sciendo

Improvement of Cyber Resilience by Implementation of a Digital Business Continuity Management System: Evidence from Romania

Irina COICIU*
National University of Science and Technology POLITEHNICA Bucharest, Romania
**Corresponding author, irina.coiciu@gmail.com*

Gheorghe MILITARU
National University of Science and Technology POLITEHNICA Bucharest, Romania
ghmilitaru.militaru@gmail.com

Abstract. *This paper aims to present a model for increasing the cyber resilience of organizations. Under the business context when cyber incidents risk is the most important risk worldwide for organizations for the third consecutive year, the model proposes a solution for improvement of cyber resilience of organizations, by implementation of a management system based on Business Continuity Management framework and a related software solution for handling the Risk Management data, Business Impact Analysis, Emergency and Recovery Planning, as well as Cyber Crisis Management. The implementation of the digital Business Continuity Management System and Cyber Crisis Management processes is tested through a simulation of a cyber incident leading to disruption of activities and cyber crisis caused by a ransomware attack. The simulation is presented both as design and execution and it can be implemented in any organization having the Business Continuity Management System in place and an internal IT department. The results of the simulation bring evidence for the contribution of the study to the increase of the cyber resilience of the organization. The novelty of the study is represented by the mix of concepts and instruments brought together in the model through which the framework of Business Continuity Management is implemented by means of a dedicated software solution, facilitating steps towards the digitization of the management processes and increase of the organizational and cyber resilience.*

Keywords: cyber resilience, resilience, business continuity, disruption, risk.

Introduction

In recent years, the cyber incidents risk is the most important global risk in 2024, according to Allianz Risk Barometer (2024). Cyber incidents, namely cyber events that disrupt normal operations, such as data breaches, malware attacks, ransomware attacks, Information Technology disruptions, are the top concern for businesses globally, across all company sizes for the first time, according to Allianz Risk Barometer (2024).

Emergency situations and crises – including the ones triggered by cyber incidents - are not announced in advance. Moreover, their effects are difficult to be predicted. However, such disruptive events and situations need to be effectively managed in order to potentially minimize the negative effects. The complexity increases, as these incidents appear quickly and unexpectedly, sometimes overlapping, for example: cyberattacks, blackouts, climate change, pandemics etc. The cyberattacks, data loss, unavailability of different Information Technology resources, either physical or digital are some of the most commonly taken into consideration by organizations as risk scenarios with disruptive potential to be prepared for, due to their increase in frequency and impact during the last several years. The preparation for possible situations for handling cyber disruptive events leads to increased cyber resilience for the organization. Moreover, cyber resilience is an important aspect considered at management level in negotiations and partnership

DOI: 10.2478/picbe-2024-0209

decisions, playing important role as well on the customer related areas. Business Continuity Management framework governed by ISO 22301 standard ensures an overview over aspects related to continuity of activity and resilience. The preparation of organizations to handle cyber risks that can materialize into disruptive events includes the creation of emergency and recovery planning, as well as testing and simulation of disruptive scenarios.

Further on in this paper, the remaining sections of the article present the literature review, outline the theoretical background, develop the study's research model and hypotheses, and describe the research methods before presenting empirical findings and implications of results for research and practice.

Literature review

Cyber incidents risk

The cyber incidents risk is the most important risk worldwide, for the third consecutive year, based on the data retrieved from Allianz Risk Barometer (2022, 2023, 2024). Total or partial loss of data following a cyber-attack, unavailability of the IT infrastructure from various reasons, compromise sensitive data are examples of such cyber risk scenarios. If referring for example to a cyberattack, it can take many forms, such as ransomware attacks, data breaches, malware attacks, denial of service (Li & Liu, 2021). These attacks can result in the loss of sensitive data, data leakage, financial loss, significant operational disruptions.

According to Global Cyber Security Outlook (2023), 43% of organizational leaders think it is likely that in the next two years, a cyberattack will materially affect their own organization. If it is not managed effectively, a cyberattack can quickly and unexpectedly escalate into a crisis, impacting the organization and its stakeholders, such as customers, employees, partners. The process and organization of Crisis Management is set up and runs until there is done the restoration of the processes for resuming the activity (Coiciu, 2022a). There are numerous scenarios that activate the risk of business interruption. Cyber incidents risk is one of them. This risk of business interruption is on the second position in 3 consecutive years in the top business risks for 2022, 2023 and 2024 globally and on the third position in the top business risks in Romania for 2022 and respectively on the 5th position for 2023, according to Allianz Risk Barometer (2022, 2023, 2024).

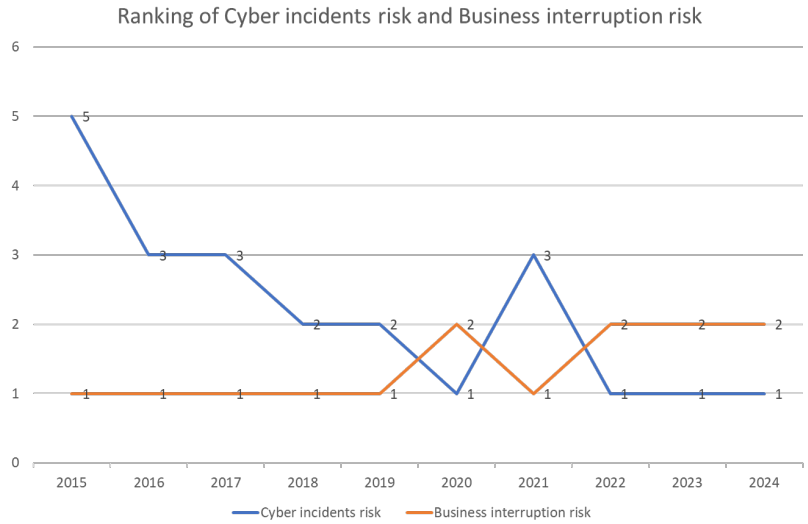

Figure 1. Ranking Evolution of Cyber incidents risk and Business Interruption risk

Source: Author's own research, based on data from Allianz Risk Barometer for 2015-2024.

