: *Own elaboration on based of Good Practice Guidelines (2008 i 2018).*

The Business Continuity Management System applies to all areas of the organization's activities (technical protection, physical security of persons and property, and support for all internal and external auxiliary units in implementing management processes).

Analyzing the environment and the surrounding environment both near and far, the acquisition of information and analyses is essential to maintain the organization's operations' stability. Any disturbances in the external or internal surrounding environment should be identified and analyzed as soon as possible. This is the basis for further actions to create scenarios: to resume or maintain business continuity at a level acceptable by the customer, organization, and parties involved. Such an action applies to all types of activities, but the particular emphasis on stability of the quality of information should be placed where the activity is based on information processing using software specifically written for this purpose. Their task is to support the seamless management of all business processes. Their proper course is crucial and guarantees time and cost optimization.

An example of such support in the effective and efficient implementation of processes is the software applications used in logistics organizations with large vehicles, large storage areas, and international customers. The key task here is to organize the transport process to optimize the order of loading, the customers visited and eliminating or minimizing unloaded trips on the return route or to the customer.

Despite the implementation and maintenance of systems supporting the smooth implementation of processes, and thus the provision of services, it happens that processes supported by high-class computer software applications are exposed to independent factors, causing a real threat to their implementation and often disrupting or even causing the interruption of their business activities. To minimize or even eliminate the effects of a materialized threat and the occurrence of a factor partially or completely disrupting the organization's functioning, Business Continuity Plans (BCPs) are being implemented in organizations.

According to ISO 22301 - Business Continuity Plans are documented procedures that guide an organization to respond appropriately, reproduce, resume, and restore business operations to a predetermined level after a disturbance has occurred. Typically, this plan covers the resources, services, and activities required to ensure the continuity of critical business functions (PN-EN ISO 22301, 2014).

Business Continuity Plans (BCPs) should be designed to limit their impact, loss of information in undesirable situations, and restoration of the organization's information assets within a set time frame. There can be many reasons for undesirable situations. These are factors that are often beyond our control. It should be remembered that there are no universal emergency plans. Each organization must have its own plans, which can be implemented based on its own resources. Depending on the organization's activities' specifics, the same disruptions may pose a completely different scale of the threat to the company's operation.

The primary objective to create, implement and maintain Business Continuity Plans is to prevent business operation interruptions and to protect critical business processes from extensive failures of IT systems or catastrophes and to ensure the resumption of operations in due time (PN-ISO/IEC 17799, 2007).

To be prepared to take protective measures, maintain or restore the working environment, an action plan containing all the necessary elements and steps to be taken if the hazard materializes should be prepared separately for each threat. The result is to prevent, restore, or maintain the continuity of the process within a period acceptable by a customer.

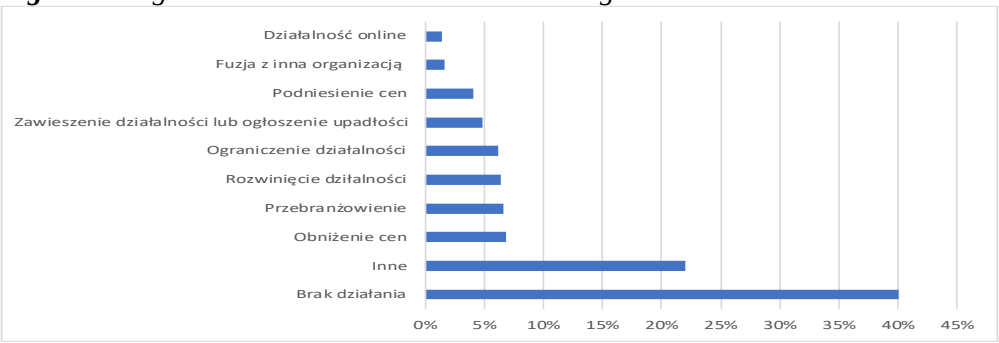
3. Activities Undertaken by Organisations in COVID-19 Era in Poland

Organizations undertake activities in Poland in the era of SARS-CoV-2 were and still are different. This largely depends not only on the organization's size but, above all, on the industry in which it operates. Looking at the current situation, we can conclude that the pandemic has excluded one vital resource in the organization: people, without which it cannot function.

