UNIVERSITY OF ECONOMICS AND MANAGEMENT
Nárožní 2600/9a, 158 00 Prague 5, Czech Republic

DIPLOMA THESIS

CRISIS MANAGEMENT IN LINET GROUP

University of Economics and Management
info@vsem.cz / www.vsem.cz

UNIVERSITY OF ECONOMICS AND MANAGEMENT

Nárožní 2600/9a, 158 00 Prague 5, Czech Republic

TITLE OF DIPLOMA THESIS
Crisis Management in LINET Group

DATE OF GRADUATION AND DIPLOMA THESIS DEFENCE (MONTH/YEAR)
June/2024

NAME AND SURNAME OF THE STUDENT/STUDY GROUP
Petr Němeček / DEMMA07

NAME OF THE SUPERVISOR
doc. Enzo Essenza, D.Phil., M.P.A

STUDENT'S DECLARATION

By submitting this thesis, I declare that I have independently completed the assigned diploma thesis on the specified topic and that I have used only the literary sources listed in the work for the preparation of this thesis. I am aware that this work will be published in accordance with § 47b of the Act on Higher Education Institutions, and I agree to such publication regardless of the result of the thesis defense. I declare that the information I used in the work comes from legal sources, i.e., it is not subject to state, service, or trade secrets, or other confidential information for which I do not have the necessary permission to use in the work or its subsequent publication in connection with the anticipated public presentation of the work.

Date and place: 1. 5. 2024, Prague

ACKNOWLEDGEMENTS

I would like to express my gratitude to the supervisor of my thesis for the methodical guidance and expert consultations provided during the preparation of my diploma thesis.

UNIVERSITY OF ECONOMICS AND MANAGEMENT

Nárožní 2600/9a, 158 00 Prague 5, Czech Republic

SUMMARY

1. Main Objective:

The primary objective of the diploma thesis, "Crisis Management in LINET Group", is to strategically incorporate the cybersecurity mandates of the NIS II Directive into the crisis management protocols of LINET Group. This integration aims to enhance the organization's resilience against cyber threats and ensure operational continuity within the healthcare industry. Employing a comprehensive multi-disciplinary methodology, the thesis endeavors to fortify LINET Group's crisis management infrastructure, thereby aligning with regulatory compliance and bolstering the organization's preparedness for operational crises.

2. Research Methods:

In the thesis "Crisis Management in LINET Group," a multidisciplinary methodology was adopted to examine the implementation of the NIS II Directive requirements within the organization's crisis management framework. The methodology included legislative analysis, an extensive literature review, detailed interviews with stakeholders, case study analysis, comprehensive risk assessments, scenario planning, development of framework approaches, creation of implementation plans, evaluation, and feedback. This approach enabled a thorough exploration of both theoretical and practical aspects of crisis management in accordance with the NIS II Directive requirements, aiming to enhance resilience and compliance within the LINET Group.

3. Result of Research:

The research conducted for the thesis 'Crisis Management in LINET Group' demonstrated significant insights into the integration of the NIS II Directive's cybersecurity requirements into the existing crisis management practices of the organization. The adopted methodology, which included regulatory analysis, a thorough literature review, detailed stakeholder interviews, case study analysis, comprehensive risk assessments, scenario planning, and framework development, proved effective. This approach facilitated an in-depth exploration of both theoretical and practical aspects of crisis management, aligning with the NIS II Directive to significantly enhance the LINET Group's resilience and regulatory compliance. The results confirm the effectiveness of the implemented frameworks and strategies in strengthening the organization's capabilities to manage and respond to crises.

4. Conclusions and Recommendation:

The diploma thesis on crisis management at LINET Group concludes by recommending the establishment of strong security policies, the creation and regular testing of a cyber incident response plan, and improvements in communication during crises. It emphasizes the importance of conducting independent cybersecurity audits and regular, practical training for employees to strengthen the organization's defenses. The thesis also highlights the necessity of maintaining updated and tested business continuity and disaster recovery plans to effectively manage and minimize the impact of crises. These measures aim to bolster LINET Group's resilience against various crisis scenarios.