Based on Allianz Risk Barometer for the years 2015 to 2024, the evolution of the ranking of cyber incidents risk and business interruption risk is presented in the diagram below, from Figure 1. During the last 10 years, Business interruption risk was ranked as first most important risk globally in 6 out of 10 years. The cyber incidents risk was in top 5 most important risks globally during the last 10 years, keeping rank 1 in 4 of the last 5 years.

These 2 risks have been in focus of management for several years now and as a result of this, Business Continuity Management was brought under the attention of business stakeholders, as well as the concepts of resilience and cyber resilience. Additionally, the importance of these concepts is supported by the fact that, according to PWC's Global Crisis and Resilience Survey (2023), in 2023 96% of organizations have experienced disruptions in the past 2 years and 91% of organizations have experienced at least one disruption other than the pandemic. The figures were much lower in the past years, as for example in 2019, 69% of organizations said that they experienced a disruption in the last 5 years.

Business Continuity Management System

The standard ISO 22301, "Societal security – Business continuity management system – Requirements" provides a framework for implementation and maintenance of business continuity, with a focus on the ability of organizations to manage disruptive incidents of the activity (Coiciu, 2022a) and organizations can have it in consideration on cyber resilience related aspects.

Business Continuity Management (referred to further on in this paper also as BCM) is a management system which supports management of organizations to plan and organize business continuity, for the case when disruptive incidents occur (Coiciu, 2022b). Business Continuity Management is also a process, which is implemented in organizations to increase resilience and management capability to plan and prepare for possible disasters and disruptive scenarios that may lead to various losses or unavailability of resources, such as personnel or technology (Redmond, 2018). The BCM System offers a framework for organizations to establish the optimal measures to respond to the disruptive risk scenarios in order to restore the business processes at optimal costs, reducing the negative impact, train the management and the teams that manage the crisis. It is also a widely used framework to build up and increase the resilience and cyber resilience of organizations. Also, this system allows organizations, in case of eventual disruptions, to restore the availability of services at established/ assumed levels (Redmond, 2018, p. 1-3).

Once implemented, BCM is a continuous process in an organization. Moreover, all crisis management activities should be considered as a permanent continuous process beginning with prevention and ending with organizational learning (Vašíčková, 2019).

Cyber resilience for organizations

Cyber resilience refers to the degree to which organizations are prepared to face and overcome disruptions due to cyber incidents. In order for an organization to be resilient and successfully face disruptions, the attitude of the leadership team towards disruptions and the readiness of the organization to face them is critical. The process of an organization to become resilient needs resources, objectives, actual actions and consistency during time. During the latest years, top management of organizations pay more attention to cyber resilience, as cyber incidents risk is the first one in the top of global risks, according to Allianz Risk Barometer (2022, 2023, 2024).

Interconnected data services continue to grow in size and complexity, exposing new vulnerabilities to cyberattacks and outages (Hero, Kar, Moura, Neil, Poor, Turcotte, Xi, 2023). The numerous challenges that arise from the rapid and multiple overlapping threats and risks, the

increasing number of cyber-attacks, the increasing dependence on technology bring to the picture more and more the necessity to consider models of increasing cyber resilience for preventing and handling the disruptions and crises with the aid of software systems. According to Global Cybersecurity Outlook 2023, only 27% of business leaders were confident in 2023 that their organization is cyber resilient. Moreover, this percentage is lower than in 2022, as presented in the diagram from Figure 2.

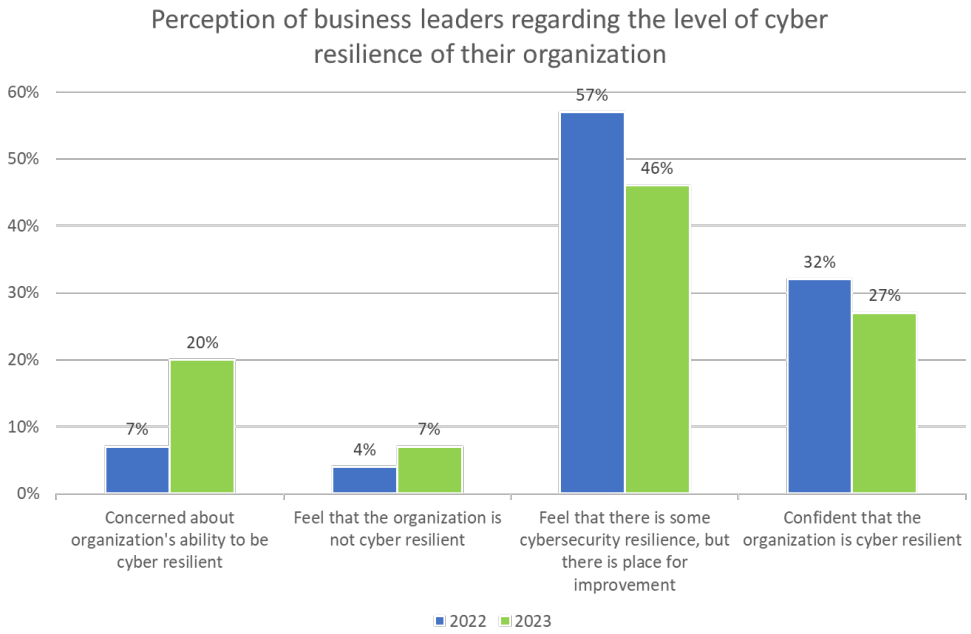

Figure 2. Perception of business leaders regarding the level of cyber resilience of their organization
Source: Adapted diagram, based on data from Global Cybersecurity Outlook 2023.

