INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Business Continuity Management in Wartime: A Case Study of IT Companies from Ukraine

Oleksandr Harkavenko

Master in International Management

Supervisor:
PhD, Florinda Maria Carreira Neto Matos, Assistant Professor,
ISCTE-IUL

September, 2024

BUSINESS
SCHOOL

Department of Marketing, Operations and General Management

Business Continuity Management during Wartime: A Case Study of IT Companies from Ukraine

Oleksandr Harkavenko

Master in International Management

Supervisor:
PhD, Florinda Maria Carreira Neto Matos, Assistant Professor,
ISCTE-IUL

September, 2024

I dedicate this work to honor all the defenders of Ukraine,
particularly to my friends:
Hryhoriy Tsekhmistrenko and Viktor Stselnikov,
who have fallen in Bakhmut in 2023

Acknowledgements

I would like to thank my professor, Florinda Matos, of ISCTE, for her support and understanding during the work on the master's thesis.

Thanks to my family and friends who have supported and encouraged me during the last years.

Abstract

During last years, the world has witnessed a number of unexpected and disruptive global events like COVID-19 and the Russian invasion of Ukraine. This trend marks a dramatic shift to the more uncertain and volatile global business environment. Due to the increasing number of new risks and potential threats, business continuity management becomes more important for organizations. This study aims to research Business Continuity Management practices of IT companies in wartime conditions.

Since February 2022, IT companies from Ukraine have met unprecedented challenges and gained unique real-life experience in business continuity management. The main purpose of this study is to identify key success factors of effective business continuity management in the conditions of war by analyzing the real experience of IT companies in keeping business continuity during the war.

The methodology of the study is based on qualitative analysis of semi-structured interviews and quantitative analysis of the risk assessment matrix. The data was collected from a sample of five IT companies from Ukraine.

The results of the study analyzed key challenges during the war and show that companies with pre-developed business continuity plans and mature business continuity management were more prepared for the first challenges of war.

The findings of the study will help other organizations in Ukraine to navigate the ongoing crisis and offer insights for international businesses facing geopolitical instability challenges combined with other types of crises.

Keywords: Business Continuity Management, war, crisis, Ukraine, IT

JEL Classification System:

- M1 Business administration
    - M15 IT Management
    - M16 International Business Administration

Resumo

Nos últimos anos ocorreu uma série de eventos globais inesperados e perturbadores, como a COVID-19 e a invasão russa da Ucrânia. Esta tendência marca uma mudança dramática para um ambiente empresarial global mais incerto e volátil. Devido ao número crescente de novos riscos e potenciais ameaças, a gestão da continuidade do negócio torna-se mais importante para as organizações. Este estudo investiga as práticas de Gestão da Continuidade de Negócio de empresas de TI em condições de guerra.

Desde fevereiro de 2022, as empresas de TI da Ucrânia enfrentaram desafios sem precedentes e ganharam uma experiência única na vida real na gestão da continuidade do negócio. O principal objetivo deste estudo é identificar os principais fatores de sucesso da gestão eficaz da continuidade do negócio em condições de guerra, analisando a experiência real das empresas de TI nesse âmbito.

A metodologia do estudo baseia-se na análise qualitativa de entrevistas semi-estruturadas e na análise quantitativa da matriz de avaliação de riscos. Os dados foram recolhidos de uma amostra de cinco empresas de TI da Ucrânia.

Os resultados do estudo, com vista a analisar as principais dificuldades durante a guerra, mostram que as empresas com planos pré-desenvolvidos estavam mais preparadas para os primeiros desafios provocados pela instabilidade vivida.

As conclusões do estudo ajudarão outras organizações na Ucrânia a navegar na crise em curso e oferecerão perspetivas para as empresas internacionais que enfrentam desafios de instabilidade geopolítica combinada com outros tipos de crises.

Palavras-chave: Gestão da Continuidade de Negócio, guerra, crise, Ucrânia, TI

INDEX

Acknowledgements iii

Abstract v

Resumo vii

List of Abbreviations xi

List of Figures and Tables xiii

Chapter 1. INTRODUCTION 1

1.1. Contextualization 1

1.2. Motivation and purpose of research 2

1.3 Research objectives and questions 3

Chapter 2. LITERATURE REVIEW 5

2.1. Structure of literature review 5

2.2. Business Continuity Management 5

2.2.1 Definition of BCM 5

2.1.2. Scope of BCM 7

2.1.3. BCM objectives and outcomes 8

2.1.4. Main frameworks of BCM 9

2.3. Business continuity management in the context of war 13

2.3.1. Specificities of BCM in the context of war 13

2.3.2. Challenges to traditional BCM frameworks 14

2.3.3. Adaptive strategies and success factors for BCM in wartime 15

2.4. IT sector in Ukraine 17

2.4.1. Overview of the IT sector 17

2.4.2. Typology and segmentation of the IT sector 18

2.5. Impact of the war in Ukraine 19

2.5.1. Impact on Ukraine 20

2.5.2. Impact of the war on the IT industry 21

Chapter 3. METHODOLOGY 23
Chapter 4. RESULTS AND DISCUSSION 25
4.1. Introduction of interviewed companies 25
4.2. Pre-war period Management (2020-2022) 26
4.3. Military Invasion Emergency Period Management (February - May 2022) 30
4.4. Ongoing War Period Management (May 2022 - May 2024) 34
4.5. Quantitative analysis of Risk Significance Perception Matrix 37
Chapter 5. CONCLUSIONS 41
5.1. Preparedness of the IT companies from Ukraine and implementation of BCM strategies 41
5.2. Evolution of risk perception and main challenges in BCM 43
5.3. Effectiveness of BCM strategies and key factors for successful BCM 44
5.4. Limitations and suggestions for further research 46
BIBLIOGRAPHIC REFERENCES 47
Annex A 51
Annex B 55

List of Abbreviations

BC – Business Continuity

BCM - Business Continuity Management

CMMI - Capability Maturity Model Integration

CM - Crisis Management

COBIT - Control Objectives for Information and Related Technologies

DRP - Disaster Recovery Planning

FinTech – Finance Technology

GDP - Gross Domestic Product

HIIK - Heidelberg Institute for International Conflict Research

ICT - Information and Communication Technology

ILO - International Labour Organization

ISO - International Organization for Standardization

ITIL - Information Technology Infrastructure Library

ITSM - IT Service Management

MilTech - Military Technology

NFPA - National Fire Protection Association

RPO - Recovery Point Objective

RTO - Recovery Time Objective

SMEs - Small and Medium Enterprises

List of Figures and Tables

Figure 1. Main BCM frameworks, components and activities

Table 1. Company information

Table 2. Results from the pre-war period

Table 3. Results from the military invasion period

Table 4. Results from the ongoing war period

Table 5. Average values of risk category perception across the research periods

Table 6. Average values of risk perception by companies during the research periods

Chapter 1. INTRODUCTION

1.1. Contextualization

On February 24, 2022, Russia invaded Ukraine and started an unprecedented full-scale war in Europe for the last 80 years. This large-scale invasion led to the deaths of thousands of civilians, the destruction of cities, extensive damage to critical infrastructure, industrial and transport infrastructures, and numerous private properties. This invasion has become the peak of eight years of Russian aggression against Ukraine.

The aggression started earlier in 2014 with the annexation of Crimea and initiated the hybrid war in Donbas. As the result, the economy of Ukraine has passed through significant transformation during the last decade. The main changes were a re-orientation of exports towards the EU and USA as well as rapid growth in the IT sector. The sector has seen almost 20% average yearly growth. The share of IT industry in the structure of Ukraine's exports increased from 0.8% of GDP in 2012 to 4.0% in 2021. This reflects that Ukraine became a significant IT outsourcing hub in Eastern Europe during this period. Moreover, the structure of the Ukrainian IT sector became more diversified due to the increase of IT service consulting and R&D segments.

In 2021, the Ukrainian IT exports increased to 6.8 billion USD. This indicated a historical growth peak of 36% in the Ukrainian IT sector. The number of IT specialists rose from 244,000 to 285,000. In the last three years, the industry has more than doubled its exports and increased its employment by over 50% (*IT Association of Ukraine 2021 Annual report*, 2021).

In the decade before the invasion, the Ukrainian companies were less concerned about the geopolitical risks than about government regulations or increased hiring demand for IT specialists. However, the geopolitical tensions imminently continued to rise and prompted Ukrainian businesses to invest in business continuity management (BCM) strategies.

The ongoing Russian invasion of Ukraine is the case of both - a significant humanitarian crisis and global economic and business disruption. Even before the invasion, the economies of Eastern Europe countries were struggling to recover after the harsh effect of COVID-19 pandemic on their economies. Overall, this is a case of a uniquely compounded crisis that poses unprecedented challenges for business continuity and risk management by combination of the post-pandemic effects and the immediate and long-term impacts of war.

1.2. Motivation and purpose of research

The motivation of this research is driven by the fact that the Russia's full-scale invasion is causing widespread disruption to daily life and business operations in Ukraine. Every day the war is inflicting human losses and damage on Ukraine's infrastructure and economy. However, the economy of Ukraine and particularly its IT sector managed to survive and recover despite the wartime conditions. Moreover, the IT sector became an extremely important part of nowadays economy and crucial for Ukraine's exports. The resilience and adaptability of this sector during turbulent times presents a unique chance to explore the effectiveness of business continuity management practices of IT companies in extreme turbulent conditions.

This research aims to contribute valuable insights into the practical application of BCM strategies in real-world scenarios. The study is going to research the potential gap between business continuity management theory and actual practices used by Ukrainian IT companies in wartime conditions. The key element of the research is the collection and examination of real-life experiences of the IT companies from Ukraine during the war.

The primary purpose of this research is to understand how to effectively manage the business continuity of a technology company in highly volatile conditions like wartime conditions. To fulfill the primary purpose, the research seeks to complete the secondary purposes as to analyze the wartime business environment characterized by multidimensional volatility and uncertainty. Then, the study will explore the wartime challenges experienced by IT companies in Ukraine throughout the ongoing war. Finally, the study aims to identify effective management strategies and investigate how they approach specific business continuity challenges caused by the war. The research also seeks to identify and evaluate the best practices and key factors that contribute to successful business continuity management.

The research findings will help navigate the current crisis and offer insights for other organizations operating in similarly unstable conditions. The research may benefit international businesses facing geopolitical instability challenges combined with other types of crises.

The insights and recommendations derived from this research will help IT companies and other organizations improve their BCM practices, ensuring better preparedness and resilience in the face of potential future conflicts or crises.

1.3. Research objectives and questions

For each research objective, there was defined a set of research questions in order to approach the different aspects of the corresponding objectives:

1. Examine preparedness of the Ukrainian IT companies and implementation of the BCM strategies across the pre-war, military invasion, and ongoing war periods:

- What was the level of preparedness of the Ukrainian IT companies in terms of business continuity? How did the companies make preparations before the potential invasion? How was BCM implemented during the war? How did the adaptation of business operations happen in the conditions of the war?

2. Identify the main challenges in BCM and analyze evolution of risk perception across the pre-war, military invasion, and ongoing war periods:

- What were the main challenges in maintaining business continuity during the pre-war, military invasion, and ongoing war periods? How did the perception of risk significance evolve among the IT companies across the pre-war, military invasion, and ongoing war periods?

3. Analyze the effectiveness of BCM strategies and determine key factors for successful BCM:

- What BCM strategies were effective in ensuring business continuity for Ukrainian IT companies during the war? What gaps can be identified between the BCM strategies and practices “on paper” and their real-world execution? What key factors have contributed to the successful business continuity management of Ukrainian IT companies across the pre-war, military invasion, and ongoing war periods?

This master thesis is organized into five chapters to fulfill the specified research objectives.

The first chapter gives a context for the research, describes research motivation and purpose, and establishes research objectives and questions to lead the research.

The second chapter presents a review of the research literature on business continuity management and the IT industry of Ukraine.

The third chapter describes applied methodology, and the methods used to analyze collected data during the research process.

The fourth chapter demonstrates the results from qualitative and quantitative analyses and presents some relevant findings.

The fifth chapter presents the conclusions obtained from the discussion of the research results aligned according to the research objectives. This chapter also explains the limitations of the study and proposes suggestions for further research.

Chapter 2. LITERATURE REVIEW

2.1. Structure of literature review

The literature review is structured in the deducing order from reviewing the broader context of the BCM concept to setting the focus on the research topic details. In this chapter, the definitions and the scope of the concept are outlined, the main frameworks are presented and assessed. Then provided contextualization of the concept within the research phenomenon, reviewed external environment factors that contribute to the contextualization of qualitative data analysis.

The data for literature review research was collected through Scopus, Web of Science, SAGE Premier, accessed via ISCTE Repository, as well as some sources collected from Google Scholar. The time frame for the literature source publications was set to last 15 years with several exceptions for highly cited and relevant literature sources.

The search process was elaborated using the following keywords and queries: “Business continuity management”, “war in Ukraine”, “Business continuity” + “Ukraine”, “BCM” +” conflict”, “BCM” + “war in Ukraine”.

The main literature source types found during the research and used for this literature review were peer-reviewed research articles, reports and “white papers” from industries and international organizations.