KEYWORDS

Crisis Management, Cybersecurity, NIS II Directive, Risk Assessment, Business Continuity, Regulatory Compliance, Healthcare Sector, Stakeholder Engagement, Scenario Planning, Cyber Incident Response

JEL CLASSIFICATION

K23: Regulatory Law, M21: Business Economics, O32: Management of Technological Innovation and R&D

UNIVERSITY OF ECONOMICS AND MANAGEMENT
Nárožní 2600/9a, 158 00 Prague 5, Czech Republic

FINAL THESIS ASSIGNMENT

Name and surname:	Petr Němeček
Study program:	Master of Science (MSc.)
Study group:	DEMMA07
Title of the thesis:	Crisis management in LINET Group
Content of the thesis:	1. Introduction 2. Theoretical-methodological part Risk and threat, crisis and crisis management, strategy in crisis conditions, work methodology 3. Analytical part Presentation of the organization, analysis of the organization from the point of view of crisis management, evaluation of results, proposal of measures and recommendations for the organization 4. Conclusions
References: (at least 4 sources)	• COLE, T. A., VERBINNEN, P. Collaborative Crisis Management: Prepare, Execute, Recover, Repeat. Chicago: University of Chicago Press, 2022. ISBN 978- 0226821375. • FOTR, J., SOUČEK, I. Scénáře pro strategické rozhodování a řízení: Jak se efektivně vyrovnat s budoucími hrozbami a příležitostmi. Praha: Grada, 2019.240 s. ISBN 9788027120208. • FRASER, J. R. S., QUAIL, R., SIMKINS, B. Enterprise Risk Management: Today´s Leading Research and Best Practices for Tomorrow´s Executives. New Jersey: John Wiley & Sons, 2021. 944 p. ISBN 9781119741480. • WENZEL, M., STANSKE, S., LIEBERMAN, M. B. Strategic responces to crisis. Strategic Management Journal, 2020, vol. 42, no 2, p. 1-12.
Schedule:	• Aim and methods until 28 Februar 2024 • Theoretical part until 31 March 2024 • Results until 30 April 2024 • Final version until 1 May 2024
Supervisor:	doc. Enzo Essenza, D.Phil., M.P.A

prof. Ing. Milan Žák, CSc.
rector

In Prague 1. 12. 2023

Prof. Ing. Milan Žák CSc.

Digitálně podepsal Prof. Ing. Milan Žák CSc.
DN: cn=Prof. Ing. Milan Žák CSc., c=CZ, o=Vysoká škola ekonomie a managementu, a.s., givenName=Milan, sn=Žák, serialNumber=ICA - 10393535

Content

List of abbreviation

BCM	Businnes Continuity Management: p.6., p.13
BCP	Business Continuity Plan: p.7, p.13, p.36, p.74, p.83, p.92, p.94, p.98
CIA	Confidentiality, Integrity, and Availability: p.47, p.53. p.57, p.60. p.63
CERT	Computer Emergency Response Team: p.97
CMT	Crisis Management Team: p.26
CS	Communication System: p.46
DRP	Dissaster Recovery Plan: p.7, p.13, p.36, p.74-76, p.86, p.87-92, p.94-95, p.98
DRT	Disaster Recovery Team: p.78
EDR	Endpoint Detection and Response: p.36
EMS	Environmental Management System: p.30
EMT	Emergency Management Team: p.78, p.80, p.86
ESG	Environmental, Social, and Governance: p.30
HR	Human Resources: p.27
HRO	High Reliability Organizing: p.18
HW	Hardware: p.8, p.93, p.98
ICT	Information and Communication Technology: p.33, p.81
IS	Information System: p.45
IT	Information Technology
ISO	International Organization for Standardization: p.6, p.14, p.25. p.27, p.30, p.67
KBI	Kyberneticko bezpečnostní incident: p.7
KBU	Kyberneticko bezpečnostní událost: p.7
MDR	Medical Device Regulation: p.30
MDSAP	Medical Device Single Audit Program: p.30
MFA	Multi-Factor Authentication: p.33, p.37.-38.
MTDL	Maximum Tolerable Data Loss: p.75
MTO	Maximum Tolerable Outage: p.75
MRSL	Minimum Required Service Level: p.75
NCISA	Czech National Cyber and Information Security Agency: p.95-96
NIS II	The Network and Information Security ver.2
NIST	National Institute of Standards and Technology: p.19-21
NUKIB	Národní úřad pro kybernetickou a informační bezpečnost: p.7, p.35, p.77, p.81
OT	Operational technology: p.84, p.98, p.101
PR	Primary Assets: p.58, p.72-3, p.97
PO	Supporting Assets (from Czech language „podpůrný“): p.97