However, the gap between the perception of business leaders and cyber leaders diminished significantly in 2023 in comparison to the previous year, as shown in the same report, Global Cybersecurity Outlook 2023. In 2022 only 12% of the cyber leaders were confident that the organization is cyber resilient, while in 2023 it increased to 29%, which is 2% higher than the corresponding percentage. Moreover, in the same report it is shown that a close communication between business leaders and cyber leaders has a positive impact over the perception of cyber resilience. More frequent communication means more opportunities to align on cybersecurity priorities. Of respondents who meet at least monthly, 36% are confident that their organization is cyber resilient and only 8% of those respondents report that their organizations either are not cyber resilient or that they are concerned about their organization's ability to be cyber resilient.

Considering the increasing awareness over organizational and cyber resilience, the need of having in place flexible and high-performance IT solutions to support the processes of risk, crisis and continuity management. In this context, the business continuity management system, as well as crisis management can be implemented in organizations using software solutions, digitization of these management processes providing clear advantages for the organization, for the management team, for the incident management teams, as well as for emergency and crisis management teams.

Methodology

The paper presents the design and implementation of a model for organizations to increase the cyber resilience – digital Business Continuity Management System. There are used mixed research methods including case study, observations, interviews, simulation in order to analyze the validity of the model for increasing the cyber resilience of the organization. The simulation of a cyber incident (ransomware attack) in a Romanian manufacturing company, leading to a cyber crisis, supports the validation of the model implementation, as well as future research and improvement opportunities.

Although some organizations have measures in place to handle cyber incidents, the local handling in the technical teams/ technical departments is not enough, as the impact of cyber incidents or cyber crises might affect the entire organization, leading to disruptions and even affecting the continuity of their operations. For this reason, a model for a systemic approach embedding digital implementations supports this research hypothesis. Awareness is created in the organization, cross-functional teams are formed and management team involved to support and commit to the implementation. In this paper the model is exemplified with brief data from a ransomware attack.

The process model for preparing the organization to face cyber incidents and disruptions leading to increased cyber resilience is presented in Figure 3.

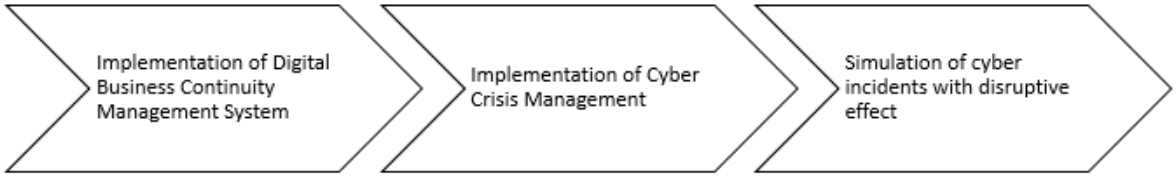

Figure 3. Model for preparing the organization to increase cyber resilience

Source: Author's own research.

Digitization supports all these steps, bringing significant added value especially that hybrid work and remote work are often used by the organization as it has distributed teams. The software solution which supports the implementation of these stages ensures traceability of data and scenarios, real time access to data, automatic generation of reports and documents and can ensure the needed proof in case of audits or verification for compliance.

Step 1 - Implementation of digital Business Continuity Management System

The implementation of digital BCM System is performed in three main steps and the data and information is input in the BCM software system, which performs automatic processing, documents and reports generation. The process steps are presented in Figure 4.

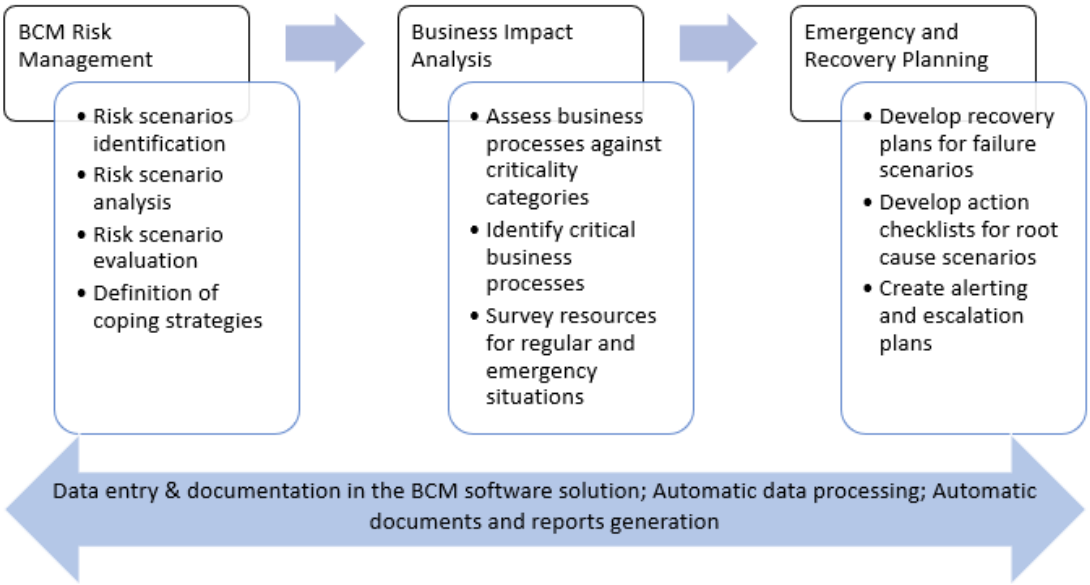

Figure 4. Digital Business Continuity Management System implementation

Source: Author's own research and usage of BCM software system.