2.2. Business Continuity Management

2.2.1 Definition of BCM

Business continuity management originated in the 1970s as a concept that synthesizes areas of psychology, engineering, facilities management, risk analysis, disaster recovery planning, and crisis management (Herbane, 2010). This multidisciplinary foundation showcases BCM's comprehensive nature and approach which integrates human resources, organizational skills and hardware assets to manage and mitigate crises effectively.

Academic literature and industry standards provide a diverse range of definitions of the BCM. These definitions complement each other in their perception of this management concept.

The research paper by Herbane, Elliott, and Swartz (2004) defines Business Continuity Management (BCM) as a systematic management activity to identify "potential threats to an organization and the effects of crises and interruptions, ensuring operational continuity and preserving competitive advantage". The researchers state that BCM involves synthesizing both "hard and soft assets" to provide effective crisis prevention and recovery (Herbane et al., 2004).

Later, Herbane (2010) provides further elaboration on the earlier definition of BCM. He emphasizes the holistic nature of BCM as a framework for organizations to build resilience and facilitate effective responses to protect tangible and intangible assets of organizations, as well as the interests of key stakeholders (Herbane, 2010).

Păunescu argues that managing business continuity is a method for determining which business processes are essential and then creating strategies to keep these business processes running with minimal interruptions (Păunescu, 2017).

A recent research paper by Vanichchinchai (2023) defines BCM as "a holistic management process" that analyses possible risks to identify potential threats to an organization and their impacts on business operations (Vanichchinchai, 2023).

In the industry contexts, BCM is often closely bonded with risk management and continuity of IT service and telecommunications. For example, Wan and Chan (2008) discussed that in the IT and telecommunications sectors, BCM is primarily about prioritizing IT operations management activities by application of business impact analysis frameworks with the help of automated network and system alerts (Wan & Chan, 2008).

Chen and Hu (2009) found that in the context of e-business, BCM is defined by the various components such as hardware resources, grid server systems, and user portals integrated into high-level systems to improve the reliability and continuity of operations in distributed e-business environments (Chen & Hu, 2009).

The international standard "ISO/DIS 22313" describes Business Continuity Management (BCM) from holistic point of view as the management process that focuses on identification of potential threats and the impacts to business operations of those threats. It provides a framework for developing resilience in organizations so that they have capability to respond effectively and protect its reputation, brand, and value-creating activities as well as their important stakeholders (ISO/DIS 22313, 2011).

While in the recently published international standard ISO 22300:2021, business continuity management was defined as “a process to implement and maintain business continuity in an organization” (ISO 22300:2021). However, this definition requires a more thorough understanding of what business continuity actually is. The most commonly accepted definition of business continuity was provided by International Organization for Standardization (ISO) in the standard “ISO 22301:2019” where business continuity was defined “as an organizational capability to continue the delivery of products and services within acceptable time limits at predefined capacity during a disruption event” (ISO 22301:2019).

The academic and industry approaches in defining BCM similarly highlight the importance of preparedness for potential threats and ensuring continuity of operations. The academic researchers together with industry specialists agree with the idea that in reducing risks related to business interruptions, BCM plays a crucial role (Varajão & Amaral, 2021).

However, there emerge some differences in BCM definitions. Academic definitions often provide a broader and more theoretical perspective. These definitions tend to incorporate elements of organizational resilience and strategic value into the BCM concept. In contrast, industry definitions tend to focus more on practical aspects.

For example, Herbane (2004) and Păunescu (2017) presented an academic viewpoint to comprehensive practices of resilience and preparedness within organizations. On the other hand, the industry perspective, Chen and Hu, 2009, is focused on real-world application of BCM practices inside IT frameworks and on the operational continuity of IT services and infrastructure.

2.1.2. Scope of BCM

In terms of scope, BCM is often compared to similar concepts like Crisis Management (CM) and Disaster Recovery Planning (DRP). Crisis management deals with managing unexpected events on both strategic and tactical levels whereas disaster recovery planning is more narrowly focused on restoring IT activities after a disaster (Herbane et al., 2004).

Unlike crisis management and disaster recovery, BCM covers the entire timeline from pre-crisis to post-crisis stages and focuses on anticipation and prevention of disruptions (Herbane,

2010). The BCM concept includes proactive approaches to protect businesses from failures, natural disasters, attacks, and economic crises (Rodríguez-Rojas, 2021).

Furthermore, the scope of BCM incorporates processes of risk analysis to identify vulnerabilities and potential threats (Torabi et al., 2016). Schätter (2019) also discusses risk control role of BCM in supply chain management. This role helps organizations to run critical supply chain operations during emergency events and therefore provides a competitive advantage for organizations (Schätter, 2019).

2.1.3. BCM objectives and outcomes

Herbane (2004) determined the principal objectives of BCM are to secure operations without interruptions and preserve competitive advantage under turbulent conditions (Herbane, 2004). Păunescu (2017) elaborates on the next key BCM objective of organizations as the ability to continue performing critical functions during and after a disruption. The scope of this objective includes minimizing interruption effects, protecting critical business functions, and speeding up recovery to normal operations (Păunescu, 2017). Russo et al. (2024) add BCM aims to safeguard the organization's physical and digital assets, ensuring these assets are protected against potential threats (Russo et al., 2024).

Another important objective of BCM, discussed by Boh (2023) is building resilience within the organization. This research outlines key means to reach the objective by being able to absorb, withstand, adapt, and recover from the major shock disruptions of digital infrastructure failures (Boh et al., 2023).

When an organization establishes a BCM program, its key focus is high effectiveness of organization’s capability to recover after disruptive incidents. To measure the effectiveness of the BCM there are used a set of recovery time objectives (RTOs) and recovery point objectives (RPOs). These objectives are quantitative checkpoints within IT system and throughout business end-to-end flow. The goal of high effective BCM program is maximum possible recovery of impacted assets by minimally possible time spent for recovery (Russo et al., 2023).

Implementation of BCM provides a range useful outcomes which lead to organization success. Russo et al. (2024) state that successful outcomes of BCM depend on objective to comply with international standards and following established frameworks. In the context of the benefits of effective BCM, Rodiguez-Rojas (2021) concluded that the implementation of

business continuity management improves life, property and environmental protection. Moreover, well-implemented BCM not only preserve the reputation of an organization but also enhance the credibility of stakeholders (Rodiguez-Rojas, 2021).

Thus, organizations with working BCM programs get a significant relative competitive advantages over organizations with low level of BCM practices. The core competitive advantage is developed capabilities to operate during interruptions. Furthermore, BCM improves cost reduction and efficiency improvement, increase of resilience capacity, reduction of legal and financial exposure (Rodríguez-Rojas, 2021). Also, during the period of significant operational disruptions, decision-makers may encounter difficult scenarios challenged with uncertainty, complexity, and tight deadlines. In this context, effective BCM practices facilitate prompt decision-making and enhance organizational value (Schätter et al., 2019).

To summarize the studied publications, the primary objectives of BCM are to recover from disruptions, manage risks, ensure business continuity, establish organizational resilience based on prevailing international standards. The expected outcomes include minimized time of disruption, improved recovery capabilities, protected assets, compliance with international standards.

2.1.4. Main frameworks of BCM

In Business Continuity Management (BCM), a framework is referred to a structured collection of guidelines and standards aimed to help organizations to achieve the objectives of business continuity management. Also, organizations can extend frameworks by including best practices into the main body of knowledge (Russo et al., 2023).

The research conducted by Russo et al. (2023) analyzed existing business continuity frameworks and identified the most relevant frameworks for BCM such as ISO 22301 (22301:2019), CMMI v2.0, COBIT 2019, ITIL 4 and the NFPA 1600. Each of these frameworks highlight specific components needed in different contexts to sustain essential functions of organizations during and after emergency incidents (Russo et al., 2023).

ISO 22301:2019 specifies the requirements for Business Continuity Management Systems (BCMS). The standard describes a structure of business continuity management and the logic of incorporating a continuous improvement cycle. ISO 22301 presents performance metrics organizational resilience and recovery from disruptions (ISO, 2019).

As the result, ISO 22301 serves as the foundational framework for business continuity planning and the integration of various systems due to its systematic approach to BCM and adaptability to the context of IT development management. The reviewed literature indicates a broad acceptance of ISO 22301 and adaptation of the standard especially among ICT companies (Russo et al., 2023).

Based on existing ISO 22301 standards, Cedergren and Hassel (2024) present a comprehensive Multiactor framework. Their customized framework diverges from the original one by focusing on societal safety and promoting high conceptual harmonization among actors. This framework emphasizes the necessity of expanding BCM beyond individual organizations to accommodate networks of interdependent actors. This expansion is crucial, as modern societal functions rely on multiple actors collectively delivering essential services to end users (Cedergren & Hassel, 2024).

COBIT 2019 refers to Control Objectives for Information and Related Technologies family of frameworks designed by the Information Systems Audit and Control Association. COBIT 2019 has a primary focus on IT governance, but it also involves BCM as part of its comprehensive governance model. For implementation of BCM program, COBIT 2019 framework promotes the widespread application of performance measurement to monitor operational activities turbulent conditions and improve BCM practices (ISACA, 2018).

The reviewed publication of Russo et al. (2023) leads to conclusion that COBIT and ISO align well to be used together. These frameworks complement each other int their respective characteristics. COBIT is a broad, general framework often applied at the strategic level. Therefore, combining these frameworks can create a sustainable approach, with ISO providing detailed guidelines and COBIT offering strategic direction for decision-making and governance.

The ITIL 4 framework for BCM outlines comprehensive standard practices for IT service management (ITSM) activities and detailed techniques how to handle service disruptions in different scenarios. Main goal defined in ITIL's BCM framework is to minimize impact on IT services and business operations. In contrast to COBIT 2019 framework, ITIL specifies guidelines for IT service management and prioritizes the alignment of business requirements with IT services. Thus, IT support services departments or outsourcing support companies adopt this framework for their BCMS. Similarly to other frameworks, this one introduces Key

Performance Indicators and highlights their importance to ensure the effectiveness of BCM activities (AXELOS, 2019).

The CMMI v2.0 framework allows to assess maturity of organizations' capabilities and their integration within organizational system. This maturity assessment helps to identify bottleneck areas for improvement and shape further strategic development of an organization. Moreover, CMMI v2.0 framework holds the Continuity practice which showcases how to integrate business continuity activities into broader context of transformations to improve processes in organizations. The framework provides tools to enhance BCM quality by providing structured guidelines for improving processes (CMMI Institute, 2018).

However, the application of CMMI model to develop mitigation plans has a drawback because it does not offer specific metrics tailored to BCM, in contrast to the ITIL 4 framework. Addressing potential drawback, Henríquez et al. (2021) investigated the alignment of Agile methodologies with CMMI v2.0 within organizations. They conclude these cases boost implementation of agile practice within organizations without impacting its overall resilience (Henríquez et al., 2021).

The NFPA 1600 framework focuses on outlining criteria to manage wide variety of emergencies and continuity programs. This framework structures components to create and manage BCM programs to be applicable in different emergency scenarios. NFPA 1600 is different from the other frameworks because it covers a wide range of activities of emergency management beyond just business continuity (NFPA, 2019).

Considering the wide coverage of NFPA framework, Petrenko (2021) discusses integrating NFPA 1600 with other international standards like ISO 22301 to create a robust BCM system by developing quantitative metrics for assessing cyber resilience and integrating BCM with disaster recovery management (Petrenko, 2021).