QMS	Quality Management System: p.30
RDP	Remote Desktop Protocol: p.32-33
RTO	Recovery Time Objective: p.7, p.13, p.42, p.47, p.75-76, p.80, p.86, p.88, p.97
RPO	Recovery Point Objective: p.7, p.12, p.42, p.47, p.75, p.80, p.86, p.88, p.97
RACI	Responsible, Accountable, Consulted, Informed: p.27, p.31, p.67-68, p.73.
SLA	Service Level Agreement: p.12, p.42, p.47, p.88, p.95, p.97
SW	Software: p.8
SCCT	Situation Crisis Communication Theory: p.18
TFEU	Treaty on the Functioning of the European Union: p.96
VPN	Virtual Private Network: p.32-33, p.36-37, p.97, p.100

List of pictures

List of tables

1 Introduction

Problem Statement/Context: In the current era, marked by rapid technological advancements and unpredictable global challenges, crisis management is increasingly recognized as an essential component of strategic management within organizations. It is believed that effective crisis resolution starts with a clear vision of its conclusion, a principle that may seem counterintuitive initially. This proactive approach to planning and anticipating challenges before they manifest is deemed vital for sustaining an organization's resilience and adaptability in an uncertain and dynamic environment.

Topic Definition: This thesis is focused on the implementation of the aforementioned principle within the context of crisis management at LINET Group, a leader in the international manufacture of medical technology and beds. The integration of strategic planning and the anticipation of potential crisis scenarios into corporate governance at LINET is examined, and how this preparation aids in the organization's ability to effectively respond to unforeseen events is explored.

Goals: Several goals are set forth by this study: to analyze the existing approaches to crisis management within LINET, to identify potential areas for improvement, and to innovate within these processes. Additionally, the aim is to demonstrate how a comprehensive crisis management strategy can benefit not only the organization but also contribute positively to the healthcare sector and beyond.

Research Question: How can the application of the 'begin with the end in mind' principle in crisis management strategies enhance organizational resilience and operational continuity at LINET Group?

Hypotheses:

- It is hypothesized that the application of proactive crisis management strategies will significantly enhance the resilience and sustainability of LINET Group.
- It is also proposed that the effective implementation of these strategies will serve as a model for other organizations within the healthcare industry and other sectors, contributing to a more stable and resilient global economy.

Theory Statement: The theoretical framework of this research is built upon the principles of crisis management, strategic foresight, and organizational resilience, exploring how these can be effectively applied in a real-world business context.

Method Statement: The methods employed in this study include a review of secondary literature, interviews with key stakeholders at LINET, and case studies on crisis management implementation. Data gathered are analyzed through a comparative case study approach, emphasizing the interpretation of empirical data within the theoretical framework established.

Boundaries and Limitations: This research is constrained by its focus on LINET Group and may not directly apply to organizations outside the healthcare technology sector without modifications. Additionally, the interpretation of data might be influenced by subjective biases of the respondents.

Structure: The thesis is structured into several key sections: an introduction that outlines the theoretical and practical relevance of the study, a literature review that frames the current knowledge and gaps, a methodology section that details the research approach, followed by an analysis and discussion of the findings, and concluding with recommendations for future research and practical applications.

Global and European Union Benefits: It is envisioned that the improvements in crisis management explored in this thesis will not only strengthen the resilience and sustainability of LINET Group but will also have far-reaching impacts. Effective crisis management is seen as crucial for reducing environmental impacts, improving global quality of life by minimizing societal disruptions during crises, and enhancing public trust in technological advancements and healthcare services.

Building a House Analogy: To make the complex concepts of crisis management more comprehensible, an ongoing analogy of building a house is incorporated. Just as careful planning, the right tools, and an understanding of potential challenges are required to construct a resilient structure, effective crisis management requires a robust framework, akin to laying a foundation. The integration of specific strategies and protocols is compared to the detailed work of installing essential systems within a house. This analogy will be revisited throughout the thesis, illuminating theoretical discussions with practical examples, thereby bridging the gap between abstract concepts and tangible implementations (beginning on page 28).

2 Teoretical-Methodological Part

Crisis management is considered a strategic and tactical necessity of leadership, which can positively or negatively affect the competitive capabilities and potential for long-term success, survival, and sustainability of organizations or nations. Therefore, crisis management should be integrated into the overall strategic and tactical plans of organizations and nations. Organizational leaders should be equipped with a crisis management process that is capable of being consistent and easily replicable. In addition, an example of integrating crisis management into an organizational strategic plan is provided. Recommendations for future research in crisis management are also presented (Taneja, S., Pryor, G, M. and Zhang, L., 2010).