During the BCM Risk Management stage there are identified possible risk scenarios for the organization. A sample of the identified risk scenarios is presented in Figure 5.

Risk Scenarios

+ Create | Refresh | Delete | Export

Number	Name	Responsible
3	Ransomware attack	IT-Manager
4	DDoS	IT-Manager
5	Backdoor	Head of IT
6	Pandemic	Head of HR
7	Explosion plant hall	Quality Manager
8	Technical fault main system	Quality Manager
9	Accidental passers-by	Facility Manager
10	Traffic accident on the comp...	Logistics Manager
11	Strike of the employees	Head of HR
12	Sabotage	BCM Manager
13	Accident at work with seriou...	Product Manager
14	Spy	BCM Manager

Figure 5. Sample of risk scenarios list from the BCM software

Source: Author's own research and usage of BCM software system.

The risks scenarios are then analyzed based on the probability of occurrence and impact criteria. In Figure 6 there is presented a part of such analysis for the Ransomware attack risk scenario.

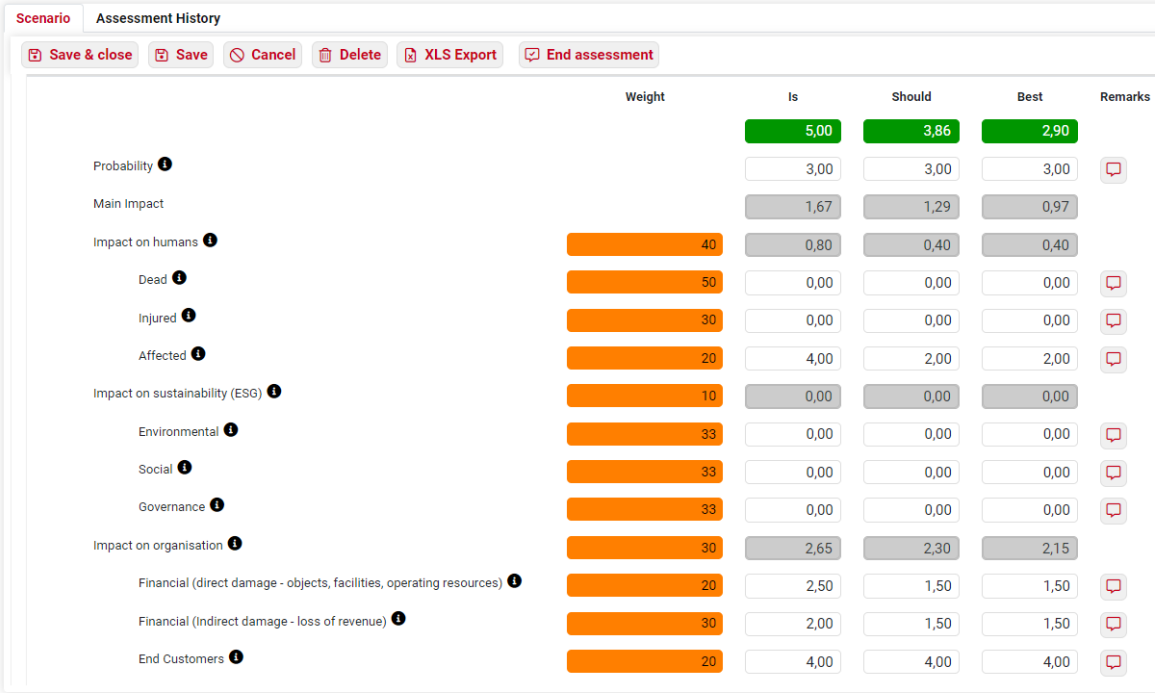

Figure 6. Sample of risk analysis in the BCM software for the Ransomware attack

Source: Author's own research and usage of BCM software system.

Based on the risk analysis a Risk Matrix is created and automatically generated from the BCM software. Moreover, based on the risk analysis, coping strategies are defined and the top risk scenarios based on the risk matrix representation are decided for the next steps in the BCM implementation. An example of risk matrix generated by the software is presented in Figure 7. Due to limited space, only part of the risk scenarios list is displayed in the figure.