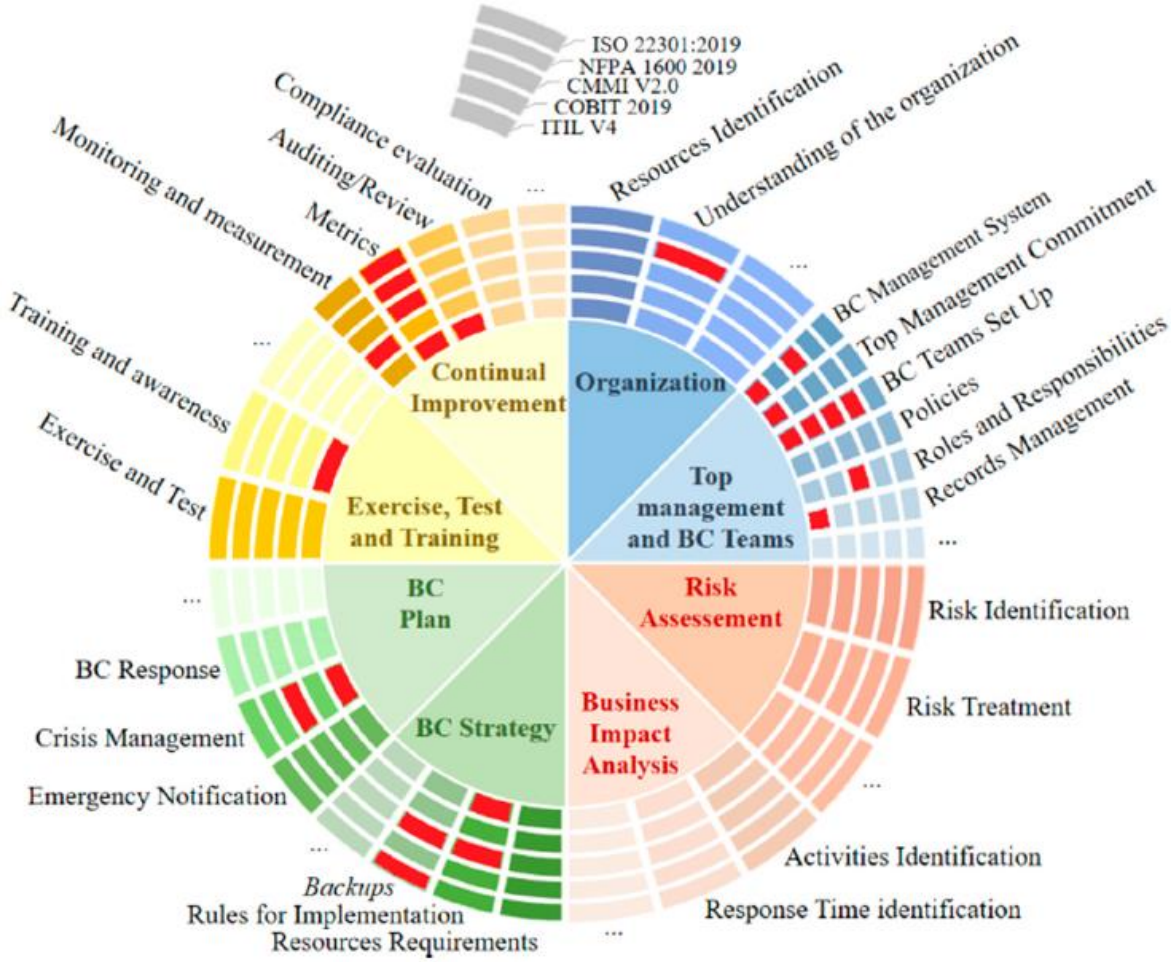

Figure 1. Main BCM frameworks, components and activities

Source: Russo et al., 2023, p. 4

A comparative analysis of BCM frameworks conducted by Russo et al. (2023) reveals gaps in their coverage of BCM activities. Summarizing the analysis, ISO 22301:2019 lacks specific guidance on backups and metrics activities (ISO, 2019). NFPA 1600 does not adequately address understanding the organization, BC team's setup, and metrics activities (NFPA, 2019). CMMI v2.0 and ITIL 4 show several gaps, particularly in areas such as the business continuity management system, roles and responsibilities, rules for implementation, and crisis management (CMMI Institute, 2019; AXELOS, 2019). These gaps highlight that in order to have effective BCM and to be resilient against disruption, organizations need to integrate best practices from multiple standards.

Despite the differences between these frameworks, they share common elements required for effective BCM. These key elements include risk analysis, business impact analysis, strategy development, plan documentation, training, testing, and measurement.

In conclusion, the most recognized BCM frameworks, including ISO 22301, CMMI, COBIT, ITIL, and NFPA 1600, offer structured approaches to managing business continuity and share some common elements. However, their BCM methodologies and purposes are different due to different contexts of each framework. Therefore, understanding these differences and commonalities can help organizations select, combine and adapt the most suitable BCM practices into the custom framework that address unique needs and contexts of the organization.

2.3. Business continuity management in the context of war

2.3.1. Specificities of BCM in the context of war

According to Obłój and Voronovska (2024), a war is “an extreme case of disruption” creating existential threats to the survival of businesses and their personnel.

In the past decades, wars and military conflicts have become a "new normal" type of disruption of business operations due to the increasing trend of number and violence in recent years (Obłój & Voronovska, 2024). For example, in 2022 the number of wars is increased to 21 as well as the increased number of violent crises to 174, mainly in Africa and Asia (HIIK, 2023). Moreover, the nature of modern wars tends to turn into prolonged military conflicts. Opatska et al. (2024) defines war as a crisis type characterized by its unpredictability, diffusive and prolonged disruption, and its impact on both the physical and psychological landscapes of affected societies and businesses.

In war zones and buffer zones operating businesses must navigate environments characterized by the conditions of significant “uncertainty, depleted resources, unreliable financial systems, heavy reliance on foreign aid to sustain its operations” (Obłój & Voronovska, 2024).

Bai and Yelisieiev (2023) further explores the business operating conditions in the context of war, on the example of the war in Ukraine. Mass migrations of the population, both internal out of the frontline zones and external abroad, has led to a reduced workforce and necessitated the reorganization of work processes to accommodate remote work and other new operational demands. The full-scale invasion has profoundly disrupted traditional management methods in Ukraine. Companies have to relocate and restructure due to the life risks of personnel and

destruction of infrastructure and ongoing military risks. This process significantly requires strategic planning, logistical efforts, and financial resources to maintain business continuity.

The chaotic nature of Russian rocket attacks on Ukrainian cities with all of the associated risks has complicated business operations and created disruptions in productivity. This needs to be addressed by the implementation of safety protocols, such as shelters for remote work during air raid alerts.

The mobilization of employees and changes in labor legislation have also introduced additional layers of complexity to human resource management, including the need to manage military service obligations and navigate new legal frameworks governing labor relations. These factors have collectively resulted in decreased labor availability and productivity, disrupted supply chains, business operations and planning (Bai &Yelisieiev, 2023).

2.3.2. Challenges to traditional BCM frameworks

The conditions of war and different forms of disruptions challenge existing BCM frameworks and approaches to manage crises. The traditional BCM approaches have traditionally developed managerial behaviors around other types of crises which differ significantly in the context of war.

The studies by Bai and Yelisieiev (2023), and Obłój and Voronovska (2024) reveal that existing BCM practices are insufficient in the face of such extreme and hostile wartime conditions and disruptions caused by military conflicts.

Bai and Yelisieiev (2023) exposes the limitations of BCM frameworks that assume predictability in the operating environment. Then, Obłój and Voronovska (2024) argue that existing theoretical frameworks of business continuity management have been primarily concerned with isolated disruption events such as natural disasters or cyber-attacks.

The existing BCM frameworks are often focused on the importance of protecting and recovering specific business domains which is not sufficient to cover the complex, systemic and prolonged nature of war-related disruptions (Obłój & Voronovska, 2024).

This gap highlights the need for more adapted BCM approaches to better address the unique challenges posed by war. This requires a broader theoretical framework that can link the

complex interactions between different business operations and external factors in a military conflict environment (Obłój & Voronovska, 2024).

Opatska et al. (2024) reveal that, in the context of the war in Ukraine, business leaders had to rely heavily on improvisation and resilience, given that traditional BC plans were often inadequate in the face of the complex and dynamic nature of the war.

Several studies highlight the value of past crisis experiences in preparing organizations for potential disruptions. The most common crisis management experience was the COVID-19 pandemic that gave impetus for remote IT infrastructure and experience in managing remote teams, and the more specific experience related to the evacuation of companies and employees was related to 2014 Crimea annexation and Donbass conflict (Obłój & Voronovska, 2024).

However, the research by Opatska et al. (2024) shows the experiences of Ukrainian business leaders who found that no amount of prior crisis preparedness could fully prepare them for the shock and ongoing uncertainty brought by scale and severity of the ongoing war. In that context, the absence of a clear endpoint increased a sense of disorientation, making traditional BCM strategies less effective.

2.3.3. Adaptive strategies and success factors for BCM in wartime

The research by Obłój & Voronovska, 2024 further explores how the companies respond to war-induced crises, on the example of the war in Ukraine. The initial responses often align with threat-rigidity theory. Initially companies avoid proactive actions and react conservatively with focus on survival due to uncertainty and stress. However, as the crisis persists companies tend to follow contingency theory by operating with more flexibility and proactive measures to adapt to the changing environment.

Obłój et al. (2024) discuss that the combination of both response strategies can be an essential feature for BCM in IT where the initial response has to secure critical data and infrastructure while subsequent strategies focus on adapting to the new normal. Therefore, this can lead to more flexible and resilient business continuity plans (Obłój & Voronovska, 2024).

The authors, Bai and Yelisieiev (2023) and Kostruba (2024), highlight that organizations have to quickly adapt to the new realities, develop management structures that prioritize flexibility, implement rapid decision-making, integrate digital technologies to maintain communication and productivity under the wartime conditions.

These include more adaptive organizational hierarchies, enhanced focus on employee safety and well-being, and the adoption of short-term planning strategies for better control of the high level of uncertainty in the operating environment. Bai and Yelisieiev (2023)

Additionally, Kostruba (2024) pointes out the importance of resilience and adaptability in BC management. In the context of the IT sector, this includes diversification and distribution of human resources, flexible operational models, and comprehensive contingency planning.

Kostruba (2024) underscores the importance of governmental support in the form of simplified business regulations, grants and tax incentives for companies operating in conflict zones. The implementation of regulatory frameworks such as e-residency allows businesses to legally operate remotely, which is particularly relevant for the IT sector. This approach can mitigate the physical risks associated with conflict zones, ensuring that IT companies can continue their operations without the need of physical representation.

The research by Kostruba (2024) also highlights the critical role of digital transformation in ensuring business continuity. Investments in internet infrastructure, digital tools and platforms can help companies manage operational challenges more effectively but also encourage growth despite adverse conditions (Kostruba, 2024).

In addition, Obłój and Voronovska (2024) introduced the idea of "leap of faith" in business continuity. This concept means that companies move beyond simple survival to seek and develop new opportunities amidst crises. Small and medium IT companies can foster risk-taking, innovation and development capabilities for addressing the existing threat from the crisis environment, creating new business values and reinforcing their market position within the same development branch. This concept can be particularly impactful for IT companies and especially IT human resources as an approach of how to thrive under the crisis challenges and during post-crisis adaptation (Obłój & Voronovska, 2024).

Considering the migration, humanitarian and labor market situations, Borowska-Pietrzak et al. (2023) underscore the importance of corporate social responsibility in the context of war to contribute to societal resilience, humanitarian aid, and ensuring the well-being of employees and local communities. This helps in sustaining the affected population, maintaining the operational business continuity and reputation of businesses in wartime and during the post-war recovery.

Obłój and Voronovska (2024) agree that businesses can play a certain role in mitigating the impacts of war, but their conflict reduction abilities in war environments remain limited and underexplored. The researchers came to the conclusion that the nature of war and practical challenges in the war-affected zones often limit the effectiveness of supporting local communities and the results of these efforts on peace and stability (Obłój & Voronovska, 2024).

Studies by Bai et al. (2023), and Borowska-Pietrzak et al. (2023) highlight the critical role of psychological support of employees and sustainable human resources management to maintain operations stability during the wartime. The researchers suggest that effective BCM during wartime should include employee welfare and psychology programs.

Moreover, Opatska et al. (2024) underscored the critical role of leadership during the wartime. To manage continuity of business, leaders were required to engage in constant, frequent and transparent communication with their employees. In some contrast with the piecetime, the focus of communication during wartime was not only on operational continuity matters but mainly on maintaining morale and a sense of hope among teams. Leadership during this period was characterized by a need to sustain optimism and provide a vision of future recovery, even in the face of ongoing uncertainty. This aspect of the research highlights the importance of emotional intelligence and adaptive leadership in BCM in turbulent times.

2.4. IT sector in Ukraine

2.4.1. Overview of the IT sector

Over the past few decades Ukraine's IT industry has been transformed from an emerging sector of economy into a key component of the national economy. This transformation is particularly noteworthy considering the political and economic challenges in Ukraine since 2014 marked by conflict in Donbass and economic instability. Despite these challenges, since 2014 the IT industry has demonstrated annual growth of 25% and contributing around 4% of GDP. From 2017 to 2022 the industry has shown a remarkable rise in export of IT services with a 26.8% annual growth rate. In 2022, the annual export of IT services reached its record high of $7.34 billion (Prokhorova et al., 2023).

According to the 2023 research by IT Ukraine Association, the key competitive advantages that contributed to these results were: highly skilled workforce; cost-effective services and the best ratio between the quality of services and cost; diverse expertise across technology sectors;

cultural similarities. The main export destination since 2014 has been the USA, followed by Malta, the UK and Cyprus (IT Ukraine Association, 2023).

As of 2021, approximately 289,000 people were employed in IT industry, representing 1.9% of Ukraine's workforce. 80% of all employees are in the age group of 21-35 years. The gender distribution before the war was 74% of male and 26% of female employees (IT Association of Ukraine, 2021).

2.4.2. Typology and segmentation of the IT sector

As per Melnyk and Zavhorodnya (2022) the Ukrainian IT companies can be categorized into several types of companies based on their business models and areas of specialization:

- **Service Outsourcing Companies**:

Service-oriented companies focus on software development and IT services to clients based outside Ukraine. The outsourcing model is prevalent in the Ukrainian IT industry. The outsourcing companies are the leaders by size and revenues including SoftServe, EPAM Systems, and Ciklum.

- **Product Companies**:

Product-oriented companies focus on developing their own software products, which they market and sell globally. Product companies are fewer in number compared to outsourcing firms. However, the trend is the growing number of product companies as Ukraine's tech ecosystem matures.

- **R&D Centers**:

Several multinational corporations and companies, such as Samsung R&D Institute, Oracle, Materialise, have established research and development (R&D) centers in Ukraine to have access to the country's IT workforce. These centers are mainly located in the capital of Ukraine and focus on leveraging tasks from the regional R&D centers.

- **Startups**:

Ukraine has a startup ecosystem which got boosted during the COVID-19 pandemic. These startups are supported by the Ministry of Digital Transformation, local incubators, accelerators, and venture capital firms. Examples of the most famous Ukrainian startups include Reface, Petcube, Ajax Systems.