In these chapters, individual aspects of crisis management are discussed with overlap to other areas such as risk assessment, human resources, public relations, legal considerations, and emergency response planning.

2.1 Crisis and Crisis Management

Crisis management involves making strategic decisions in a complex and unstable situation to mitigate the damage inflicted by a crisis. This process can be divided into three stages: pre-crisis, crisis response, and post-crisis recovery. The pre-crisis phase encompasses steps taken for preparation and prevention, such as risk assessments and the development of crisis management plans. The crisis response stage involves the organization actively managing and responding to the immediate effects of the catastrophe, focusing on minimizing impact and maintaining essential operations. Finally, the post-crisis phase focuses on learning from the crisis, analyzing outcomes, and preparing for future crises by adjusting strategies and plans based on lessons learned (Bassim, M. et al., 2021).

Crisis management entails managing crises in a way that minimizes damage and facilitates rapid recovery for the affected organization. Properly addressing a crisis is crucial for maintaining a company’s public image. Crises can manifest in various forms, including technological, financial, and reputational challenges, among others. Therefore, it is advisable for companies to develop and maintain a comprehensive crisis management plan in advance to ensure preparedness and resilience (Institute, F. C., 2020)

The pre-crisis phase involves preparation and risk assessment to minimize the impact of potential crises. During the crisis response phase, the organization implements its crisis management plan and strategies to effectively address the situation. The post-crisis recovery phase focuses on restoring normal operations and rebuilding any aspects of the organization that were adversely affected (Taneja, S., Pryor, M. G., and Zhang, L., 2010).

Crisis management is regarded as a strategic and tactical leadership imperative, which ought to be integrated into the overall strategic and tactical plans of organisations and nations. It is a strategic framework within which the security of network and information systems across EU member states is addressed (Crisis Management, 2022).

Each crisis, irrespective of its category, is subjected to various phases depending on the timing of its occurrence, with each phase impacting the organisation differently. These include the Pre-crisis, Acute, Response, and Recovery phases. It is characterised by the factors that precipitate it. There are primarily four main categories of critical situations, determined by the causes of the crisis, which can arise from either internal or external factors of the organisation and may be classified as 'technical-economic' or 'human-organisational-social' factors. (Lemonakis, C. and Zairis, A., 2020)

2.1.1 Types of Crises

Most often, crises are divided into external and internal, with external crises being those whose source stems from the external environment of the company and internal crises being defined by their origin being directly from the company (Zuzák, Konigová, 2009). They can also be divided into unintentional and intentional, depending on the intention with which the crisis was created. Some types of crises are listed below.

Accidental disasters are those that happen unintentionally by human cause. Fire is one example of accidental disasters that can affect the workforce and leave a lot of damage to the entire organization. Especially in fields such as mining and construction, that involve physical labor and operation of large machinery, drastic accidents that can happen to the workforce in the performance of their duties can lead to serious consequences (Institute, F, C., 2020).

Accidental disasters are in today's rapidly changing world for to enhance the effectiveness of crisis management strategies and processes (Heath, W, R., 1998).

Natural disasters are generally environmental crises that are beyond human ability to prevent. Earthquakes, tornadoes, and floods are examples of natural disasters (Institute, F, C., 2020).

Financial crises would be a huge problem for any organization but is predictable to quite an extent when compared with other types of crises. Such a crisis would basically involve the organization heading in the direction of bankruptcy (Crisis Management, 2014).

Technology disasters are most undertakings in an organization involve technology in one way or another. In some cases, a slight disruption in a company's technology structure can cause all operations to come to a standstill. Some technology crises can happen accidentally, while others can be maliciously caused. Under technology disasters, you will find examples such as (Institute, F, C., 2020).

Political & Social with the current political climate the world over, you may also want to take into consideration any threats to security and any form of terrorist aktivity (Crisis Management, 2014).