However, this is a false conclusion because a large part of the organization, for example, by introducing remote working, has proved that it can operate and successfully carry out its processes without humans. What seemed to be the biggest problem at the beginning, however, is not because, from an economic point of view, it is the isolation of suppliers and customers that is the biggest problem of organizations.

The existing pandemic inspires many organizations to act, force other organizations to develop or change their business activities and leave no choice to others but go bankrupt. Organizations continue to work remotely, transfer sales to the Internet, reduce the number of fixed sales outlets, merge with other organizations, or find another profile of their activity - Figure 3.

Figure 3. *Organisation's activities in Poland during SARS-CoV-2*



Działalność online	Online activities
Fuzja z inną organizacją	Merger with another organisation
Podniesienie cen	Price increases
Zawieszenie działalności lub ogłoszenie upadłości	Suspension of activities or declaration of bankruptcy
Ograniczenie działalności	Limitation of activity
Rozwinięcie działalności	Development of activities
Przebranżowienie	Change of sector of activity

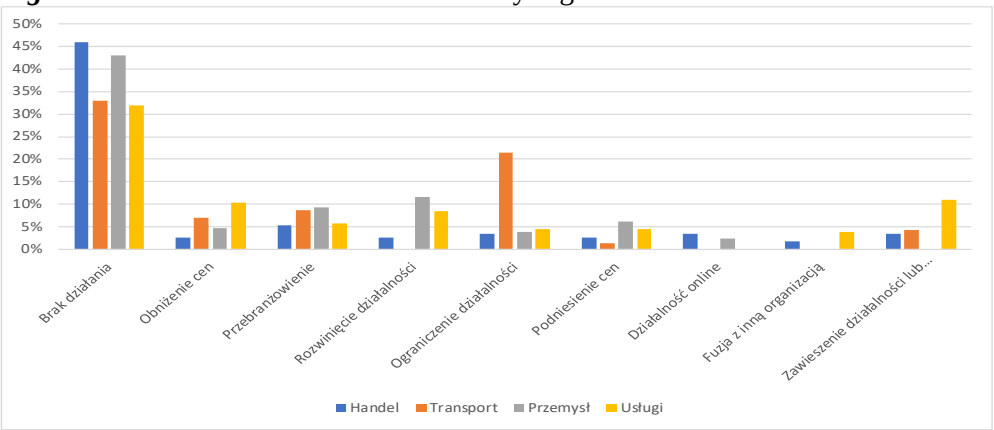
Obniżenie cen	Price decreases
Inne	Others
Brak działania	Failure to act

Source: *Own elaboration on based of BIG InfoMonitor (2020).*

During the COVID-19 pandemic, 40% of organizations declared that they did not decide to change their business strategy adopted. 7% of the organizations took actions to reduce prices when, at the same time, 4% raised prices in order to be able to continue their business and to put off the spectre of bankruptcy. However, 5% of the organizations have taken actions to suspend their activities or declare bankruptcy.

The differences in the extent to which COVID-19 has impacted organizations' activities in Poland can only be seen when we analyze it in terms of the industry. Figure 4 presents the activities undertaken by organizations in the four basic sectors affecting the Polish economy.

Figure 4. Activities undertaken in Poland by organisations in four basic sectors



Brak działania	Failure to act
Obniżenie cen	Price decreases
Przebranżowienie	Change of sector of activity
Rozwinięcie działalności	Development of activities
Ograniczenie działalności	Limitation of activity
Podniesienie cen	Price increases
Działalność online	Online activities
Fuzja z inną organizacją	Merger with another organisation
Zawieszenie działalności lub ogłoszenie upadłości	Suspension of activities or declaration of bankruptcy
Handel	Trade / retail
Transport	Transportation
Przemysł	Industries
Usługi	Services

Source: *Own elaboration on based of BIG InfoMonitor (2020).*

In transport, 21% of organizations are planning to reduce their activities, almost 9% want to change a sector of their activity, 7% are thinking about lowering prices, and 4% consider suspending their activities or going bankrupt. No actions are being taken on mergers. Simultaneously, in the trade/retail sector, only 3.5% of organizations intend to reduce their activities, 5% are thinking about reshaping, 2.6% are planning to reduce prices, and 3.5% consider suspending their activities or going bankrupt. This is not optimistic data, especially for transport organizations.