The total number of IT companies and startups in Ukraine is difficult to calculate due to the specificities of one company having several legal entities in Ukraine. Therefore, before the Russian invasion of Ukraine in 2022 the government Tech Ecosystem portal estimated the number as 2300 active IT companies. As of November 2022, the last estimate was 2400 active IT companies. Tech Ecosystem portal estimated that the product-oriented companies make the majority in the market with 70%. Service outsourcing companies represent 20% of the market with more than 550 companies. R&D centers represent around 4.5% with 89 companies in Ukraine. Startups represent the rest 5% with around 100 companies (IT Ukraine Association, 2023).

By the number of employees, 74.7% of Ukrainian IT companies have up to 50 employees, 16.8% have 50-200 employees, 6.9% have 201-1000 employees, 1.5% have 1001-5000 employees and 0.1% of companies have more than 5001 employees representing GlobalLogic, SoftServe and EPAM (Khomenko et al., 2022).

The main hubs of IT in Ukraine centered around big cities with technical educational institutions. The main IT hubs of Ukraine are Kyiv, Kharkiv and Lviv. Kyiv is located 100 km from the border with Belarus. Kharkiv is located 30 km from the border with Russia which played a negative role for development of the hub after the full-scale war. Kyiv as the capital and economic center is the largest IT hub of Ukraine with 44% of the total number of IT professionals working in the city and its region. Followed by Kharkiv with 14%, Lviv with 10%, Dnipro 9% and Odesa with 5%. After the start of the war, the hubs closer to the border with Russia have significantly declined due to the relocation of IT specialists to the western Ukraine or abroad. The number of IT specialists tripled in the hubs of western Ukraine increasing the importance of the cities of Ternopil, Ivano-Frankivsk and Uzhhorod (Prokhorova et al., 2023).

2.5. Impact of the war in Ukraine

In the past decades military conflicts have often taken place in regions relatively disconnected from global politics and economy such as Liberia, Rwanda, Sudan, Syria. In contrast, the ongoing war in Ukraine is happening in a large European country that is more integrated into the global economic and political system (Obłój & Voronovska, 2024). Example of this interconnected nature is Ukraine’s role in chipmaking. The Russian invasion of Ukraine significantly disrupted global value chains of electronic components and equipment for ICT

sectors as Ukraine supplied about 50% of neon in the world for chipmakers (DeCarlo & Goodman, 2022).

The Russian invasion of Ukraine in February 2022 has had profound and far-reaching impacts on the global economy, with significant implications for the Europe and Central Asia (ECA) region. There are a multitude of devastating impacts such as disruption in economies, labor markets and employment, social and humanitarian crisis, supply chain repercussions, and regional spillover effects. The initial impact got especially significant stress on low- and middle-income economies that were still recovering from the COVID-19 pandemic in the beginning of 2022 (ILO, 2022; World Bank, 2023).

2.5.1. Impact on Ukraine

The World Bank (2023) reports that the crisis has significantly disrupted local labor markets, both in Ukraine and in neighbouring countries that have received large numbers of refugees. The Russian invasion of Ukraine caused a catastrophic impact on the Ukrainian economy and businesses. As detailed in the ILO report 50% of businesses in the regions close to the frontline had to close down (ILO, 2022). The conflict has caused significant disruptions, leading to large-scale employment losses, economic stagnation, destruction of infrastructure, and massive internal and external displacement (World Bank, 2023).

The invasion has caused massive job losses on the labor market. The ILO projected that up to 7 million jobs have been lost in Ukraine which represent 43.5% of the pre-conflict employment workforce. The displacement of workers and the destruction of business infrastructure are key factors driving this labor market crisis (ILO, 2022).

World Bank (2023) estimated that on average Ukrainian firms lost 25% of their workforce. One of the immediate consequences of the invasion has been huge disruption of sales. On average, sales across firms dropped by 53%, with small businesses experiencing the most significant decline at 55%. The correlation between the drop in sales and employment is notably strong, indicating that firms experiencing severe sales declines also tended to reduce their workforce more significantly. About 70% of companies reported disruptions in the supply of raw materials and intermediate goods. These disruptions in supply chains have also led to widespread sales cancellations.

Russian air-missile attacks on the energy system of Ukraine destroyed around a half of its electricity capacities which caused power outages and blackouts. Power outages have compounded all other challenges in the economy (World Bank, 2023).

The financial security of Ukraine has been significantly impacted by macroeconomic disruptions. Factors such as increased military spending, the devaluation of the hryvnia, and rising external debt have negatively influenced the country's financial security, necessitating strategic management to stabilize the economy during and after the conflict (Zhuravka et al., 2024).

In the context of finances, the main challenges reported by 80% of Ukrainian companies are high interest rates, access to refinancing, VAT invoice blocking, and increased repayment risks (World Bank, 2023).

The ongoing war in Ukraine has also resulted in significant psychological and stress-related health effects impacting civilians, military servicemen and especially vulnerable groups such as children, elders and refugees (Maltseva, 2024).

Furthermore, the invasion war has had a severe environmental impact. Destruction of ecosystems and natural parks due to military actions, occupation and destruction of Kakhovka reservoir, contamination and degradation of soils result in long-term impact for the environment. Deterioration of air quality and contamination of water are posing serious health risks at the moment and have significant long-term consequences for human health in Ukraine (Leal Filho et al., 2024).

2.5.2. Impact of the war on the IT industry

Information and communication sectors are highly globalized and integrated sectors. IT companies are dependent on cross-border data flows and international partnerships. Therefore, geopolitical instability and consequent shifts in global investment patterns are significant challenges for these companies. Governments likely increase regulations and compliance requirements, restrictions on cross-border data transfers. Moreover, companies may potentially face increased cybersecurity threats in numbers and severity as side effects of cyber warfare (Ruta, 2022).

The physical destruction caused by military actions has damaged essential information and communication infrastructure such as data centers, telecommunication networks, and internet service providers infrastructure. These conditions during wartime also further accelerated the transition to cloud-based services and digital remote operations. As reported after the start of the invasion, 71.5% of IT companies have more than 75% of employees work remotely. The

damage to physical infrastructure has led to internet outages and disrupted the continuity of services and the reliability of internet connectivity, which are crucial for both consumers and businesses. Since October 2022 Russia has been carrying out the air missile campaign to destroy energy infrastructure of Ukraine. The prolonged power outages became a constant threat for daily war operations and delivery of projects. The most implemented measures include the acquisition of power generators and fuels, the use of power banks, diversification of internet service providers, and the use of Starlink systems (Khomenko et al., 2023).

The 2022 report from the IT Association of Ukraine highlighted that the main challenge of the war was relocation. 64% of all IT professionals in Ukraine were among those groups of people who were internally displaced or migrated abroad. Resulted "brain drain" reduced the available talent pool in Ukraine and created hiring challenges for companies to maintain specialized operations and service delivery. As a direct result of the war, a substantial 70.8% of IT companies from Ukraine were forced into unplanned relocation. Poland became the primary destination, with 40.1% of companies relocating there. Followed by destinations such as Germany with 14.6% and the USA with 9.5%. Other popular relocation destinations included Romania, Bulgaria, and the Czech Republic (IT Association of Ukraine, 2022).

The effects of the war changed the market structure and dynamics in the IT sector of Ukraine. Domestic demand for IT services had a significant drop because Ukrainian SMEs scaled down their operations and closed existing projects due to the economic impact of the war. Based on results of 2022, 43% of companies expect any growth for 2023. On the other hand, the war boosted innovations and development of conflict management technologies (Miltech) segment within the IT sector. Since 2014 the Miltech segment has grown seven times. Main areas are software for military purposes, AR/VR application for training simulators, robotics with focus on unmanned vehicles and drones. In 2022, 41 military-tech companies became part of the national ecosystem (Shvets, 2022).

Moreover, war and its effects have complicated access to international markets. International markets are the vital source of revenue for Ukrainian outsourcing and export-oriented IT companies. The increased geopolitical risks, clients' uncertainty and fears challenged the Ukrainian companies to maintain their international client relationships and contracts (World Bank, 2023).

Chapter 3. METHODOLOGY

The focus of the research on IT companies in Ukraine provides a unique opportunity to investigate a complex real-life phenomenon of how businesses adapt and maintain operations during wartime. This research employs a case study approach for understanding complex phenomena in real-life contexts. Yin (2018) suggests this approach is well-suited for cases with an emphasis on ongoing events within real-life contexts when the researcher has minimal control over these events (Yin, 2018).

The interview questionnaire is based on open-ended questions. The questions outlined in the research plan focus on understanding the processes, decisions, and strategies IT companies used to manage risks and continue operations during a highly disruptive and unpredictable period as war. Specifically, the interview questions are designed to uncover cause-effect relationships through temporal evolution of research phenomena.

In order to capture the temporal evolution of risk perceptions and business continuity strategies the structure of the interview questionnaire reflects on various phases of the conflict such as the pre-war period, military invasion, and the ongoing war periods. The chronological structure of the interview allows to monitor and analyze the dynamics of business continuity management in response to escalating conflict.

The research interview questionnaire has qualitative and quantitative components for analysis. The qualitative data analysis is organized around open-ended questions addressing different phases of crisis management. The main requirements for the open-ended questions were high relevance, direct focus and clarity in order to obtain relevant answers due to the extensive scope and time limitations during interviews.

The quantitative component is based on the elaborated Risks Significance Perception Rating Matrix. Risk significance matrix is a tool to visualize the results of risk assessments. The significance of risks is estimated by responding experts. According to Fan et al. (2024) the risk significance rating matrix is useful for researchers when it’s needed to capture subjective assessments of risk across multiple dimensions such as various risk categories and time periods.

Three-point measurement scale is used in the designed matrix in order to simplify understanding of tasks for respondents and keep the necessary level of granularity. The designed matrix has 6 risk categories and 18 risks with detailed descriptions of the risks. The

respondents rate perceived significance of various risks from 1 to 3 across three distinct periods: the pre-war period (2020-2022), the military invasion period (February - May 2022), and the ongoing war period (2022-2024).

The data collection is approached in 2 stages: quantitative data collection through the filling risk significance matrix; and qualitative data collection through the one-to-one online interview. Combining methods of quantitative and qualitative data collection for the research analysis enables the application of triangulation techniques to mitigate the biases of qualitative research with a small sample size and, therefore, enhances the robustness of the research.

Firstly, quantitative data collection is done prior to qualitative data collection in order to review the matrix scores for validation and adjust open-ended questions for clarification with the respondent if needed. Collected quantitative data will be analyzed using descriptive statistics to identify patterns in risk perception across different periods. For qualitative data collection there are applied semi-structured interviews. The semi-structured approach allows one to focus on exploration of the research objective and also provides some flexibility to elaborate related research areas of interest (Kvale & Brinkmann, 2009).

The interviews were conducted by Zoom and MS Teams video calls between May and September 2024. The duration of interviews was on average 40 min for qualitative analysis questions. The interviews were recorded, transcribed and analyzed to identify patterns and themes within qualitative data.

The main criteria for selection of interviewees was their role and participation in the BCM activities of their companies. Therefore, through the personal network of contacts there were contacted around 12 people who were responsible for the BCM in their companies. The respondents from 5 companies agreed for online call interviews with recording. Other respondents did not want to make an interview call but agreed to respond to a Google form questionnaire. However, the responses from Google form were not considered due to the incompleteness and low quality of provided information.

The defined methodology has several considerations regarding the broad set of questions and assessment of past pre-war events and experience. These considerations were addressed by the prioritizations of questions during the interviews and requesting a short follow-up interview calls after the main one to capture missing info.

Chapter 4. RESULTS AND DISCUSSION

4.1. Introduction of interviewed companies

Category	N-ix	Wix Kyiv	Mono	Turnkey Lender	Payforce
Business type	Full-cycle IT Outsourcing	Product-oriented	Product-oriented	Product-oriented	Outsourcing development
Foundation year	2002	2018	2017	2017	2018
Number of employees	1500-2000	700-800	500-600	50-100	Up to 50
Regional units or subsidiaries	Ukraine, Poland, Malta, Bulgaria, Colombia	Ukraine, Poland	Ukraine	Ukraine, USA, Malaysia	Ukraine

Table 1. Company information

Source: Author's elaboration

Company N-ix specializes in multi-industry outsourcing, software development, and IT consulting. They provide services to the industries of finance, manufacturing, logistics, retail, telecom, automotive, healthcare, energy, agritech. Main office is in Lviv (Ukraine).

Wix Kyiv focuses on cloud-based web development and support of products Wix Website Builder, Wix Online Store, Wix Blog. Wix Kyiv is in Kyiv (Ukraine). The company is an affiliate to Wix.com Ltd based in Israel.

Mono is a multi-product FinTech company that works as neobank, payment solution, digital financial service. They became first and most popular neobanking app in Ukraine. Their main products are applications monobank, Experienza, Base. Main office is in Kyiv (Ukraine).

Turnkey Lender specializes in the development of FinTech products in loan management. Their main products are "box" loan management system and configurated platform for loan portfolio risk management. Main offices are in Kharkiv (Ukraine) and Kuala Lumpur (Malaysia).

Payforce specializes in contracted development of payment gateways, online payment platforms, electronic money processing and e-wallets. Their success stories include mobile banking app for BISBANK, online payment transfer app PAY4. Main office is in Kyiv, Ukraine).