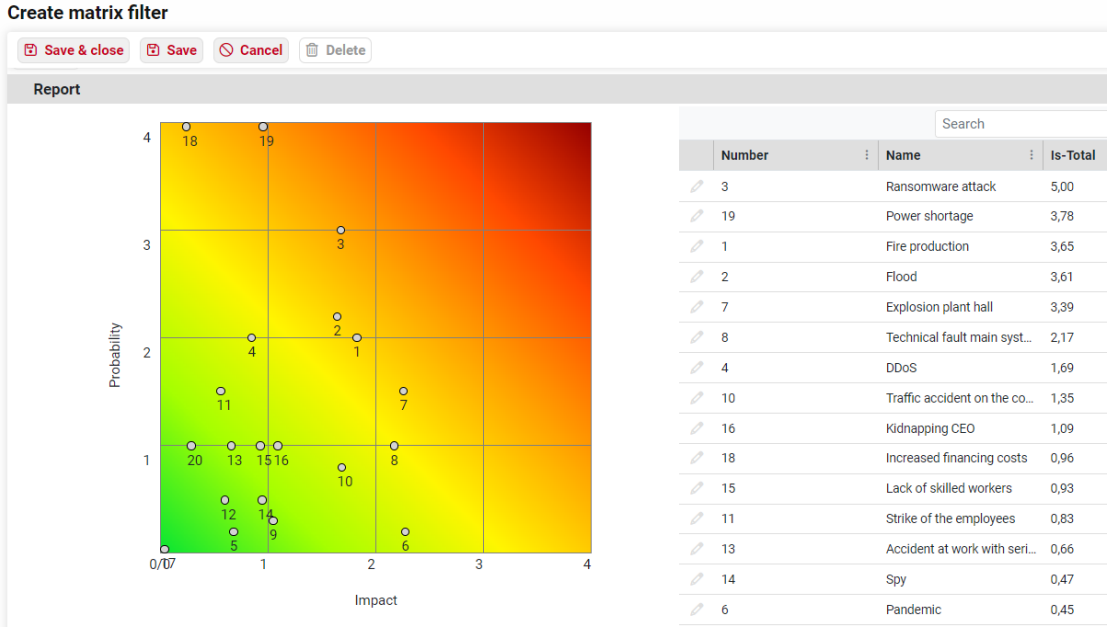

Figure 7. Risk matrix sample generated by the BCM software solution

Source: Author's own research and usage of the BCM software system.

The second stage of implementation of the digital BCM system, as presented in Figure 4, is Business Impact Analysis (further referred to also as BIA). Through this stage, the business processes are assessed against criticality categories such as: availability, confidentiality, integrity etc. and the critical business processes are identified. Also, BIA represents an important step for the ellaboration of the disaster recovery plan, in later stages of the BCM implementation (Krahulek). All collected data regarding the criticalities of the processes are input in the software, in an interface as the one presented in the Figure 8. Due to the high number of processes, resources, IT systems and limited space of the paper, there is presented only a data sample.

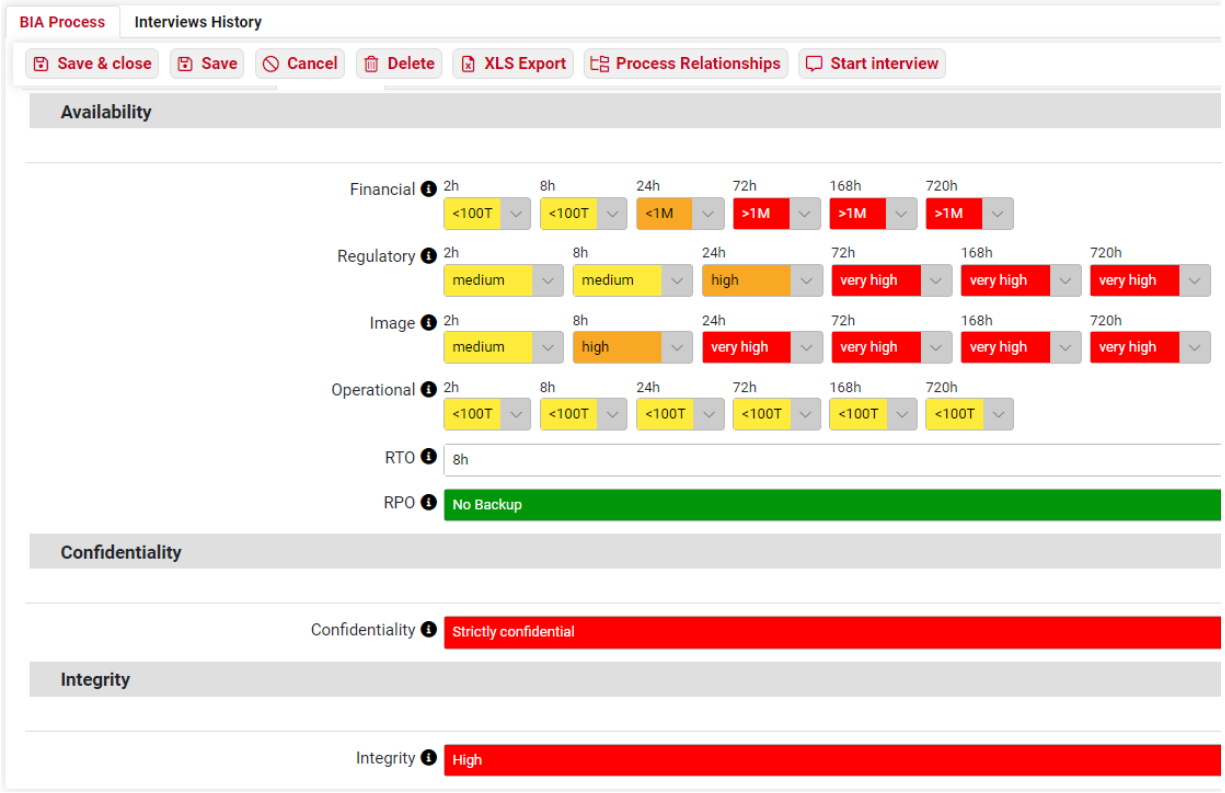

Figure 8. Sample of criticalities input in the BCM software for a process during the BIA interview
Source: Author's own research and usage of the BCM software system.

During BIA there are also collected, centralized and analyzed for each process the two important parameters, namely the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as shown in Figure 8. Also, during the BIA interviews held with the process owners, the resources for regular and emergency/ crisis situations are being surveyed, collected and centralized in the BCM software. The BCM software assesses the interdependencies between the processes, IT systems, resources and prepares the list of critical processes and related resources, which can be exported in a BIA report.

