Proceedings of 4th International Conference CNDCGS'2024
ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / DOI 10.3849/cndcgs.2024.326

Cyber Security and Business Continuity Management: Ensuring Resilience in a Digital World

Katarína MÄKKÁ[1], **Katarína KAMPOVÁ** [2]

[1] *Department of Security and LawAMBIS University, Lindnerova 1, 180 00 Prague, Czech Republic*
[2] *Faculty of Security Engineering, University of Žilina, 010 26 Žilina, Slovakia*

Correspondence: [1]*katarina.makka@ambis.cz*

Abstract

This article examines the critical importance of implementing Business Continuity Management (BCM), particularly in the field of cybersecurity, to address unexpected disruptions to organizational operations. With a focus on cyber threats and technological disruptions, the study emphasizes the need for close integration between cybersecurity and BCM to minimize risks and effectively mitigate impacts. Drawing from the legal frameworks of the European Union and the Slovak Republic, the article highlights the imperative of integrating BCM into the processes of providing essential services by organizations. Through impact analysis methodology, the article evaluates key processes within a representative entity in the energy sector, identifies critical areas, and resource requirements to maintain continuity. The findings underscore the necessity of proactive planning and response strategies to ensure the stability and competitiveness of the organization in an environment with evolving cyber threats. The study concludes with insights into future research directions, emphasizing the evaluation of supporting processes and their impact on the overall workflow stability within BCM.

KEY WORDS: *cyber security, business continuity management, impact analysis, requirements.*

Citation: Mäkká, K.; Kampová, K. (2024). Cyber Security and Business Continuity Management: Ensuring Resilience in a Digital World. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959. DOI 10.3849/cndcgs.2024.326.

1. Introduction

Unexpected disruptions to an organization's operations, including cyber security incidents, technological failures, and process errors, underscore the need for implementing Business Continuity Management (BCM) with a focus on cyber security and the use of information technology. Cyber threats have become an integral part of the business environment, making it essential for organizations to take measures to minimize risk and mitigate the impacts of these incidents.

Business continuity in the context of cyber security involves planned procedures and actions designed not only to ensure the continuity of providing products or services after a cyber incident but also to minimize damages and restore normal operations. Within business continuity management, it is necessary to consider specific threats and vulnerabilities associated with information technologies and ensure that recovery and resilience measures take the cyber context into account.

The implementation of BCM in the realm of cyber security includes the development of plans, testing their effectiveness, and continuously updating them based on new threats and technological developments. Close integration between cyber security and BCM is critical to ensuring that organizations can respond rapidly and effectively to cyber events and minimize their impacts on their business operations.

New dimensions in the realm of compliance with security standards, reliability, and business continuity in cybersecurity are linked to measures of the European Union concerning cybersecurity through the NIS I [1] and NIS II [2] directives. Within the Slovak Republic, the NIS directive has been transposed into the Act No. 69/2018 on cybersecurity [3]. This law and its implementing regulations require the integration of business continuity into processes related to providing essential services in the cyber domain. Organizations subject to this law must demonstrate that they have developed a business continuity strategy, conducted impact analysis, and defined business continuity plans.

Within business continuity management, it is imperative to consider specific threats and vulnerabilities associated with information technologies and ensure that recovery and restoration measures take into account the cyber context. Implementing BCM in the realm of cybersecurity involves developing plans, testing their effectiveness, and continuously updating them based on new threats and technological developments. Close integration between cybersecurity

© 2024 The Authors.
Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic

and BCM is critical to ensure that organizations can quickly and effectively respond to cyber events and minimize their impact on business operations.

As Kosutic [4] states, the basic elements of business continuity refer to the primary components used to build a company's resilience, including risk assessment, business impact analysis, continuity strategy, and business continuity planning (including incident response and disaster recovery). In the context of business continuity, it is essential to mention the ISO 22301:2019 standard "Security and resilience – Business continuity management systems – Requirements" [5]. The ISO 22301 standard specifies requirements and rules to ensure business continuity and assists companies in rapid recovery in the event of unforeseen events. Its aim is to prepare companies and protect them in case of extraordinary unforeseen events such as natural disasters, power outages, fires, workforce shortages due to pandemics, terrorist attacks, mass IT outages, malfunction of key production or technological equipment, and other threats.

42. An essential prerequisite for effective continuity planning is to have predefined scenarios of various events that could potentially have a negative impact on the organization's regular activities. Typical categories of BCM scenarios include sudden [6]:
    - Unavailability of personnel,
    - Inoperability of workplaces or buildings,
    - Inoperability of technologies,
    - Unavailability of media.