4.2. Pre-war period Management (2020-2022)

This section is dedicated for:

- Assessing efforts of companies to establish preparedness and BCM practices in the pre-war period during the COVID-19 pandemic.
- Exploring how the perception of significance of risks and threats influenced decision-making in the context of business continuity strategies before the potential war.

Topics	N-iX	Wix Kyiv	Mono	Turnkey Lender	Payforce
BCP plan for Covid-19	Yes	Yes	Yes	No	No
Frequency of BCP reviews	Quarterly, Occasional tests	Annual reviews and exercises but not specified	Quarter and annual reviews, updates and exercises	First BCP developed in 2021	N/A
BCP based on frameworks	Yes; framework not specified	Yes; framework not specified	Yes; national framework	Yes; framework not specified	No; N/A
Business challenges during the COVID-19	Transition to remote work, onboarding of new staff	Increased workload, onboarding of new staff	Transition to remote work, lack of oversight control	Transition to remote work, market uncertainty	Market uncertainty, health risks at the office
Risk impact on business strategy	High; adjusted BCP and strategy due to risk of war	Medium; adjusted BCP but not business strategy	Medium; adjusted BCP but not business strategy	High; adjusted BCP and strategy due to risk of war	Low; didn't consider war as real threat
Preparation for risks of conflict	Aid trainings, Relocation of critical roles abroad, healthchecks of facilities	Early relocation of critical roles abroad	Arranged internal relocation in Ukraine	Relocation internally and abroad, healthchecks of facilities	No collective efforts to prepare

Table 2. Results from the pre-war period

Source: Author's elaboration

For all the interviewed companies COVID-19 crisis became a surprise when the pandemic struck in early 2020. *"It caught many businesses off guard, including us in IT"*, as mentioned by the respondent from Turnkey Lender.

Some of them such as N-iX, Mono and Wix Kyiv have had formal business continuity plans, while other companies such as Turnkey Lender and Payforce didn't have any business continuity plans at the moment when COVID-19 pandemic emerged in Ukraine.

Regardless of having business continuity plans at the start, all of them stated that they were generally unprepared for the sudden disruption such as the COVID-19 pandemic. The majority of the interviewed companies quickly realized the need to develop a relevant plan or improve their business continuity plans addressing the new business environment changes brought by COVID-19 pandemic. Only Payforce did not create a formal business continuity plan documentation preferring to react depending on the situation development.

In response to the COVID-19 crisis, company N-ix developed a set of multiple Business Continuity plans for each regional and functional unit. However, these BCPs were created reactively during the early weeks of the pandemic. This was caused mostly due to client contractual requirements as the company transitioned to remote work. The primary goal of their initial BCPs was to maintain delivery at pre-pandemic levels to ensure clients get a delivery of contracted IT services. This fact reflects a focus on operational continuity.

The BCP of N-iX was structured to be a living document. The documentation got reviewed quarterly and updated in response to new escalations or crises. This flexibility allowed the company to adapt quickly to the challenges of pandemic and later to the military invasion.

Turnkey Lender emphasized that the shift to remote work was initially challenging. They used close collaboration between development, quality control, sales and project management teams. Therefore, the management had concerns about an impact on collaborative efficiency and control. In several months all teams adapted to flexible schedules and decreased the number of non-processing hours. Despite initial concerns, the measures taken in response to COVID-19 led to a spike in productivity as it allowed for better work-life balance and minimized operational disruptions. The pandemic forced the company to rethink its operational strategies, particularly concerning remote work and cloud-based infrastructure. The company decided to speed up its full transition move to cloud infrastructure. This helped to reduce the risks related to the destruction of on-premises servers at the office in Kharkiv. The transition to cloud

infrastructure eliminated a cascade of potential issues and became the best business continuity solution, as the respondent from Turnkey Lender mentioned.

As Turnkey Lender stated, *"in the end, our measures taken during the COVID-19 laid the necessary basis and proved worthy for more resilient operations during the Russian invasion of Ukraine"*.

The business continuity plan of Mono was initially designed to meet standard regulatory needs for FinTech companies in Ukraine. However, when COVID-19 struck this plan was instrumental to make a rapid shift in the operational mode to remote work. Most importantly, the plan had a risk analysis that helped to resolve challenges caused by the new way of working during COVID-19.

Before COVID-19 the Mono's internal approval process of documentation was based on paperwork on several levels. Therefore, the BCM of Mono have had big concerns about efficiency and productivity of many teams that depend on the waterfall approval process. The identified risks allowed management to quickly allocate resources, so the development department developed a native electronic document management system for the company. This electronic document management system became a key technology tool for the company to maintain productivity and efficiency in end-to-end flows. This developed system became even more valuable during the wartime conditions when teams became even more distributed geographically.

The representative of Mono summarized that the transition to remote work as part of business continuity was difficult but it revealed the potential for significant cost savings by reducing reliance on physical assets such as office equipment and space. Moreover, the pandemic experience taught the company's workforce how to be highly mobile and capable of delivering results remotely that would have proved crucial when the war began.

Across different companies, the assessment of the risk of military invasion and perception of its threat varied significantly. This influenced the level of preparedness and planning for crisis management before the potential invasion. Respondents from N-iX, Wix Kyiv, Mono, Turnkey Lender stated that the risk of military invasion and the posed threat were taken seriously with highest level of attention. However, as Mono recalled "the risk of war was not publicly acknowledged by authorities, so it wasn't officially factored into our planning". At that time the government was making assurances that the risk of invasion was overestimated, and military conflict was unlikely. Therefore, some organizations such as Payforce decided not

to consider the risks of invasion as a real threat. Despite official assurances, Turnkey Lender highlighted that for them the main driver to take these risks seriously has been the geographical location of the main office in Kharkiv and cross-border witnesses of gathering of Russian troops. Kharkiv is Ukraine's second most populated city that is just in 30 km distance from the Russian border. The respondent from Mono stated that the earlier experience of the war since 2014 created the "gut-feeling" that risk of full-scale invasion should be taken seriously.

Across all interviewed companies, the safety of key team personnel and the continuity of core business operations were defined as the top priorities. Wix Kyiv had relocated key personnel to Poland along with their families by early February 2022. By mid-February, they offered relocation to Turkey for any employee who wished to leave. N-ix started preparing its affiliate units in Poland, Bulgaria, and Romania for the relocation of key employees from Ukraine at the end of 2021. Mono decided to relocate teams internally within Ukraine and defined Western Ukraine as the main relocation destination because of the distance from Russia.

Turnkey Lender prioritized the elaboration of a comprehensive business continuity plan as their takeaway from the pandemic experience. *"The pandemic indeed made us more resilient. We started sensing the threat of war around the end of 2021. Despite official assurances that conflict was unlikely, we decided to take proactive measures",* as stated by Turnkey Lender respondent. The company has also put the main effort into the early relocation of employees with critical roles such as product management, senior development architects, and team leads to Poland by opening an office in Warsaw. Also, the company supported the relocation of family members. The relocations created a pull of available team resources for the backup during the first after the invasion.

Thus, relocating human resources became a key element in the business continuity strategy. However, most employees, even with critical roles, decided not to relocate in anticipation of the invasion. This was a similar attitude among their employees across all interviewed companies.

Despite relocation efforts, some companies including Mono concluded several automation projects and increased the level of automated processes in order to improve autonomy of the system and reduce reliance on human presence. All-hands meetings were conducted by N-iX in order to clearly communicate all of the risks and preparations. Moreover, the company provided training about first aid and survival skills for all employees to increase personal preparedness level.

In contrast, Payforce showed little collective prioritization of business continuity planning before the potential invasion. *"Surprisingly, there wasn't much of a collective effort to prepare for the possibility of invasion and war. We all prepared individually, some more than others, but the company didn't hold any meetings or planning sessions to address the potential threat. Our top management was simply hoping that the Russia would not attack, and the war was unlikely"*, said respondent from Payforce. This lack of formal planning meant that individual employees had to take responsibility for their own risk assessment and preparations.

4.3. Military Invasion Emergency Period Management (February - May 2022)

This section is dedicated to:

- Understanding how the companies initially responded to the crisis of the military invasion.
- Understanding how the companies managed unique risks and threats posed by the breakout of military conflict.

Topics	**N-iX**	**Wix Kyiv**	**Mono**	**Turnkey Lender**	**Payforce**
Reaction to the military invasion	Uncertainty, sustaining critical activities while teams relocating	Psychological impact, drop in productivity of relocated staff	Shock, relocation of staff from combat zones	Relocation from combat zone, sustain critical work	Confusion shock, relocation from combat zones
Established crisis management team	Yes, board, HR team and team leads	Yes, HR team and BCP coordinators in the teams	Yes, board members and team leads	Yes, regional director and HR team	No
BCP plan for the risk of military invasion	Specifically created	Adapted from earlier BCP	Adapted from earlier BCP	Specifically created	Not created
Communication channels with stakeholders	Emails, Slack, SMS	Meta Workplace, Zoom, email	Viber, Telegram, Zoom	Telegram, phone, MS Teams	Telegram, phone, Zoom
Cooperation with organizations	Municipal authorities, volunteers	NGOs, volunteers	Local authorities, volunteers	Local and UAF authorities	Volunteers

Table 3. Results from the military invasion period

Source: Author's elaboration

The breakout of military conflict in Ukraine in February 2022 thrust organizations into an unforeseen emergency that demanded rapid and decisive responses. Companies had to navigate immediate risks while ensuring the safety of employees and continuity of business operations.

At Payforce, there was a lot of confusion during the first days of the invasion. Employees scattered to various locations to ensure personal safety. The company's director reached out to the teams on the next day to quickly advise everyone to work remotely and be safe. However, there was no coordinated relocation, no defined relocation facilities or comprehensive work arrangements in place. The lack of a plan caused stress and fully disrupted operations for about one or two weeks, as recalled respondent from Payforce.

The response of Mono was more structured as it was based on its updated BCP developed during the pandemic. The established BCM team was put in charge on the same day of invasion. The BCM team made preemptive arrangements for relocation accommodations in Western Ukraine and closely collaborated with local volunteers. Despite the chaos of the first days, the company organized the transportation of staff. Thus, during the first weeks there were enabled back-ups for senior roles, relocated staff from high-risk areas and transitioned to online operations. Overall, the respondent concluded that implementation of these efforts minimized operational disruption during the first period of the war. However, during this period the company's revenue was significantly reduced. This caused them to take decisions like encouraging unpaid leave to avoid layoffs and ensure business continuity and workforce sustainability.

The crisis management team, consisting of board members and key department heads, made critical decisions about business continuity, while contingency planning designated backups in case senior management became incapacitated.

In the initial weeks of invasion, N-iX was similarly focused on relocation and employee support. The company relocated staff from high-risk areas in Ukraine and offered financial assistance to help employees transition. They also converted offices into temporary residence shelters for refugees and employees from Eastern Ukraine and their families. This comprehensive approach to physical safety and financial security underscored the company's dedication to maintaining morale and operational stability.

At Turnkey Lender the first reaction to the invasion was to prioritize the safety of staff as 70% of the company workforce were in high-risk areas like Kharkiv when the invasion started. Prior to the invasion, the crisis management team had drawn the evacuation route for company

employees and made arrangements with transportation company for evacuation from Kharkiv to the city of Dnipro in central Ukraine. This city was defined as the staging place for the first phase of relocation. On the next phase many female employees relocated to Poland where there was company office and other team members were dispersed all over Ukraine. In the early weeks of the invasion all operations slowed with only 10-20% of the workforce available, mostly those who were already abroad. Turnkey Lender stated that the pre-existing crisis management plan with pre-arrangements played a key role in saving the team, managing client relationships and maintaining business continuity.

At Wix.com around 50% of employees from Ukraine were already relocated to Poland and Turkey in anticipation of the invasion. However, as the respondent from Wix Kyiv recalled, the psychological impact of the invasion was significant for all employees, including those working remotely. The initial weeks were marked by shock and anxiety. Many employees were unable to work effectively despite being in physically safe locations. Thus, in addition to financial assistance and relocation support, the company placed a strong emphasis on employee wellness and mental health. There were made available therapy sessions with psychologists

The company's support systems, including financial assistance, relocation services, and mental health resources, proved crucial. This support helped employees adapt more quickly, although the initial weeks remained challenging. Wix Kyiv also had to pivot quickly as the conflict forced the company to withdraw from the Russian market, compelling employees to learn new markets and procedures under extreme stress.

Companies that had made some preparations for crises were overall better positioned to handle the immediate aftermath. The responses to emergencies demonstrate that the crisis management demanded rapid adaptation and flexibility.

During the initial stages of the military invasion BCM communication was critical for coordinating relocation, maintaining morale, internal cohesion and manageability. In its communication strategy Payforce relied on digital tools like WhatsApp, Viber, and Skype to communicate with stakeholders, including employees, clients, and partners. However, there were no all-hands meetings. The company had little experience of remote work and online communications before the invasion. Thus, it was difficult for managers to effectively track employee activities during this shift. The effect was additional stress and timeout for the company during this period.

For other interviewed companies (Mono, N-iX, Wix Kyiv, Turnkey Lender) there was seamless shift to remote work and online communication because all of them were already operating in this mode since COVID-19.