The next stage in implementing the BCM system, as shown in Figure 4, is Emergency and Recovery Planning, in which the continuity plans are being developed. In these continuity plans there are included alerting and escalation plans, there are presented responsibilities and needed resources, as well as workarounds for handling activities and processes that have possibly been affected by the disruptive events. There are also included checklists for different possible scenarios, together with responsibilities and needed resources. All the data is input in the BCM software,

which can automatically generate the checklists and the continuity plans, based on predefined structure. In Figure 9 there is presented a sample list of emergency measures which were identified for the ransomware attack, filtered from the entire list of emergency measures recorded in the BCM software for the BCM risk scenarios.

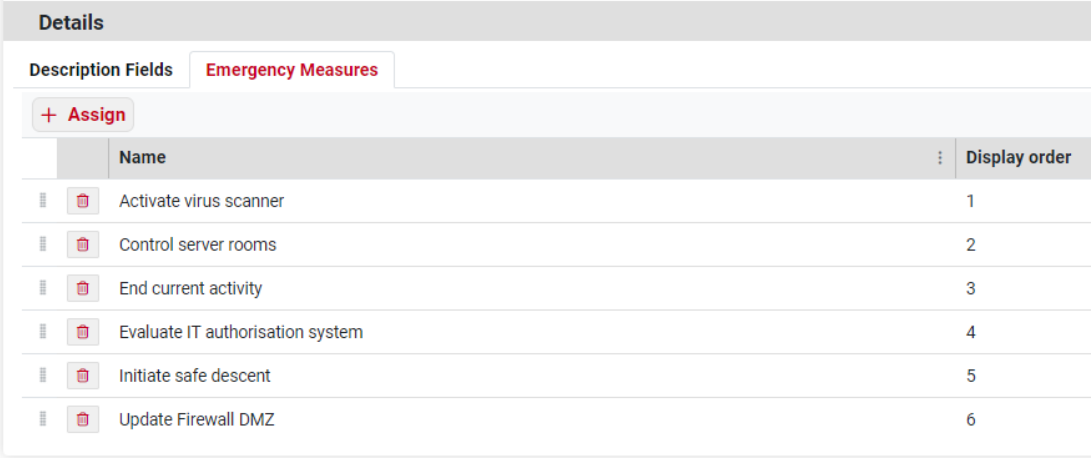

Figure 9. Sample list of Emergency measures in the BCM software for the ransomware attack
Source: Author's own research and usage of the BCM software system.

Recovery plans are generated for the ransomware attack and they are further used as input in Step 2 and Step 3 of the BCM implementation shown Figure 3.

Step 2 - Implementation of Cyber Crisis Management

Cyber Crisis Management is activated when a crisis situation due to a cyber incident occurs. According to Redmond (2018), a crisis situation is any situation that causes an interruption of the activity. Crisis Management refers to applying strategies in order to help the organization manage a sudden negative event, with significant effect, maintaining the continuity of the operations. Even if the definition of crisis management has been facing different changes throughout time (Vasickova, 2019), crisis management as a process has as main objective to define and implement procedures to manage, reduce and prevent a crisis.

The steps for implementing the Cyber Crisis Management are presented in Figure 10.

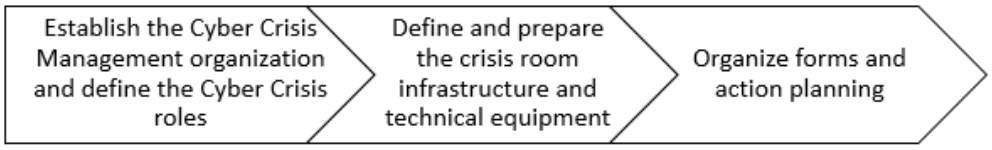

Figure 10. Steps for implementing Cyber Crisis Management
Source: Author's own research.

In the current paper there is considered the ransomware attack as cyber risk scenario for which the Cyber Crisis Management is implemented in the organization.

The management of the organization decided upon the crisis management structure, which was structured on 3 layers: Strategic, Tactical, Operational. On the strategic level there is the CEO, having the ultimate decisions regarding the crisis and financial resources, on the Tactical level there is nominated a Cyber Crisis Manager, in this case the IT Manager, who decides the team that he needs to handle the crisis at operational level. The Crisis Management Team is responsible for

managing and coordinating the response to the cyber crisis. The team is composed of senior executives and subject matter experts from various departments: IT, operations, communication and public relations, legal. Experts in cybersecurity were included and the Cyber Crisis Management Team was extended to partnership with a cybersecurity company, in order to assess the impact of the attack, identify and address vulnerabilities, recover systems and data.

A crisis room, the related infrastructure and technical equipment were prepared, such that the Cyber Crisis Management Team can meet, operate, communicate, take decisions and easily be connected to people from all working locations, remote work being usual for the company. There were prepared communication devices, whiteboard, access to emergency and recovery plans, printer, secondary access to IT systems, etc. Preparation, planning and organizing the activity of the personnel during the crisis was done. As in any crisis and especially in cyber crises, communication management is very important, and ensuring a proper documentation and logging of the cyber crisis events, actions, decisions is essential for proper handling, as well as to ensure traceability of the events that take place and for the decisions that are being taken during the crisis, the access to the BCM software was ensured for the Cyber Crisis Management Team and management. Action planning was coordinated by the Cyber Crisis Manager

Step 3 - Simulation of cyber incidents scenario with disruptive effect

Step 3 in the process model for preparing the organization to face cyber incidents and disruptions, which is presented in Figure 3, is very important in the current paper from 2 perspectives. A first perspective is that the simulation of cyber incidents is an important phase in preparing the organization to increase cyber resilience, as this offers the opportunity to test the implementation of the BCM and Cyber Crisis Management processes, as well as to create a feedback loop for the continuous improvement of the system. Also, the simulation exercise increases the degree of responsibility and the motivation to support the implementation of the BCM and Crisis Management processes. Moreover, the simulation can be used by the organization as a powerful tool to create awareness and train the personnel. Additionally, a second perspective is for the current research, namely the fact that the role of the simulation is to validate the model for increasing the cyber resilience of the organization.