43. Based on the requirements of the ISO 22301:2019 standard "Security and resilience - Business continuity management systems - Requirements" (BCM), it can be argued that the organization's management should formally decide which incident scenarios, considering the organization's limited resources, are subject to business continuity management. In the context of information and cybersecurity, the scenarios mentioned above are most commonly defined in practice. In general, an organization prepares for the interruption of its activities. By planning and enhancing the employee culture regarding accepted security incidents, the organization creates conditions to increase its success in addressing a real incident. Based on continuity plans, the organization establishes conditions to manage a real incident or failure of processes, services, or technologies, in order to return to productive activity in the fastest and most effective way possible, thereby minimizing potential negative impacts. Business Continuity Plans are generally defined for these three areas [4]:
    - Continuity of disrupted priority activities at a predefined level
    - Recovery of disrupted priority activities to the normal level of service, process, technology
    - Mitigation of the impacts of a security incident.

To achieve the organization's capability to create and validate business continuity plans, it is essential to define a business continuity strategy [7]. Within the BCM strategy, approval of recovery time objectives and assessment of third-party capability to ensure supply chain continuity are included. Establishing and selecting an appropriate BCM strategy are based on the results of risk analysis and Business Impact Analysis (BIA) [8]. BIA represents a crucial building block for the BCM process. Through BIA, it is possible to more accurately identify and quantify potential impacts and losses in the event of operations disruption. The goal is to delineate primarily those processes that are critical to the organization, often referred to as critical processes. Business Impact Analysis (BIA) involves assessing the economic, reputational, and regulatory impacts and estimating the costs of process recovery in case of downtime, at various time intervals from the onset of the outage. Assessing dependencies of individual processes on critical resources provides a basis for creating critical process recovery plans. V Within BIA, it is possible to determine attributes that are crucial for determining the criticality of processes, such as [5]:

- Recovery Time Objective (RTO) - the time within which an acceptable level of activities is restored after an outage, or the maximum time it would take to restore the functional state of applications in the event of a sudden service loss. For each process, a predefined recovery time goal, known as RTO, is established, with this time determined based on the criticality of the process.
- Recovery Point Objective (RPO) - the maximum acceptable data loss measured at the time of the recovery point. In other words, it is the data loss that would be acceptable for customers and the organization to recover operations and also considers the acceptability factor of data loss. In relation to process recovery, the activation of the recovery process is required.
- Maximum Tolerable Downtime (MTD) - the maximum outage time representing the time limit for restoring fully functional status. After this time elapses, it is likely that the organization will incur losses.

Disaster recovery significantly differs from business continuity planning (BCP) as it focuses on specific responses to incidents and is often more technologically oriented. While BCP deals with organizational processes, disaster recovery concerns the operation of information technologies and is closely dependent on the specific technological environment [9].

The requirement for continuity is typically found in various legal regulations, such as banking laws, GDPR, and cyber security legislation. According to a general definition, business continuity is referred to as the organization's ability to plan and respond to events and incidents in order to maintain its operations at an acceptable level. This definition often aligns with the ISO 22301:2019 standard [5]. Business continuity is of paramount importance, especially in the realm of critical infrastructures and industrial systems. In relation to the Law No. 69/2018 on Cyber Security of the Slovak Republic and the Regulation of NBU No. 362/2018, we can discuss security measures in this area, which organizations were required to

implement within 12 months from the date of inclusion in the list of essential services (law). Within this article, we will focus on implementing impact analysis into a selected organization.

Impact analysis is the first step in the process of managing process continuity [6]. Its output is to identify critical processes for the organization's core activities and the assets that support these processes. Based on the outputs of impact analysis, the organization decides which process continuity strategy to adopt, as it is important for it to have resources - material, financial, and human - available and in what quantity to be able to recover from an incident resulting in the interruption of its core activities. The process following impact analysis is then the creation of continuity plans and recovery plans.

2. Method of Investigation

The chosen company for the research is a representative entity governed by the Cybersecurity Act, operating within the energy sector. Classified as a Small and Medium-sized Enterprise (SME) based on its employee count, the company specializes in the production, sale, and distribution of heat for both households and businesses. Details such as the company's name, location, and other identifying information are intentionally withheld to maintain confidentiality. The disclosed information is partial, constituting a subset of available data, and is presented with the aim of safeguarding sensitive company details.

The impact analysis was conducted through a combination of methods selected to achieve the defined objectives.

Interviews were a crucial method for gaining subjective insights and information from relevant participants. In the context of impact analysis, they were utilized in initial meetings to understand expectations, goals, and the analysis process. This method served to identify potential areas of interest and contributed to forming a comprehensive picture of the situation based on direct experiences and opinions of stakeholders.