Mainly the companies changed their approaches in the communication with employees and added additional communication back-up channels. Mono decided to use Viber, Telegram, and Zoom as primary tools for immediate BCM communication. This ensured constant coordination and instant connection with staff. During this period, BCM communication at N-iX, as characterized by the respondent, became more direct, straightforward, and much more frequent. The main communication channels for BCM were work Slack, emails and SMSs. These communication tools have a lower rate of feedback and proliferation, so the company needed to increase the frequency of communication. During the first period all-hands meetings were dismissed because of the emergency state and their limited efficiency. N-iX concluded that the communication strategy during the crisis achieved its goals to keep employees informed and ensure swift responses to any emerging needs. This focus on clear, regular communication helped maintain a sense of normalcy and structure. Both Turnkey Lender and Wix Kyiv also implemented shorter and more frequent BCM communication. Turnkey Lender established regular all-hands company meetings with CEO and top management to communicate company's strategic direction and financial state of the company as well as to make for direct Q&A and introduced sessions with psychologists to support employees. Wix Kyiv stated the role of corporative communication policy. The company used Meta Workplace, Zoom and emails as the principal BCM communication channels in order to comply with the policy.

All respondents underscored that successful BCM communication must be clear, concise, and have frequent updates. They agreed that BCM communication is a key instrument to maintain employee morale and business operations during the most critical emergency period. Companies that adapted quickly to more digital communication channels were better able to manage the crisis.

4.4. Ongoing War Period Management (May 2022 - May 2024)

This section is dedicated to:

- Analyzing BCM processes of the companies during the ongoing war period.
- Understanding of the new business environment created by the war conditions.

Topics	N-iX	Wix Kyiv	Mono	Turnkey Lender	Payforce
Timeline of Business Recovery	3 months for partial recovery	Gradual recovery for 2-3 months	Partially recovered in 2 months	3 months to reach 80%, full recovery in 6 months	4 months to recover
Reasons of business disruptions	Employee relocation, Power outages, internet issues	Employee mental health, Power outages, internet issues	Cyberattacks, Power outages, layoffs	Employee relocation, Power outage, internet issues, layoffs	Power outage, internet issues, equipment damage
Most impacted operations	Sales, business development, client relations, project delivery	Customer support, project delivery	Marketing, business development	Sales, project development and delivery	Software development, project delivery
Regulatory challenges	Martial law restrictions and mobilization	Transport restrictions	New financial regulations and restrictions	Martial law restrictions and mobilization	Martial law restrictions and mobilization
Most useful technology in BCM	AI, remote work and collaboration tools	Backup power solutions, cloud	Native e-document management system	Cloud technologies, power storage	Remote work and collaboration tools

Table 4. Results from the ongoing war period

Source: Author’s elaboration

As the war continued, companies faced prolonged challenges, including business restructuring, power outages, employee displacement, shifting client demands, cost-cutting and layoffs. All companies concluded that during the first period of war their main strategy was to survive and recover.

Directly after the invasion many companies who have had business relations with clients and companies from Russia and Belarus decided to leave these markets and close the ongoing projects. The main reasons were ethical code and reputation, employees' boycott, financial and technological sanctions. Among companies that had to restructure their market presence were Payforce and Wix Kyiv. Payforce had a big client from Belarus that represented around 15% of company operations. The project with this client had to be closed due to the employees' boycott because of Belarussian support of the invasion. In its turn, Wix Kyiv took decision to stop services for Russian market after the invasion. However, the business impact of this decision was minimal due to the small customer share in the market.

The martial law in Ukraine has been the main factor that shaped business environment for N-iX as IT outsourcing and outstaffing company. One of the primary concerns was the restriction on male employees from traveling abroad due to military mobilization laws. This posed significant challenges in meeting client requirements that necessitated on-site visits. To mitigate this, N-iX relied on consultants from neighboring countries and occasionally subcontracted firms from the European Union. This approach increased operational costs per man-hour. Despite these challenges, the company maintained operational stability by leveraging its distributed workforce. N-iX stated that recovery time to pre-war level of operations took approximately 3 months.

By May 2022, Payforce commanded a return to the office for employees with the ultimatum to either return or leave the company. While this move was controversial, only one employee decided to not return to the company. The respondent from Payforce stated that it helped restore operational efficiency till the end of June 2022 and the time for recovery to pre-war level took around 4 months. Payforce managed to recover because of the intensive work of sales and project delivery teams. The key factor for recovery was consolidation of workforce.

Nonetheless, power outages and infrastructure instability continued to pose challenges. The company quickly invested in backup solutions like personal generators and Starlink for internet connectivity, enabling them to adapt to ongoing disruptions. The staff's adaptability played a

crucial role in the company's survival, highlighting the importance of workforce resilience in crisis management.

Due to the long-term impact of the war on financial activities, ono decided to reevaluate its initial BCM strategy. As a result of the BCM review, they had cut non-essential expenses and set a focus on critical services for their business, like products for housing loans and clearance. Also, the company continued investing in IT infrastructure and cybersecurity to ensure business continuity. Mono relocated servers and data centre abroad and continuously updated its risk assessment processes to manage potential future crises. Since September 2022 Mono faced increased cyber threats and several huge DDoS attacks from Russian hacker groups. The BCM of Mono emphasized the importance of strong cybersecurity capabilities within the company. These capabilities protected the company´s digital infrastructure and continuity of the core business processes. Overall, the recovery time for Mono took approximately 5 months since the invasion.

For Turnkey Lender the main problem during the recovery of operations was the loss of competitiveness due to factors of increased development backlog, lack of senior workforce during this period and therefore delayed product releases during 2022. By May 2022, Turnkey Lender had resumed 80% of its pre-war operations and within six months after the invasion, the company had returned to full capacity despite initial problems with the loss of competitiveness. For Turnkey Lender the idea of prolonged conflict became a "new normal." Thus, Turnkey Lender shifted its business strategy focus to work with more mature FinTech clients. This caused adjustments in the business model as the development and project delivery cycles became longer with bigger scope.

The ongoing war and its consequences as well as the changing business environment forced N-iX to continuously adapt its BCM strategy. The company started to search for more contract opportunities all-around the world

Since September 2022 Russia launched the series of missile attacks to destroy the electric power generation system of Ukraine. As a result, there were started deficit of electricity and heat, prolonged power and internet outages. To address these critical problems the interviewed companies took two main approaches. Firstly, companies who had foreign offices redistributed operations and used the foreign offices as back-up centers. This was applied by N-iX, Wix.com and Turnkey Lender. For example, Turnkey Lender stated that company relocated abroad over

50% of its employees This helped to reduce the impact of the war on daily operations during the period of power outage in Ukraine.

Secondly, all the companies organized “work continuity hubs” in their offices in Ukraine by purchasing electric generators, big power banks, reserve electric stations for internet commuters, Starlink terminal internet connection. The companies who didn’t have foreign offices like put high priority for this approach N-iX and Turnkey Lender incentivized and even financed employees to buy generators, power banks (such as EcoFlow system) and Starlink terminal for the home offices because many employees were too far away from the hubs.

Overall, the power outage crisis made a significant impact on project deadlines and consequently on reputation. However, every respondent noted that amid this crisis they expected a much worse situation and more serious impact due to the power outages. They managed overcame that dire crisis of autumn and winter 2022-2023 due to the flexibility of their employees who prioritized the work and worked whenever there was available power, support from government authorities who deployed the network of hubs with constant power and internet in every town in Ukraine and loyalty of clients who understood the situation.

4.5. Quantitative analysis of Risk Significance Perception Matrix

Quantitative analysis results are based on the Risk Significance Perception Matrix fulfilled by the respondents in the first part of interviews. Risks in the matrix have detailed description and definition of scope to ensure quality of responses. The matrix is presented in the annexes with aggregated raw data from the 5 interviewed companies.

After the aggregation into a table, the data was normalized by obtaining the average mean score of risk significance. The normalization was done to get the same scale of values for the risk categories and companies’ data. The purpose is to track evolution of how companies perceive risks significance throughout the crises and to identify patterns in risk management and adaptation across companies. The analysis in this chapter provides valuable insights about risk significance trends and helps to prioritize resources and efforts toward areas of greater risks or vulnerability. Understanding these aspects will improve future risk management and consequently BCM.

The full set of collected data per company cannot be represented in this chapter due to the page limits of the work. Therefore, in this chapter we present key takeaways from the quantitative analysis.

Risk Category	Pre-war period (2020-2022)	Military Invasion period (Feb - May 2022)	Ongoing war period (2022-2024)
Physical Security Risks	1.3	2.9	2.6
Operational Risks	1.3	2.2	1.9
Human Resources Risks	1.3	2.3	2.5
Cybersecurity Risks	1.3	1.9	1.6
Commercial Risks	1.5	2.5	2.5
Legal and Compliance Risks	1.3	1.9	1.9

Table 5. Average values of Risk category perception across the research periods

Source: Author's elaboration

During the pre-war period, most risks across categories were perceived within the lower tier. This reflected slightly increased risks than normally in the overall stable environment.

The military invasion period marked a sharp increase in the perception of risks, particularly Physical Security, Commercial Risks, Human Resources. The companies characterized this period with high sensitivity to all risks and survival challenges for the organizations and employees.

The top risks underscored by all companies were Employee Safety (3), Damage to Facilities (2.8) (both risks belong to the Physical Security Risks category), Employee morale (2.8) (Human Resources Risks), Market Uncertainty (2.8), Financial Instability (2.8) (both risks belong to the Commercial Risks category), and Regulatory Changes (2.8) (Legal and Compliance Risks).

Risk for employee safety had the highest significance perception, at 3 points across all risks during the military invasion period. As there were taken safety measures and many people relocated from dangerous zones the perception of risks from Physical Security Risks decreased after the first period of the full-scale war. Thus, Employee Safety risk decreased to 2.6 during

the ongoing war period. The same trend was with the risk of Damage to Facilities which also decreased to 2.6. The risks from categories as Commercials risks and Legal & Compliance risks remained on the same high level (2.8) of the significance across the periods during the war. The Human Resource risk related to Employee morale has shown an increase in its significance across the period during the war from 2.8 to 3 and became the risk with highest significance perception in the ongoing war period. Another risk that showed a drastic increase from 1.4 to 2.4 in significance during the ongoing war period was the risk of Staffing Shortages. This is explained by the fact that all interviewed that all companies froze hiring during the invasion. However, the risks arose in significance because of the drain of relocated specialists to other European markets. Thus, only the risks from Human Resources which highlight the importance of human resources during the severe long-term crises.

The bottom risk identified by all companies were Intellectual Property risks (Legal and Compliance Risks category) and Vendor Reliability (Operational risks). The significance of risk with Vendor Reliability decreased throughout the ongoing war period from 1.4 to 1.2. This suggests that companies became more effective and confident in managing vendor relationships by cutting off unnecessary vendor services such as Mono and N-iX indicated in the interviews. The significance of risk of Intellectual Property risk was perceived as the lowest score 1 during all three periods of time, indicating that companies feel confident about their software Intellectual Property.

Company	**Pre-war period (2020-2022)**	**Military Invasion period (Feb - May 2022)**	**In-war period (2022-2024)**
N-ix	1.4	2.1	2.2
Wix Kyiv	1	1.8	1.9
Mono	1.1	2.1	2.3
Turnkey Lender	1.1	2.6	2.2
Payforce	1.6	2.4	2.2

Table 6. Average values of risk perception by companies during the research periods

Source: Author's elaboration

All companies show the same trend of significant increase (from 0.7 to 1.5) in their risk perception from the pre-war period into the military invasion period. During the pre-war period Payforce had the highest risk perception because the teams had to work from the office which

increased the risks overall as indicated by the respondent from Payforce. Turnkey Lender had the highest increase from 1.1 (Pre-war) to 2.6 (Military Invasion) which also became the highest perception risk during the military invasion period among the companies. The respondent from Turnkey Lender explained this high perception of risks on their side was due to the company location in Kharkiv in 30 km from the border with Russia. On the day of the invasion, combat actions in the city started almost immediately. So, their top management had to initiate BCP crisis response in the very dangerous conditions. The second highest risk perception was at Payforce with also a notable rise from 1.6 to 2.4. The Payforce respondent highlighted that this is the result of lack of BCM planning, preparedness and communication.

By analyzing these data, there can be distinguished two groups of companies. The first group that included Payforce and Turnkey Lender showed a jump with highest scores of the risk perception during the invasion. This correlates with the high sensitivity of these companies to the rapidly escalated conditions of the first period war due to several different reasons. Later both companies mitigated immediate threats and stabilized their situations which were also reflected in the risk perception values during the ongoing war period.

The second group, that includes N-iX, Wix Kyiv, Mono, represents the companies with established BCM practices and teams, more resources or better logistics for emergency response. This group has shown gradual This pattern can be attributed to the more mature approach to BCM within these companies.

Overall, in the current period all interviewed companies have very close values of the risks' perception which shows that all of them completed adaptation to the new business environment during the war and they similarly perceive and assess the indicated risks in the current period.

Chapter 5. CONCLUSIONS

5.1. Preparedness of the IT companies from Ukraine and implementation of BCM strategies

This sub-chapter concludes the first research objective and its corresponding research questions to examine preparedness of the IT companies from Ukraine and implementation of BCM strategies.

The results of research show different levels of preparedness among the Ukrainian IT companies before the war. There were identified two groups of companies: one with a higher level and one with a lower level of preparedness. This division across companies has been mainly influenced by company size, available resources, requirements from clients, and prior business continuity management experience.