Malevolence crisis – is not a standard term in the crisis management field, but it can be a situation in which an organization faces deliberate malicious acts, attacks, or manipulation by external actors, such as cyber attacks, terrorist threats or attacks on reputation. In this context, a "malevolence crisis" could be a crisis in which an organization faces acts of malice or malicious attacks that can cause serious damage to their operations, reputation or even to people's lives. Criminal technology attack by opponents; hostile employees with malicious intentions of destabilizing the organization (Lemonakis, C. and Zairis, A., 2020). A subset can also be **Cybercrime crisis** – a situation that arises because of a cybercrime or an attack on an organization's information technology and digital systems. This type of crisis can have serious consequences on the functioning of the organization, including threats to data confidentiality, systems integrity, service availability and the organization's reputation. Cyber attacks can take various forms such as malware attacks, ransomware, phishing, data leaks, website attacks or network attacks. These attacks can lead to financial losses, reputational damage, loss of credibility with customers and partners, legal repercussions, and other negative impacts. Intentional theft crime by technology. Critical virus attacks - Accidental or maliciously infected (Lemonakis, C. and Zairis, A., 2020).

There are significantly more types of crises but listing them all would be beyond the scope of this thesis.

2.1.2 Characteristicss of Crisis

Crisis is a sequence of sudden disturbing events harming the organization. Crisis generally arises on a short notice. Crisis triggers a feeling of fear and threat amongst the individuals (Crisis Management, 2022).

The points are:

1. **Unexpectedness**: crises are usually unexpected events or situations that organizations did not anticipate or for which they were not properly prepared (Alzatari, A, A, M. and Ramzani, R, S., 2019).
2. **Escalation**: crises often escalate rapidly and can spread or worsen if not properly managed or stopped in time (Fraser, J. R. S., Quail, R., Simkings, B., 2021).
3. **Unpredictability**: the consequences of a crisis and the way it will unfold may be unpredictable or difficult to predict (Fraser, J. R. S., Quail, R., Simkings, B., 2021, page 168)
4. **Stress**: crisis situations often cause high levels of stress, pressure and emotional strain on the parties involved (Alzatari, A, A, M. and Ramzani, R, S., 2019).
5. **Impact**: crises can have long-term effects on an organisation, including financial losses, reputational damage, loss of credibility and other negative consequences (Alzatari, A, A, M. and Ramzani, R, S., 2019).
6. **Running the company**: crises often disrupt the normal running of an organisation and can lead to disruption of operations, services, or processes (Fraser, J. R. S., Quail, R., Simkings, B., 2021).
7. **Response**: effective crisis management requires a quick and efficient response to minimize damage and restore normal operations (Alzatari, A, A, M. and Ramzani, R, S., 2019).
8. **Collaboration**: crisis management often requires collaboration and coordination between different teams, departments, agencies, and other stakeholders (Fraser, J. R. S., Quail, R., Simkings, B., 2021).

These characteristics of a crisis help organizations better understand the nature of crisis situations and prepare to manage and resolve them (Crisis Management, 2022).

2.1.3 Stages of Crisis: Preparation, Response, and Recovery

Crisis management involves three key stages: preparation, response, and recovery (Alzatari, A, A, M. and Ramzani, R, S., 2019)

During the preparation stage, organizations need to anticipate and plan for potential crises by conducting risk assessments, developing crisis management teams, and creating crisis communication plans (Taneja, S., Pryor, G, M. and Zhang, L., 2010).

During the response stage, organizations must effectively and swiftly address the crisis by implementing their crisis management plans and strategies. This includes disseminating accurate information, coordinating with relevant stakeholders, and mobilizing resources (Taneja, S., Pryor, G, M. and Zhang, L., 2010).

During the recovery stage, organizations focus on restoring normal operations and rebuilding their reputation (Taneja, S., Pryor, G, M. and Zhang, L., 2010).

Western organizations typically adopted a four-stage model: prevention, preparation, response, and recovery (Alzatari, A, A, M. and Ramzani, R, S., 2019).

2.2 Crisis Management Versus Business Continuty Management

When dealing with crisis management within companies, it is important to look at a similar area, BCM namely Business Continuity Management (BCMpedia, 2020). Often these terms are used interchangeably, and it is true that in some situation's certain steps overlap. The primary focus is on managing unexpected events or crisis situations that may threaten the functioning of the organisation, where risks may arise from a variety of factors such as natural disasters, accidents, terrorist attacks, financial problems, reputational damage, etc (Alzatari, A, A, M. and Ramzani, R, S., 2019).

Crisis management focuses on solving the problem immediately, minimizing damage, protecting lives and property, preserving the reputation of the organization, and restoring normal operations as soon as possible and this is where the intersection with business continuity management occurs. This deals with planning and implementing measures to ensure that the organisation can continue to operate its critical functions in the event of a crisis (Wenzel, M., Stanske, S., Lieberman, M. B, 2020).