The simulation of a ransomware attack is conducted by a "Trainer Group", as predefined in advance in a scenario schedule, that details the actions, the roles, and the timing. An extract of the scenario script is presented in Figure 11.

The Trainer Group is formed at least of the following roles: BCM responsible persons, one or more cyber specialists not involved in the restoration of the processes nor in handling the cyber crisis, external consultants (if needed).

For smooth implementation of the simulation exercise, several constraints and rules are taken into consideration, such as: the organization must have minimum disruption, so there is a parallel continuation of the usual processes while the simulation exercise is in progress; the communication with external sources is done only with informed and prepared people; for real external communication, the Trainer Group must be informed in advance and afterwards.

Cyber incident Scenario Script - Ransomware

Nr	Time	Role	From	To	Chanel	Action	Exp. Response	Remark
1	09:15	Trainer Group	Trainer Group	All	Meeting	Introduction: Rules and coordination (including daily work): - Contact details - name officers, BCM, Cyber Crisis Manager etc		
2	09:50	Staff	Trainer Group	Crisis Manager	Phone	Ransomware attack identified	Alarming, first aid, ...	START OF SCENARIO
3	10:00		CM	Trainer Group	Phone	Ransomware attack identified, Cyber Crisis Management activated	EXPECTED	
4	10:05		Crisis Manager	BCM	Phone	Activate needed people	Activate Recovery Plan	Define people in advance (Trainer Group)
5	10:10		Crisis Manager	Board	Phone	Status to Board	Info to CEO	Board is at a meeting in HQ
6	10:20		Crisis Manager	HQ CM	Mail	Inform Group Security Crisis Management	Info HQ CM	Request if no Info
7	10:25	Media	Trainer Group	Crisis Manager	Phone	Media request (status, data loss, impact to customers, ...)		ask for mobile number of communication point to media
8	10:35	Orange	Crisis Manager	Orange	Phone	Info Orange?	expected	not done in reality
9	10:45	Clients	External	Call Center	Phone	What happens to my rights, I need access to my data etc	Overload for communication	
10	10:55	External	External	Crisis Manager	Phone	Mother of cleaning lady (works in the HQ) cannot reach his daughter	Ask officer in charge	
11	11:10	Client	Trainer Group	Crisis Manager	Phone	urgent business case of top client		
12	11:20	Group CM	Trainer Group	Crisis Manager	Phone	Additional Info to Group Security Crisis Management		
13	11:25	Media	Trainer Group	Crisis Manager	Phone	Media request (status, data loss, ...)		
14	11:30	Authority	Trainer Group	Crisis Manager	Phone	Request Info about BCM		Are BCPs working?
15	11:45	Group CM	Trainer Group	Crisis Manager	Mail	Request Info		
16	11:50	Client	Trainer Group	Crisis Manager	Mail	Security calls because of client asking for his data info in front of building		

Figure 11. Scenario script extract for the simulation of cyber incident – ransomware attack

Source: Author's own research.

A sample set of principles and rules for the simulation exercise is presented in Table 1, which was also used as a checklist and filled in by all participants at the end of the simulation exercise, whether fulfilled or not during the simulation exercise.

Table 1. Example of Simulation principles and rules (checklist)

No.	Principle/ Rule description	Was respected during the simulation? [Y/N]
1	Safety always goes first, before any purpose of the simulation exercise	
2	Daily business has higher priority than the exercise	
3	No real alarming, communication to emergency rescue services, authorities or other internal or external agencies	
4	All actions and items are fictious assumptions during the exercise	
5	All actions and items are done in real time	
6	All documents, information and conversation must be marked as TEST	
7	Logs, minutes, protocols must be done in written form (including lessons learned)	
8	The Crisis Team must be supported by a BCM specialist (internal or external)	
9	The simulation exercise can be stopped or interrupted at any time	

Source: Author's own research.

Results and discussions

In the simulation exercise performed, the compliance with the set of rules the was 100% and it was executed smoothly, without incidents. The simulation exercise was finalized with a feedback form, in which all participants to fill in their comments and observations, such that the BCM team can extract lessons learned based on the feedback and perspectives of all roles involved in the simulation exercise.

The BCM team organized a meeting at the end of the simulation day in which the feedbacks were discussed, centralized and a list of lessons learned issued. In Table 2 there is presented an extract of the list of lessons learned, based on the collected feedbacks.