Moderated workshops with owners of relevant processes were strategically employed to gain a deeper understanding of their activities. In the impact analysis, these workshops were used to identify potential risks and impacts. This method facilitated direct involvement of key stakeholders and created a space for the collective identification of potential issues, ensuring a comprehensive view of the analyzed issue from the perspective of internal processes.

Analysis of internal documents was used in crafting the scope of processes and activities for a detailed examination of internal documents. These documents included information about processes, information systems, and their dependencies. Analyzing this input data allowed a better understanding of the context and factors influencing the organization, providing an informational foundation for subsequent impact analysis.

By employing **risk analysis**, the impacts of potential unavailability of processes on the organization's main processes and activities were identified.

The process of conducting impact analysis was structured into several main phases:

1. Introduction Meeting to Impact Analysis: A series of introductory meetings were organized to familiarize stakeholders with the goals and procedures of impact analysis. These meetings also served to set expectations and gain support from involved parties.
2. Proposal of the Scope of Processes and Activities: This phase involved proposing the scope of processes and activities to undergo impact analysis. The proposal was developed based on information obtained about the organization's structure and main processes.
3. Moderated Workshops with Owners of Relevant Processes and Activities: These workshops aimed to gather input data necessary for conducting impact analysis and garner support and cooperation from relevant stakeholders.
4. Impact Analysis: The actual impact analysis was conducted based on collected input data. In this phase, potential risks and their possible impacts on defined processes and activities of the organization were identified.

3. Investigation Results

Impact analysis is based on processes within the organization, during which the following were investigated:

- Data and information used in individual processes.
- Requirements for data and information availability.
- Supporting assets processing data (hardware, software, human resources, suppliers, and others).
- Contexts and dependencies between individual processes.
- Quantitative resource requirements in processes.

Impact analysis was conducted based on information obtained from the provided internal documentation of the analyzed organization. This analysis was performed for the information systems supporting the organization's core processes, as listed in the table below. The provided information is partial and not comprehensively presented due to the extensive amount of information.

Table 1.

Main Processes

Business Process	IS Activity within the business process / IS	Type of IS process
Production Process	his system provides planning and control of production processes, management of material storage, tracking of their consumption, as well as management of raw material orders / MRP-Material Requirements Planning	Main Process
Supply Chain Process	The Supplier Management System ensures tracking and management of material and information flow within the supplier network, including order management, deliveries, and supplier relationships / SCM - Supply Chain Management	Main Process
Production Planning Process	The Inventory Planning System ensures optimization of production resources and capacities based on demand and resources. It includes the creation of production plans, production resource planning, production order management, and plan performance tracking / IPS - Inventory Planning System	Main Process
Distribution and Logistics	Sales and Distribution Management System (SaDS) is a system that manages customer orders, product distribution, shipment tracking, and customer relationship management.	Main Process

The impacts of potential unavailability of processes, information systems, and associated data were assessed on a scale from 0 to 5. These criteria are listed in Table 2.

Table 2.

Description of Impacts

Value	Description of Impact	Financial Loss	Operational Impacts	Legislative Impacts	Reputational Impacts
1	Negligible Impact, Losses	10	Internal, One Person	Disciplinary	Internal dissatisfaction within the department
2	Small Impact, Loss	100	Internally, multiple people	Change in internal legislation	Internal dissatisfaction across multiple departments
3	Significant Impact, Loss	1000	Internally, department	Initiation of corrective action (low penalty)	Internal dissatisfaction throughout the organization, unfavorable publicity
4	Significant Impact, Loss	10 000	Part of the company	Initiation of corrective action (high penalty)	National negative publicity
5	Catastrophic Impact, Loss	More than 100,000	Impact on the entire company	Initiation of corrective action at EU level leading to a high penalty	International negative publicity

Based on interviews, potential impacts for individual processes, as well as RPO and RTO values, were determined. In addition, process owners and possible external dependencies were identified. Prioritization of recovery was established for the main processes. We provide an example for main processes only. Due to sensitive company data, the numbers presented are adjusted.

Table 3.