In the pre-war period during the COVID-19 pandemic, more proactive companies like N-iX, Mono, and Wix Kyiv had developed formal BCPs and implemented comprehensive BCM strategies. As a result, they were better positioned to meet potential military invasion. The implementation of BCM strategies included risk assessments, regular BCP reviews, facilities preparations, preemptive relocations of legal entities and critical roles, and deployment of employee support systems. The results highlighted that such preemptive measures significantly contributed to higher levels of preparedness to the wartime conditions

Research literature presents BCM as “a holistic management process” (Herbane, 2010). This corresponds with the BCM implementation demonstrated by the companies’ mature BCM teams. This included development of comprehensive BCP plans for each regional and functional unit during the pre-war period. Later these plans became the foundation for the BCP to respond to the invasion and then were adjusted during the ongoing war.

The key takeaway is that the companies with the pre-existing plans, even if the BCPs were designed for different crises like COVID-19 pandemic, were better prepared to navigate the most challenging first period of the war.

The sudden military invasion in February 2022 caused shock and uncertainty among all companies. However, companies that had already developed BCM plans were able to quickly deploy the crisis management teams and respond to the emergency. In contrary, the companies that deprioritized risks of potential invasion faced greater disruption during

The main strategy consisted of relocation from the war zones to safer areas and ensuring backup and continuity of critical business processes. Companies with already established foreign offices have chosen the main relocation direction abroad as a more stable place for future operations.

In this context, companies that arranged early relocation of critical staff faced minimal disruptions as the relocated employees took the workload of people who were relocating from the war zone. However, despite safety and relatively stable environments, relocated offices faced challenges with adaptation, psychological impact of the war on relocated staff and later drain of specialists to the local markets. Due to the general uncertainty and relocation process, companies had to prioritize the critical business process and restructure businesses due to market changes before getting the clear strategy vision for the future. 3 out of 5 companies decided to restructure their businesses and cut off some projects. The BCM research of Păunescu (2017) confirms these actions as the first priority of BCM to protect all critical business functions, even during crises.

The outbreak of military invasion acted as a catalyst to accelerate implementation of robust BCM strategies among all companies operating in Ukraine. During the ongoing war period all companies have been handling BCM as an evolving process that adapts to the emerging risks and threats from the new and highly volatile operational environment. Some companies were investing further into remote work capabilities while others were ensuring work in the relocated offices. Despite these adaptations, the ongoing war period continued to challenge traditional BCM frameworks, as highlighted in the research by Obłój and Voronovska (2024). This became evidently after Russian mis strikes destroyed most of power generation capacities in Ukraine, so all organizations faced the same threat of operational disruptions. Companies were experimenting in their own optimal way to adapt to the new threat and challenges. Some decided to supply employees with power and internet back-up equipment while others focused on establishing work hub shelters with secured power and internet facilities.

The new wartime environment and constantly emerging new threats posed by Russia's war require companies to adopt more flexible, agile, and employee-centered BCM strategies as also stated by the aforementioned research.

5.2. Evolution of risk perception and main challenges in BCM

This sub-chapter concludes the second research objective and its corresponding research questions to identify the main challenges in BCM and analyze evolution of risk perception across the pre-war, military invasion, and ongoing war periods.

The evolution of risk significance across the pre-war, military invasion, and ongoing war periods reflects the dynamic nature of adaptation to the new business environment in the wartime conditions.

During the pre-war period, the perception of significance of all risks was generally low. The risks were considered manageable, and companies focused on growth opportunity during the pandemic digital transition boom. The COVID-19 pandemic prompted companies to reevaluate their management and develop BCPs due to corporation policy, client or national regulatory requirements. Later, the companies that with already existing plans showed less sensitivity to the future risks and more stability to the crisis emergency during the first period of the full-scale war.

The increasing threat of a military invasion was not universally acknowledged by some organizations while others were taking seriously the risk of military invasion. This disparity in risk perception was partly influenced by governmental assurances that the likelihood of an invasion was low. Thus, the underestimation of the risks posed by war became initially one of the main challenges faced by Ukrainian IT companies for their preparedness.

The military invasion in February 2022 marked a sharp increase in the perception of risk related to employee safety, physical security of facilities, employees' morale, and mental health, as well as risks related to market uncertainty, financial instability, and regulatory changes of the martial law. This period was characterized by immediate safety challenges for employees' survival and the challenges with continuity of critical business processes for companies' survival. In response to the elevated risks, organizations adapted their BCM strategies to the new realities. This corresponds to Torabi (2016) that BCM must be flexible and adaptable based on its risk management as a core component.

Key challenges during the first period of war included employee safety and the relocation process, maintaining critical operations while the employees are out of the work, restructuring of the business due to the closure of projects and economic uncertainties of war.

As the military invasion turned into prolonged war, IT companies faced prolonged disruptions of their operations due power outages, cybersecurity threats, psychological impact on employees, staff shortages, increased economic and financial risks.

Therefore, the significance of corresponding risks increased for the companies and the overall risk environment remains in the high tier. The results from the ongoing war period show that increased significance of risks related to employee morale, market uncertainty, financial instability and regulatory changes due to martial law. However, there were no sharp spikes as before and some risks slightly decreased due to the mitigation measures that were taken. This indicates the stabilization of companies' risk management as all companies put similar scores during the ongoing war period. The results also showed consistently low perceptions of certain risks, such as intellectual property and vendor reliability. This suggests that companies have had control over these risks and therefore there is an opportunity to redirect available resources to more acute risks. Thus, we can conclude that the companies made their successful adaptations to the new business environment created by the wartime conditions.

Overall, the key challenges in maintaining business continuity have been identified as operational disruption due to power and internet outages, risks to employee safety and mental health, commercial challenges (decrease in sales and revenues) due market uncertainty and financial instability, mobility and financial restrictions defined by martial law state.

Despite experienced and ongoing challenges, Ukrainian IT companies have developed robust BCM strategies that highlight the critical role of flexible workforce management, leadership, support communication strategies, resilient infrastructures and technologies.

5.3. Effectiveness of BCM strategies and key factors for successful BCM

This sub-chapter concludes the third research objective and its corresponding research questions to analyze the effectiveness of BCM strategies and determine key factors for successful BCM.

Overall, the respondents concluded that all applied BCM strategies have been effective in ensuring business continuity throughout the time in their contexts. However, it is hard to measure the efficiency of those strategies and practices due to the work conditions in the context of war.

The key universal factors to define effectiveness of BCM strategies were speed and availability of resources. For example, speed and timeliness of actions which also depended on organizational structure, and available resources of the companies played crucial role for Turnkey Lender teams' evacuation from Kharkiv during the first days of the invasion. A similar conclusion can be attributed to the quick activation of crisis response of N-iX and Wix Kyiv which has been the consequence of preemptive and timely measures such as planning and early relocation of critical roles.

The most proven and effective BCM strategy became relocation of employees to safe and stable places to work. This strategy shows its human-centric focus to preserve human resources to continue business operations.

The remote work and distributed team approaches are crucial parts for successful implementation of BCM strategy as they complement the relocation approach. However, remote work is less effective if there was no prior experience to work in this mode. Moreover, remote work has shown its vulnerability during the power and internet outages as many people could not logistically ensure access to electricity or internet.

As highlighted in the research by Russo (2024), effective BCM must leverage technology solutions to enhance its recovery capabilities and resilience. All interviewed companies were actively using technologies during the crises. All respondents noted the critical role of technology in operational resilience during blackouts and power outages. The most useful technologies were long-term power stores like EcoFlow and satellite internet terminals like Starlink. Even the less advanced tools such as portable power generators made significant contributions to maintain continuity at home and work offices. Also, the respondents highlight the importance of cloud-based infrastructure, tools for remote work and collaboration. Additionally, notable examples were Mono and N-iX technology investment into internal technology capabilities.

Also, the necessary components for successful BCM strategy are leadership, communication and employee morale. The focus on leadership and regular communication during crises, as discussed by Opatska et al. (2024) ensured the needed flexibility and manageability. Moreover, the leadership during the crisis is the critical aspect of maintaining employee morale in the team. These aspects were reflected by N-iX's and Mono's approaches to leadership during the war. Both companies held regular all-hands meetings to maintain morale and provide direct and transparent communication.

The researchers in BCM highlight the importance of employee welfare and psychological support as part of BCM strategy during wartime (Borowska-Pietrzak & Stoian, 2023). Both literature research and empirical results underscore the need for adaptable, human-centered BCM strategies that prioritize both operational resilience and employee well-being in the face of prolonged disruptions such as long-term war. The gap in understanding the psychological impact of the war on daily life, work and mental health of employees was highlighted as one of the major gaps.

The main gaps that were identified by empirical data are underestimation of risks prior to the invasion, overoptimistic recovery targets in the pre-existing BCPs, unrealistic recovery planning, lack of understanding of psychological impact of the war on relocated teams, unreasonable use of resources in the early period of war.

The key attributes of effective BCM strategies were indicated as comprehensive planning, teamwork and interoperability, flexible leadership, timely decision-making, regular and transparent communication, investments into backup tools and technologies.

5.4. Limitations and suggestions for further research

The research faces several limitations that may affect the precision of its findings. The nature qualitative research introduces potential biases related to the subjective experiences of respondents which may not capture the fully objective picture of situation development. This limitation was addressed by applying triangulation techniques to mitigate the influence of bias and there was introduced a quantitative analysis part of the research to balance the biases of qualitative analysis. However, this analysis faces the limitations of small sample size of the respondents of IT companies from Ukraine. The small sample size impacts both qualitative and quantitative analyses. Finally, the dynamic nature of the conflict impacted the real-time data collection and the absence of comprehensive metrics for quantitative which limit the potential of collected data.

The research offers valuable contributions to the field of Business Continuity Management in the context of unique war-induced situation in the IT industry. The research can be further enhanced by increasing the sample size of respondents and by collecting the data from media such as the published interviews of Ukrainian businesses owners by trusted business magazine publishers such as Harvard Business Review, The Economist, Wired, etc.

BIBLIOGRAPHIC REFERENCES

AXELOS. (2019). *ITIL Foundation: ITIL 4 edition*. The Stationery Office.

Bai, S., & Yelisieiev, V. (2023). Enterprise management: wartime challenges. *SCIENTIA FRUCTUOSA, 152*(6), 64–78. https://doi.org/10.31617/1.2023(152)05

Boh, W., Constantinides, P., Padmanabhan, B., & Viswanathan, S. (2023). Building Digital Resilience Against Major Shocks. MIS Quarterly, 47(1), 343-360. Article 1. https://misq.umn.edu/contents-47-1

Borowska-Pietrzak, A., & Stoian, K. (2023). Changes in the structure of the CSR strategy of companies in the context of Russia's military invasion of Ukraine in 2022. *Scientific Papers of Silesian University of Technology. Organization and Management Series, 2023*(178), 127–147. https://doi.org/10.29119/1641-3466.2023.178.7

Cedergren, A., & Hassel, H. (2024). Building organizational adaptive capacity in the face of crisis: Insights from the COVID-19 pandemic. *International Journal of Disaster Risk Reduction, 86*, Article 104235. https://doi.org/10.1016/j.ijdrr.2023.104235

Chen, G., & Hu, K.-J. (2009). Grid-based business continuity management mechanism of e-business. In *2009 International Conference on E-Business and Information System Security* (pp. 1-4). IEEE. https://doi.org/10.1109/EBISS.2009.5137991

CMMI Institute. (2018). *CMMI V2.0: Capability Maturity Model Integration*. ISACA. https://doi.org/10.1016/9780128052217

Fan, C., Montewka, J., Zhang D., Han Z. (2024). *A framework for risk matrix design: A case of MASS navigation risk.* Accident Analysis & Prevention, 199:107515-107515. doi: 10.1016/j.aap.2024.107515

DeCarlo, C., & Goodman, P. (2022). *Ukraine's role in global chipmaking disrupted by war*. Semiconductor Industry Journal, 12(1), 35-42.

Henriquez, V., Moreno, A. M., Calvo-Manzano, J. A., & San Feliu, T. S. (2021). Agile–CMMI alignment: Contributions and to-dos for organizations. *Computer, 54*(12), 38-49. https://doi.org/10.1109/MC.2020.3039105

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History, 52*(6), 978-1002. https://doi.org/10.1080/00076791.2010.511185

Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business Continuity Management: time for a strategic role? *Long Range Planning, 37*(5), 435–457. https://doi.org/10.1016/j.lrp.2004.07.011

HIIK. (2023). Conflict barometer. Germany: Heidelberg Institute for International Conflict Research. https://hiik.de/conflict-barometer/current-version/?lang=en

ILO. (2022). *The impact of the Ukraine crisis on the world of work: initial assessments*. Switzerland: ILO. https://researchrepository.ilo.org/esploro/outputs/encyclopediaEntry/The-impact-of-the-Ukraine-crisis/995219123402676

International Organization for Standardization. (2011). *ISO/DIS 22313:2011 Societal security — Business continuity management systems — Guidance*. Switzerland: ISO.

International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements* (2nd ed.). Switzerland: ISO.

International Organization for Standardization. (2021). *ISO 22300:2021 Security and resilience — Vocabulary* (3rd ed.). Switzerland: ISO.