BCM considers a wider range of potential threats, including those that are not as dramatic as a crisis, such as systems failure, supplier unavailability, epidemics, legislative changes, etc. BCM focuses on planning and implementing measures that minimize business disruption and allow the organization to continue operations even in difficult conditions (BCMpedia, 2020).

Therefore, the primary assets of the two managements are different. The primary activities of emergency management include rapid decision making, communication with the public, coordination of rescue and recovery operations, and adapting to the situation to minimize impacts (Fraser J. R. S., Quail R., Simkings B., 2021). In contrast, business continuity management is primarily about identifying critical processes and resources, creating business continuity plans, regularly testing, and updating those plans, and creating contingencies to ensure continued operations (BCMpedia, 2020).

Simply put, while crisis management deals with the immediate response to a crisis and its consequences, business continuity management focuses on longer-term planning and ensuring the continuation of the organization's operations in the face of various types of potential threats (Alzatari, A, A, M. and Ramzani, R, S., 2019).

However, it is important to have both set up as individual building blocks for the successful survival of the company. The primary focus should be to identify the assets, the type of assets, the values of the assets, and on top of that to name the vulnerabilities and threats to the asset so that the possible impacts can be anticipated in some processes and realistic and effective crisis action can be planned to limit the damage caused (Fraser, J. R. S., Quail, R., Simkings, B., 2021). Shield all this with risk analysis (described in section 2.3) and together with the other parts create a business continuity management, elements of which can be used in crisis management. As part of this linkage, BCM is discussed below, elements of which will be used within the analytical part of the LINET Group case study.

2.2.1 BCM - Business Continuity Management

Alongside other managements, business continuity management is the most general generic framework resulting, for example, from ISO 22301:2019 (Hendaryatna et al., 2023, p. 1159) or from the proposals of the new Cyber Security Act.

According to ODOK (2024) and Fotr J., Souček I. (2019) of the draft decree on security measures of a regulated service provider in the regime of higher obligations, business continuity management should include:

a) Rights and obligations of responsible persons,
b) Business continuity management objectives for individual services,
c) Prioritization of individual services,
d) Methods of crisis communication and reporting,
e) Communication matrix with key persons for each service,
f) Escalation procedures for crisis situations,
g) Catalogue of crisis scenarios,
h) Procedures for starting and stopping the system, for restarting or resuming the system after a failure, and for handling error conditions or abnormal events,
i) The method and period of testing of each business continuity plan and recovery plan,
j) Procedures for the implementation of measures issued by the NUKIB.

The objective of business continuity management is to assess risks and analyse impacts based on the outputs (BCMpedia, 2020):

a) To set minimum service levels for the company individual agencies,
b) To ensure the security and continuity of ICT (Information and Communication Technology) services in the event of a KBI (cyber security incident – Czech language: kyberneticko bezpečnostní incident), KBU (cyber security event – Czech language: kyberneticko bezpečnostní událost), emergency or disruption of ICT (Information and Communication Technology) services,
c) Set business continuity management objectives with respect to the minimum level of service provided, IT (Information Technology) recovery time and data recovery point,
d) Initiate steps to ensure that services are restored to the required level,
e) To minimize damage to company property or assets resulting from the incident.

Each ICT element has a defined RTO (recovery time of operation) and RPO (data recovery point). Minimum service level means the minimum range of services of ICT elements that is acceptable for the use, operation, and management of the service. RTO means the time when, after a KBI or failure, the ICT elements reach the specified level of service. Data recovery point means the point at which data must be restored to the appropriate service level. In other words, the RPO shall define the amount of historical data that the obliged entity may lose. Full data recovery point means the point at which data is fully recovered. To meet business continuity objectives, BCP (Business Continuity Plans) and DRP (Dissaster Recovery Plans) are developed, managed, and regularly updated by the Cybersecurity Manager (BCMpedia, 2020).

Assets

To properly manage business continuity, it is important to define the assets to be protected under this type of management. An asset is therefore anything that has value to the organisation and needs to be protected. Assets are divided into (Jenkins, R., 2018):

- **primary**: a key element that is directly linked to the organisation's core objectives and business processes, e.g. corporate know-how, patents, information, services, or processes that are essential to the operation of the company.
- **supporting**: supports the primary assets and processes of the organisation and ensures their operation, e.g. buildings, communication facilities, staff, etc. Supporting assets can be replaced by another system, e.g. specific HW and SW can be replaced by alternatives without changing the service provided, employees can be replaced, the same for the supplier - changing them does not change the purpose and goal of the primary assets.
- **technical**: includes the hardware, software and infrastructure elements used to manage and protect information.