Table 2. Extract of the list of lessons learned following the simulation exercise of the ransomware attack

No	Feedback item	Positive aspects and comments	Challenges, opportunities, proposals
1	Cyber crisis scenario	- the cyber crisis team activation worked as planned, established very fast and started to work according to the defined crisis management organization - the scenario positively contributes to the increase of the cyber resilience	- the communication with the media was underestimated at the beginning, but eventually got on a satisfying level - too much information was delivered to media during the exercise, it is recommended to exercise this further
2	Trainer Group	- the communication of the crisis team with the BCM team was on a high level during the entire simulation	
3	Infrastructure (crisis room, IT&C, communication)		- more phone lines are needed in the crisis room - TV should exist in the crisis room
4	Flow of communication and cooperation	- the situation was always on the same level for all crisis team members, who used the software application on a regular basis during the simulated cyber crisis	- communication training for cyber crisis situations should be done for the crisis management team and all personnel of IT/ technical departments
5	Documentation	- all events and measures were documented in a proper, clear way in the software - the usage of the forms in the BCM software was highly welcome, as all information is centralized and easily accessible	- a procedure for the BCM simulation would rather be useful - BCM responsibilities are to be defined for each department
6	Checklists		- the continuity plans can be improved, as there were found gaps between the planned personnel in the software and the actual personnel involved

Source: Author's own research results.

As overall feedback, simulation of cyber incidents leading to cyber crises is highly welcome by all personnel of the organization that was involved in the exercise and they consider that this type of exercise has an important role in increasing the cyber resilience of the organization. Based on this feedback, the authors of the research consider that the model designed for increasing the cyber resilience is validated and can be further be used for maintaining the existent implementation, as well as for improvements and future developments.

Conclusions

Cyber resilience is present more and more in the preoccupations of top management of organizations. The solution designed for supporting leadership in preparing organizations to increase cyber resilience by implementation of a digital BCM System can be useful for making the transition from traditional handling of cyber incidents to implementing a BCM system, as well as for organizations that already have parts or sub-processes of the BCM system implemented, such as the Disaster Recovery Plans, but they are still missing the entire picture of the BCM system. By taking a proactive approach to cyber crisis management, leaders can help safeguard the organization from the damaging impacts of cyber incidents and maintain the trust and confidence of the stakeholders. Additionally, regular communication of business leaders with cyber leaders on cyber-related topics can have a positive influence over the increase of cyber resilience of organizations.

Digitization of business continuity, crisis management and risk management processes supports the reduction and minimization of challenges such as the availability of business continuity system data, access to data in real time for the teams and stakeholders working remotely or in hybrid manner, ensuring support and traceability in the evolution of events and in the decision-making processes during crises, quick and automatic access to reports, crisis documentation, thus facilitating the increase in the cyber resilience of organizations.

However, challenges in the implementation of the model might occur. These challenges might be related to technology and IT infrastructure, insufficient local regulations for this domain of business continuity and cyber resilience, reluctance of management and existent mindset gap and differences in opinion between business leaders and cyber leaders, difficulties in quantifying benefits due to lack of measuring systems for the cyber resilience.

Some limitations are noted in the study. The results of this study are limited to the ransomware attack cyber incident possibly occurring to organizations that have internal IT department. However, projects could be organized for implementing the model for any other cyber incident. Out of scope for the applicability of the model can be the organizations that have the IT function outsourced, as the structure and management of the Cyber Crisis Team would be rather different than presented. There is opportunity for further research to be performed, in order to analyze whether an extension of this model can be considered for types of incidents and risk scenarios that might occur and produce disruptions, affecting the continuity. Extensions could be considered, as a result of further research studies, with or without changes of the designed model.

References

Allianz Risk Barometer (2015-2021), Retrieved from https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Allianz Risk Barometer (2022), Retrieved from https://www.allianz.com/en/press/news/studies/220118_Allianz-Risk-Barometer-2022.html, Accessed on 24.02.2024

Allianz Risk Barometer (2023), Retrieved from https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html, Accessed on 24.02.2024

Allianz Risk Barometer (2024), Retrieved from https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html, Accessed on 24.02.2024

Coiciu I. (2022a), *Blackout, the danger that lurks in any company. How managers can prepare to continue the activity*, Retrieved from https://irinacoiciu.ro/blackout/, Accessed on 24.02.2024

Coiciu I. (2022b), *Everything you need to know about Business Continuity Management. Why it should not be absent from any company or public institution*, Retrieved from https://irinacoiciu.ro/bcm/, Accessed on 24.02.2024

Global Cybersecurity Outlook 2023, Retrieved from https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf, Accessed on 24.02.2024

Hero A., Kar S., Moura J., Neil J., Poor H. V., Turcotte M., Xi B. (2023), Statistics and Data Science for Cybersecurity, Retrieved from https://doi.org/10.1162/99608f92.a42024d0 , Accessed on 24.02.2024

ISO22301, *Societal security – Business continuity management systems – Requirements*

Krahulec J, Jurenca M, *Business Impact Analysis in the process of business continuity management,* Retrieved from https://www.researchgate.net/publication/ 277900650_BUSINESS_IMPACT_ANALYSIS_IN_THE_PROCESS_OF_BUSINESS_CONTINUITY_MANAGEMENT, Accessed on 24.02.2024

Li, Y., Liu, Q. (2021), A comprehensive review study of cyber-attacks and cyber security;

Emerging trends and recent developments, Retrieved from https://www.sciencedirect.com/science/article/pii/S2352484721007289, Accessed on 24.02.2024

PWC's Global Crisis and Resilience Survey (2023), Retrieved from https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html, Accessed on 24.02.2024

Redmond, M. C. (2018), *Mastering Business Continuity Management*, BookLocked, Publishing, ISBN 978-1-63491-421-5, pp. 1-3, 245, Florida, St. Petersbourg

Vasickova V, Crisis Management process: a literature review and a conceptual integration, Retrieved from https://www.researchgate.net/publication/341809953_Crisis_Management_Process_-_A_Literature_Review_and_a_Conceptual_Integration, Accessed on 24.02.2024