At the end of 2019, more than 91% of transport organizations had overdue cost-side invoices or overdue instalments of loans. Between 2012 and 2019, the number of transport organizations that went bankrupt has increased by more than 50% - from 34 in 2012 to 72 in 2019 (BIG Report, 2020, p.9-12), and the result of 4.3% at the beginning of 2020 will further increase this number.

In the service provisioning sector, 8.4% of organizations declare the development of their activities, e.g., pubs, cafés, and restaurants, are switching to a model of delivering products directly to customers. However, there are also areas of service activity where the remote provision of services is impossible or very difficult, such as hairdressing or cosmetic services. These organizations can actually prepare scenarios for a suspension to pass through the period of danger with the least possible loss.

The new reality has shown that organizations are taking many steps to change their "habits and routines." The business continuity plans often prepared under time pressure, help them to do this. These are not temporary measures, forced by a pandemic, but the measures allowing organizations to look to the future in the long term.

4. Continuity of the Organisations' Operations in COVID-19 Era in Poland

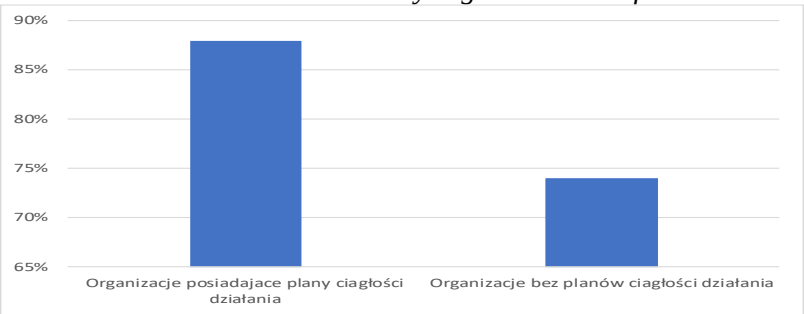
Organizations that emphasize the area of business continuity, i.e., they have a business continuity management system developed and implemented, have launched emergency plans during the pandemic. The plans developed and implemented defined key elements of the organization's functioning, such as what staff is key and who is in charge of taking particular actions. The plans launched provided the necessary resources to maintain the continuity of processes such as finances, IT equipment, communication channels, and information security procedures. It should be stressed that the organizations that anticipated the pandemic's problem and prepared themselves for it have changed their scope of operation much more quickly, which results, among other things, in opening up new areas of activity.

An earlier analysis shows that 40% of organizations did not take any action during the pandemic's initial period caused by SARS-CoV-2. What was the reason for this approach? Did these organizations have an emergency plan? Did they foresee this development of the situation and where they prepared for it? Did they have business

continuity plans in place? It is difficult to answer these questions fully. The results of research carried out in Poland by various centers do not give clear answers.

Based on the research published by the SGH (Warsaw School of Economics [pol. Szkoła Główna Handlowa]), it can be concluded that 54% of the organizations declared possession of Business Continuity Plans, which were updated on an ongoing basis. Among the organizations with Business Continuity Plans, only 13% considered the possibility of events such as a pandemic. Comparing the speed and efficiency of organizations' adaptation to the existing conditions, regardless of their size, one can see that organizations with Business Continuity Plan adapted more agilely to the realities than those without them - Figure 5 (Iwanicz – Drozdowska, 2020).