Asset management consists of identifying, evaluating, recording, and reviewing the primary and supporting assets of an organization (Cybrela, 2024).

Table 1 Primary asset assessment areas according

Area	**Example**
(a) the extent and relevance of the personal data, special categories of personal data	Leakage of personal data of an individual.
(b) the extent of any legal duties or other obligations or business secrets involved	Infringement of the obligation to publish documents on an electronic official notice board which must be always accessible by remote access. Breach of contract and resulting penalties. Trade secret leak. Violations of legislation and resulting fines.
(c) the extent of the disruption to internal management and control activities	Incompleteness or modification of information needed for management decision-making and control activities.
(d) damage to public, commercial or economic interests and possible financial loss	Unavailability of invoice information based on the unavailability of the economic system. Unavailability of information about potential business opportunities and the resulting lost profits. The unavailability of websites, for example, can lead to the public not being informed about important facts (floods, environmental disasters, etc.).
(e) impacts on the provision of essential services	Disruption of all information and services related to the regulated service and the organization's core business objective (purpose for existence).
(f) the extent of disruption to normal activities	Disruption of personnel, economic, building and fleet management activities, inability to receive data messages, etc.
(g) the impact on the preservation or protection of reputation	Non-compliance. Leaked internal information.
(h) impacts on the safety and health of persons	Inability to provide basic income, food, access to health care, freedom, etc. Potential for injury and loss of life.
(i) impacts on international relations	Leaks from foreign partners. A leak from a partner that is part of an international concern.
(j) impacts on users of the information and communication system	Loss of user access to the service due to its unavailability.

Source: own processing, Cybrela (2024)

The table 1 outlines the primary asset assessment areas in a business context. It highlights the potential risks or impacts in various areas such as personal data, legal duties or obligations, internal management disruption, public, commercial, or economic interests etc. Each area is accompanied by an example. This table serves as a comprehensive guide for businesses to assess and manage potential risks (Cybrela, 2024).

2.2.2 BIA (Business Impact Analysis)

Using impact analysis, the organisation assesses and documents in detail the potential impact of various incidents on its operations, or on ensuring the operation of its primary assets. Impact analysis and risk analysis are the cornerstones for developing a business continuity management strategy. (Quinn, S., Ivy, N., Chua, J. (eds.), 2022, p. 3-4)

In the case of impact analysis, in addition to the basic attributes of information security (confidentiality, integrity and availability), is also considered the attribute of loss (the case in which data would be lost) (Quinn, S., Ivy, N., Chua, J. (eds.), 2022, p. 4). Each assessment attribute is broken down in more detail to make the estimate of the impact on a given area for each asset as accurate as possible.

Evaluation of Attributes:

Availability (Quinn, S., Ivy, N., Chua, J. (eds.), 2022, p. 4)

- What would be the impact of the unavailability of the asset on the area?
- The evaluation is carried out in time slices from 15 min. to a month or more.

Loss (Quinn, S., Ivy, N., Chua, J. (eds.), 2022, pp. 10-12)

- What would be the consequences of losing the asset for the area?
- The evaluation is performed at time intervals from 15 min. to complete data loss.

Confidentiality (Quinn, S., Ivy, N., Chua, J. (eds.), 2022, pp. 10-12)

- What would be the consequences of a breach of confidentiality of the asset for the area?
- The assessment is made in terms of the impact of disclosure within the organisation (i.e. to employees), to contractors (i.e. to third party employees) or outside the organisation (i.e. to the public).

Integrity (Quinn, S., Ivy, N., Chua, J. (eds.), 2022, pp. 10-12)

- What would be the consequences of modifying/changing the data of the asset for the area?
- The evaluation is performed in terms of small-scale data modification (unintentional modification, minor errors) or large-scale data modification (intentional modification, major errors).

The list of impact areas is based on NIS II (Annex 1, 2022) of the draft Cybersecurity Decree relating to the higher regime and includes the following areas:

- Data protection - impact on data subjects,
- Data protection - financial harm to data subjects,
- Trade secrets,
- Legal and contractual obligations,
- Disruption of internal management and control activities,
- Public order,
- Financial losses,
- Provision of essential or basic services,
- Disruption of normal activities,
- Loss of credibility,
- Personal safety and health,
- Impact on IS users,
- International Relations,
- Criminal law proceedings,

Picture 1 The format of list of impact areas is based on Annex 1 of the draft Cybersecurity Decree relating to the higher regime.