Operational impacts during outage

Business Process/ IS	<12 hours	<1 day	<3 days	<7 days	<4 days	Impact	Critical Processes	Recovery Priority	RTO/ hours	RPO/ hours days
Business Process	Negligible Impact, Loss	Minor Impact, Loss	Significant Impact, Loss	Significant Impact, Loss	Significant Impact, Loss	13,10	Yes	1	< 3days	2 day
Production Process	Negligible Impact, Loss	Minor impact, loss	Significant impact, loss	Significant impact, loss	Significant impact, loss	13,10	Yes	2	<3 days	2 days
Supply Chain Process	Negligible impact, loss	Minor Impact, Loss	Minor Impact, Loss	Minor Impact, Loss	Significant impact, loss	11,30	Yes	4	<7 days	2 days
Production Planning Process	Negligible impact, loss	Minor Impact, Loss	Significant impact, loss	Significant impact, loss	Significant impact, loss	12,80	Yes	3	< 3days	2 days

Based on the impact analysis, it is necessary to decide on a continuity management strategy and develop specific plans/procedures in the event of a disaster that would require the recovery of all processes or some parts of the processes and

their supporting IS. When creating plans, it is crucial to consider, above all:

- The need for alternative space
- Ensuring internet connectivity
- The need for devices - end stations, printers, network elements
- Contractual arrangements for cooperation with critical suppliers
- Minimum office equipment (desks, chairs) • The possibility of remote work

As part of the further development of the impact analysis, an evaluation of supporting processes related to the main processes will also take place. In the event of a disruption to these supporting processes, there would be a disruption to the main processes as well.

4. Conclusions

In the context of current cyber threats and technological disruptions, it is evident that the implementation of Business Continuity Management (BCM) is essential for maintaining the stability and competitiveness of organizations. The continually evolving digital landscape brings forth numerous challenges that can significantly jeopardize the operations and integrity of business systems and processes. This article undertakes an impact analysis as the initial step in the BCM process, aiming to identify critical processes and resources necessary for sustaining business continuity. It is crucial to emphasize that effective protection against cyber threats requires not only technological measures but also well-thought-out risk management and continuity strategies. The close interconnection between the realms of cybersecurity and BCM is pivotal for an efficient response to incidents and the minimization of their negative impact. This connection becomes even more critical in the context of the legal framework for cybersecurity, imposing heightened responsibilities and requirements on organizations for safeguarding sensitive data and critical infrastructure.

The presented article illustrates an impact analysis focusing on the evaluation of the organization's key processes in terms of their criticality and the time required for their recovery. This process enables organizations to gain crucial insights into which areas of their operations are most vulnerable in the event of a disruption and what resources will be needed to restore normal operations. These insights are then fundamental for developing continuity plans and facilitating a prompt response in crisis situations.

The further research will focus on evaluating supporting processes within the framework of the ongoing development of impact analysis. The main objective is to assess the relationship between these supporting processes and the core processes, identifying their impact on the overall workflow. In the event of an interruption in these supporting processes, it is anticipated that the main processes would be disrupted and halted. This research aims to contribute to understanding the significance and stability of supporting processes within the broader context of impact analysis.

References

1. **Senesac L, Thunda T G.** Nanosensors for trace explosive detection. Materials Today. 2008; 11: 28–36.
2. **Hwang J, Namhyun Choi N, Aaron Park A, Park J-Q, Chung J.H, Baek S, Cho S G, Baek S-J, Choo J**. Fast and sensitive recognition of various explosive compounds using Raman spectroscopy and principal component analysis. Journal of Molecular Structure. 2013; 1039: 130–6.
3. **Moore D.** Instrumentation for trace detection of high explosives. Rev. Sci. Instrum. 2004; 75: 2499–2512.
4. **Izake E L**. Forensic and homeland security applications of modern portable Raman spectroscopy. Forensic Sci. Int. 2010; 202: 1–8.
5. **Tamuliene J, Sarlauskas J, Bekesiene S, Kleiza V**. ITELMS'2014: Proceedings of the 9th international conference, May 23-24, 2014, Panevėžys, Lithuania. Kaunas: Technologija, 2014.
6. **Steinfeld J I, Wormhoudt J. Explosives detection:** A Challenge for Physical Chemistry. Annu. Rev. Phys. Chem. 1998; 49: 203–32.
7. **Becke A.D**. Density-functional thermochemistry. iii. The role of exact exchange. J. Chem. Phys. 1993; 98: 5648–52.
8. **Zhao Y, Pu J, Lynch B J, Truhlar D G.** Tests of Second-Generation and Third-Generation Density Functionals for Thermochemical Kinetics. Phys. Chem. Chem. Phys. 2004; 6: 673–676.
9. **Kendall R A, Dunning Jr. T H, Harrison R J**. Electron affinities of the first-row atoms revisited. Systematic basis sets and wave functions. J. Chem. Phys. 1992; 96: 6796–6806.
10. **Scalmani G, Frisch M J, Mennucci B, Tomasi J, Cammi R, Barone V**. Geometries and properties of excited states in the gas phase and in solution: Theory and application of a time-dependent density functional theory polarizable continuum model. J. Chem. Phys. 2006; 124: 094107: 1–15.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of CNDCGS 2024 and/or the editor(s). CNDCGS 2024 and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.