ISACA. (2018). *COBIT 2019 framework—Governance and management objectives*. USA: ISACA.

IT Association of Ukraine. (2020). *Annual report 2020*. IT Ukraine Association. https://itukraine.org.ua/en/report/annual-report-of-the-association-it-ukraine-2020/

IT Association of Ukraine. (2021). *Annual report 2021*. IT Ukraine Association. https://itukraine.org.ua/en/report/annual-report-of-the-association-it-ukraine-2021/

IT Association of Ukraine. (2022). *Annual report 2022*. IT Ukraine Association. https://itukraine.org.ua/en/report/annual-report-of-the-association-it-ukraine/

IT Ukraine Association. (2023). *Digital Tiger: The Power of Ukrainian IT – 2023*. IT Ukraine Association. https://itukraine.org.ua/en/digital-tiger-the-power-of-ukrainian-it-2023

Khomenko, I., & Khomenko O. (2023). Peculiarities of the IT industry in Ukraine: current state and development prospects. *Problems and Prospects of Economics and Management*, (34), 143–153. https://doi.org/10.25140/2411-5215-2023-2(34)-143-153

Kostruba, A. (2024). Managing foreign business operations in Ukraine in the context of war. *Business Horizons*. https://doi.org/10.1016/j.bushor.2024.01.003

Kvale, S., & Brinkmann, S. (2009). *InterViews: Learning the Craft of Qualitative Research Interviewing* (2nd ed.). SAGE Publications.

Leal Filho, W., Eustachio, J., Fedoruk, M., & Lisovska, T. (2024). War in Ukraine: an overview of environmental impacts and consequences for human health. *Frontiers in Sustainable Resource Management, 3*. https://doi.org/10.3389/fsrma.2024.1423444

Maltseva K. (2024). Stress exposure, perceived stress, protective psychosocial factors, and health status in Ukraine after the full-scale invasion. *Journal of Health Psychology*, 13591053241259728. Advanced online publication. https://doi.org/10.1177/13591053241259728

Melnyk T., & Zavhorodnya E. (2022). The IT sector of Ukraine on the world market: *Foreign trade: economics, finance, law*, 125(6), 17–36. https://doi.org/10.31617/3.2022(125)02

Ministry of Foreign Affairs of Ukraine. 10 facts you should know about Russian military aggression against Ukraine. (2019, December 19). *Ministry of Foreign Affairs of Ukraine*. https://mfa.gov.ua/en/countering-russias-agression/10-facts-you-should-know-about-russian-military-aggression-against-ukraine

NFPA 1600. (2019). *NFPA 1600® Standard on Continuity, Emergency, and Crisis Management*. USA: National Fire Protection Association.

Obłój, K., & Voronovska, R. (2024). How business pivots during a war: Lessons from Ukrainian companies' responses to crisis. *Business Horizons*. https://doi.org/10.1016/j.bushor.2023.09.001

Opatska, S., Johansen, W., & Gordon, A. (2024). Business crisis management in wartime: Insights from Ukraine. *Journal of Contingencies and Crisis Management*, 32, e12513. https://doi.org/10.1111/1468-5973.12513

Păunescu,C., Popescu,M. & Blid, L. (2018). Business impact analysis for business continuity: Evidence from Romanian enterprises on critical functions. *Management & Marketing. Challenges for the Knowledge Society,13(3)* 1035-1050. https://doi.org/10.2478/mmcks-2018-0021

Petrenko, S. (2021). Developing an Enterprise Continuity Program (1st ed.). River Publishers. https://doi.org/10.1201/9781003337881

Prihunov, O. (2023). Trends in the development of Ukraine's IT industry: experience and challenges. *Strategii şi politici de management în economia contemporană* (pp. 358–362). SEP ASEM. https://doi.org/10.53486/icspm2023.52

Prohorovs, A. (2022). Russia's war in Ukraine: Consequences for European countries' businesses and economies. Journal of Risk and Financial Management, 15 (7), 295. https://doi.org/10.3390/jrfm15070295

Prokhorova, V. V., Diachenko, K. S., Babichev, A. V. (2023). The IT Industry as a Driver of the Strategic Development of Ukraine's Economy in the Context of Digital Transformation. *The problems of economy*, 1, 65-73. http://jnas.nbuv.gov.ua/article/UJRN-0001417946

Rodríguez Rojas, Y. L. (2021). Continuidad del negocio: conceptualización y metodologías de evaluación. *SIGNOS - Investigación En Sistemas De gestión*, *13*(1), 10-24. https://doi.org/10.15332/24631140.6337

Russo, N., Reis, L., Silveira, C., & Mamede, H. S. (2024). Towards a Comprehensive Framework for the Multidisciplinary Evaluation of Organizational Maturity on Business Continuity Program Management: A Systematic Literature Review. *Information Security Journal: A Global Perspective*, *33*(1), 54–72. https://doi.org/10.1080/19393555.2023.2195577

Russo, N., Mamede, H. S., Reis, L., Martins, J., & Branco, F. (2023). Exploring a multidisciplinary assessment of organisational maturity in business continuity: A perspective and future research outlook. *Applied Sciences, 13*(21), 11846. https://doi.org/10.3390/app132111846

Ruta, M., (2022). The Impact of the War in Ukraine on Global Trade and Investment. World Bank Group, Washington, D.C.

Schätter, F., Hansen, O., Wiens, M., & Schultmann, F. (2019). A decision support methodology for a disaster-caused business continuity management. *Decision Support Systems*, *118*, 10–20. https://doi.org/10.1016/j.dss.2018.12.006

Shvets, I. (2022). Problems and prospects of the development of Ukraine's ICT market in the conditions of war. Ekonomìčnij vìsnik Dnìprovs'koï polìtehnìki, 78:16-22. doi: 10.33271/ebdut/78.016

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science, 89*, 201-218. https://doi.org/10.1016/j.ssci.2016.06.015

Tammineedi, R. L. (2010). Business Continuity Management: A Standards-Based Approach. Information Security Journal: A Global Perspective, 19(1), 36–50. https://doi.org/10.1080/19393550903551843

Vanichchinchai, A. (2023). "Links between components of business continuity management: an implementation perspective", *Business Process Management Journal*, Vol. 29 No. 2, pp. 339–351. https://doi.org/10.1108/BPMJ-07-2022-0309

Varajão, J., & Amaral, A. (2021). Risk management in information systems projects: It can be risky not to do it. *International Journal of Project Management and Productivity Assessment (IJPMPA)*, *9*(1), 58–67. https:// doi.org/10.4018/IJPMPA.20210101.oa

World Bank. (2023). *Ukraine: Firms through the war*. World Bank. https://documents1.worldbank.org/curated/en/099121623102526502/pdf/P177312004f79e06e0b22405be65b5db5b9

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). SAGE Publications.

Annex A

BCM Research Interview (Open-ended questions)

Disclaimer: *All the answers are considered only as your personal opinions based on previous experience and not as the company's official statements.*

Introduction

Please provide here the key information about your company and your role.

Pre-war period Management (2020-2022)

COVID-19 Business continuity management - (*Assessing efforts to establish preparedness across the organization and how they develop into business continuity management*)

Was there a business continuity plan when Covid-19 started, that you are aware of?

What factors should be considered when identifying critical business functions and assets for inclusion in the BCP?

How frequently the BCP should be reviewed and updated? Should it follow BCP frameworks standards like ISO?

What were the key business continuity lessons learned during Covid-19?

How has the Covid (pre-war) period influenced your company's approach to risk management and business continuity planning in retrospective?

What were the most critical vs the most common business emergency situations during the Covid-19 and before the war that you faced?

Risk Assessment and BCP before the potential military invasion *- (Exploring how threat perception affects long-term and short-term strategies; exploring the connection between how risks are perceived and how effectively they are managed; identifying key processes and resources prioritized for continuity under such extreme conditions*)

How could the probability and potential for military conflict (before 24/02/2022) impact business activities, strategic planning and decision-making processes?

What were the company's efforts for maintaining critical operations and services during a military conflict?

What key processes and resources were prioritized for business continuity specifically under conditions of military conflict?

What were your primary concerns regarding the impact of military conflict on the company's operations and daily work?

What measures were taken to educate and prepare employees about the risks associated with military conflict?

Military Invasion Emergency Management (February - May 2022)

Crisis Management and Incident Response *- (Understanding the handling of unique risks and threats posed by the breakout of military conflict, understanding the strategies for handling the unique threats)*

What was your first reaction to the military invasion in the context of work and business?

How did you perceive the level of threat that military conflict poses to the company business in the first week of invasion?

What was the plan to act for the first weeks of the military invasion?

Was there a designated crisis management team responsible for decision-making during a crisis?

What were the most critical and the most common business emergency instances during this first period of the war that you experienced?

BCM communication **-** *(Understanding the communication strategy for internal and external stakeholders in crisis situations; assessing the level of cooperation and coordination with external entities for support and information sharing)*

How does your company communicate with stakeholders (employees, clients, partners) during a business disruption in wartime? Please specify the communication channels

What's been the difference in communicating business disruptions before the war and during wartime?

How did the company cooperate with local authorities and other organizations during a military conflict?

Ongoing war period Management (May 2022- May 2024)

Wartime business continuity management **-** *(Understanding the impact of war events on business and work activities; identifying the key vulnerabilities exposed by the war conditions and areas for improvement)*

How soon after the invasion did your business operations get back to the new normal? How much time did the team need to recover to the full capacity after the invasion?

How do you perceive the level of threat to the company during 2022 - 2024?

What are the primary concerns you have regarding the ongoing impact of military conflict on the company's operations?

How does the ongoing military conflict influence your work planning and decision-making processes? How has this influence changed throughout the last two years?

What were the most critical and the most common business emergency situations throughout the last two years?

New business environment **-** *(Understanding influence of new legal environment for doing business; exploring the applications of technology to support remote work, data protection, and communication during conflicts)*

What new regulatory and legal challenges arose due to the invasion, both in Ukraine and globally? How did you navigate through these challenges?

What role does technology play in the company's BCM during the war time (as well as in the previous periods)?

Summary questions

What do you see as the most significant gaps or weaknesses in your current BCM plans regarding the war and military actions?

What lessons has your company learned from the gap between the expectations and the realities in implementing business continuity measures?

Looking back, how do you assess the adequacy of your company's preparations and response to the pre-war conditions?

Annex B

Quantitative analysis: Risks Significance Perception Rating Matrix

Please assign a point to each of the risks below where **the highest significance is (3) and the lowest is (1)** according to your perception of how significant the risks have been at the specific period.

Risk Category	Risk	Pre-war period (2020-2022)	Military Invasion period (Feb - May 2022)	Ongoing war period (2022-2024)
Physical Security Risks	**Damage to Facilities**: Destruction or damage to office buildings, data centers, and other physical infrastructure.			
	Employee Safety: Risks to the safety and security of employees (including evacuation challenges and the risk of employees being trapped in conflict zones)			
Operational Risks	**Service Interruptions**: Inability to provide services due to infrastructure damage, forced shutdowns, loss of utility services (electricity, water, internet)			
	Quality Control: Difficulty in maintaining quality assurance processes under disrupted work conditions			
	Supply Chain Disruptions: Interruption in the supply of necessary hardware, software, and other resources			
	Vendor Reliability: Increased risk of vendor inability to deliver its services and products. Disruption in communication and coordination with key vendors.			

Risk Category	Risk	Pre-war period (2020-2022)	Military Invasion period (Feb - May 2022)	Ongoing war period (2022-2024)
Human Resources Risks	**Employee Morale**: Decline in employee morale and mental health due to ongoing conflict and instability. Challenges to motivate and engage a workforce.			
	Staffing Shortages: Difficulty in recruiting and retaining talent due to safety concerns and relocations. Increased absenteeism and turnover rates impacting productivity.			
	Training and Development: Disruptions in training programs and professional development activities. Difficulty in onboarding new employees into the company culture.			
Cybersecurity Risks	**Data Breaches**: Unauthorized access to sensitive data due to weakened defenses or targeted attacks exploiting chaotic situations.			
	Increased Cyber Attacks: Cyber-attacks exploiting the chaos of military conflict, including DDoS attacks on critical infrastructure, ransomware, phishing, and other malicious activities.			
	System Vulnerabilities: Exploitation of existing software vulnerabilities due to delayed updates and patches.			

Risk Category	Risk	Pre-war period (2020-2022)	Military Invasion period (Feb - May 2022)	Ongoing war period (2022-2024)
Commercial Risks	**Reputation Damage**: Negative impact on company reputation due to service interruptions or data breaches. Loss of client trust and potential long-term damage to brand image.			
	Financial Instability: Loss of revenue due to interrupted business operations or reduced market demand. As well as increased costs related to security, insurance, and contingency measures			
	Market Uncertainty: Fluctuations in market demand and consumer confidence affecting business stability. Difficulty in forecasting and planning due to an unpredictable environment.			
Legal and Compliance Risks	**Regulatory Changes**: Changes in legislation and regulations due to conflict affecting business operations.			
	Intellectual Property Risks: Increased risk of intellectual property theft and challenges in enforcing IP rights in conflict-affected regions.			
	Contractual and Legal Disputes: Increased likelihood of disputes with clients, vendors, or partners over contract terms and delivery expectations. Inability to fulfill contractual obligations leading to penalties or loss of clients. Disputes with clients over delayed or unfulfilled service delivery.			