Figure 5. *Activities undertaken in Poland by organisations in four basic sectors*



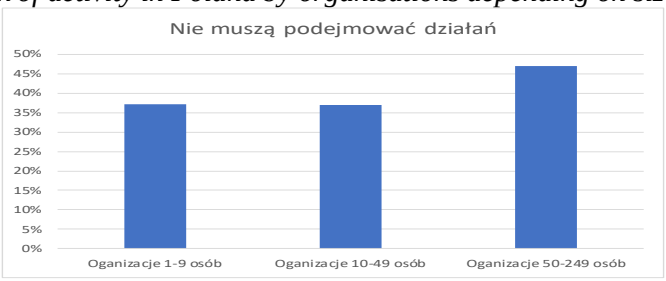
Organizacje posiadające plany ciągłości działania	Organisations with business continuity plans
Organizacje bez planów ciągłości działania	Organisations without business continuity plans

Source: *In-house elaboration based on Iwanicz – Drozdowska, (2020).*

Considering individual sectors, most organizations did not have business continuity plans in the area of education (72%), followed by IT (57%), health (54%), and trade (52%). Concerning processes critical to the functioning of an organization in the existing conditions, regardless of their size, it can be seen that in organizations with business continuity plans, most of the critical processes implemented were correct (92%) about those who did not have them (80%) (Iwanicz – Drozdowska, 2020).

It should be recognized that organizations, despite the lack of a business continuity plan developed and implemented, have managed quite well to adapt to the realities of business operation during the pandemic. In particular, plans should be implemented by large organizations employing over 50 people - Figure 6. This does not mean that micro organizations do not need such plans. However, they should also have them in a form that will help them adapt quickly to current realities.

Figure 6. *Lack of activity in Poland by organisations depending on size*



Organizacje 1-9 osób	Organisations, 1-9 persons
Organizacje 10-49 osób	Organisations, 10-49 persons
Organizacje 50-249 osób	Organisations, 50-249 persons

Source: *Own elaboration on based of BIG InfoMonitor (2020).*

Organizations that had business continuity plans did better during the pandemic. Therefore, it can be concluded that their development and implementation make it much easier to adapt to and operate in new realities.

5. Conclusions

The paper focuses on the issues related to the organization's activities during the COVID-19 pandemic in Poland. The results of studies on the use of business continuity plans are presented. It must be said that having business continuity plans in place has enabled organizations to adapt more quickly and effectively to new realities. Some organizations based their activities on improvisation. It allowed for a changeover and adaptation to new realities, but with much less effectiveness. To sum up, it is better to anticipate and plan action than to improvise, especially changing, difficult to predict conditions. Regardless of the organization's size and the industry in which it operates, each organization must take an individual approach to develop business continuity plans, which should include a cost analysis.

References:

Brundtland, G.H. 1999. Why Investing in Global Health is Good Polities. Council on Foreign Relations, www.who.int/director-general/speeches/1999/english/19991206_new_york.html.

Deloitte Database at: https://www2.deloitte.com/uk/en/pages/risk/articles/2018-global-crisis-management-survey.html.

Herbane, B. 2010. The evolution of business continuity management: A historical review of practices and drivers, Business History, 52(6).

Hiles, A. (ed.). 2007. The definitive handbook of business continuity management (2nd ed.). London: Wiley.

Iwanicz-Drozdowaska, M. 2020. Ciągłość działania w czasie pandemii SARS-CoV-2 – Polska na tle innych krajów.

Kaczmarek, T., Ćwiek, G. 2009. Ryzyko kryzysu a ciągłość działania. Difin, 18-22.

PN-EN ISO 22301. 2014. Bezpieczeństwo powszechne - Systemy zarządzania ciągłością działania – Wymagania.

PN-ISO/IEC 17799. 2007. Technika informatyczna Techniki bezpieczeństwa Praktyczne zasady zarządzania bezpieczeństwem informacji, Styczeń, 103.
Powolne hamowanie rozpędzonego transportu. Ogólnopolski Raport Biura Informacji Gospodarczej InfoMonitor o zadłużeniu sektora transportowego. Luty 2020. BIG InfoMonitor w www.big.pl.
Sikich, G.W. 2003. Integrated Business Continuity: Maintaining Resilience in Uncertain Times. PennWell Corporation, Tulsa, Oklahoma, 68-69.
The Good Practice Guidelines (GPG). 2008. The Business Continuity Institute. United Kingdom.
The Good Practice Guidelines (GPG). 2018. The Business Continuity Institute. United Kingdom
Utrata klientów i niepewna przyszłość. 2020. BIG InfoMonitor w www.big.pl.
Williams P.D. (red.). 2012. Studia bezpieczeństwa. Publishing of Uniwersytet Jagielloński.