	Availability									Loss									Confidentiality			Integrity	
Areas of impact	Unavailability 15 min.	Unavailability 1 h	Unavailability 4 h	Unavailability 8 h	Unavailability 1day	Unavailability 2 days	Unavailability 1 week	Unavailability 14 days	Unavailability for a month or more	Data loss from backup (15 min)	Data loss from backup (1 h)	Data loss from backup (4 h)	Data loss since backup (8 h)	Data loss since backup (1 day)	Data loss since backup (2 days)	Data loss since backup (1 week)	Data loss since backup (14 days)	Complete loss of data	Disclosure within the organisation	Disclosure to contractors	Disclosure outside the organisation	Small-scale data modification	Large-scale data modification
Data protection - impact on data subjects																							
Data protection - financial harm to data subjects																							
Trade secrets																							
Legal and contractual obligations																							
Disruption of internal management and control activities																							
Public order																							
Financial losses																							
Provision of essential or basic services																							
Disruption of normal activities																							
Loss of credibility																							
Safety and health of persons																							
Impact on IS or KS users																							
International Relations																							
Criminal law proceedings																							

Source: own processing, Cybrela (2023)

Picture 1 represents Business Impact Analysis (BIA) template. It's used to assess the potential impacts of various business scenarios on different areas such as personal data protection, financial losses, human safety, and health, and more. The top row indicates different levels of unavailability timeframes, data loss timeframes and confidentiality and integrity levels. In chapter 3.2.1, within the practical part, this template is filled out (NIS II, 2022).

BIA template

Using impact analysis, the organisation sets business continuity management objectives in the form of a determination:

- **SLA** (Service Level Agreement) - an indicator that specifies the minimum level of service at which the system's goal is guaranteed to be achieved (e.g., an SLA of 95% means that the system will be available 95% of the time) (Hiles, 2023, s. 1-9).
- **RPO** (Recovery Point Objective) - an indicator of the amount of data an organization is willing to lose from the last backup to the occurrence of incidents/crises (Mills, 2023).

- **RTO** (Recovery Time Objective) - A measure of the time to restore services or access to information after an incident/crisis (Mills, 2023).

2.2.3 BCP, DRP and PDCA

BCP: Business Continuity Plans are referenced immediately following the review of Business Continuity Management (BCM). These plans, designed to recover identified Primary Assets (PR), address the restoration of the company's core activities impacted by various recognized risks, such as accidents or disasters. BCP encompass non-technical aspects including personnel and suppliers. For instance, they may cover the operational impacts of a pandemic, specifically addressing issues such as a staff shortage and its subsequent effect on business operations (Dey, 2011, p. 229-232).

DRP: If the cause of an incident or crisis is non-technical, the solution should be found in the BCP, but if the cause is technical, then the BCP refers to specific disaster recovery plans, i.e., DRPs. These plans deal with the recovery of the company's support systems, regardless of the cause - the goal is to get the support systems that keep the primary assets functioning up and running as soon as possible. They cover only the technical areas in as much detail as possible (Sawalha, 2021, p. 351-361).

PDCA: Plan-Do-Check-Act is a closed-loop system. This ensures the learning from the 'do' and 'check' stages are used to inform the 'act' and subsequent 'plan' stages. In theory this is cyclical, however it's more of an upward spiral as the learning moves you on each time you go through the process (Watson, 2022, p. 1-2).

2.3 Risk Management

The primary difference between risk management and crisis management is when it is applied. Risk management occurs or should occur before a problem or crisis occurs. Jirásek, Novák, and Požár (2015, p. 202) in defining the risk management process and risk management per se, emphasize that it is an activity that must be coordinated and take risks into account. The process as such then needs to be systematic, where it must consider the context and analyse, monitor, and then review risks. Půjček, Páleníková (2022, p. 9), then consider risk management as a specific type of management comprising the phases of identifying the risk, then analysing, then managing the risk and finally monitoring the risk. These authors stress that the key thing about risk management is not to forget the objectives of the company, whether economic or otherwise. Thus, risk management should be effective.

Risk management is also a key part of cybersecurity, and since cybersecurity as such aims to protect not only information technology but also business as such, the definitions provided by Půjček and Páleníková are applicable in this thesis (2022, p. 9).

Other definitions of risk management can also be found in the literature, for example the National Office for Cyber and Information Security on its website (2024, Annex 14) to the Cybersecurity Decree provides wording that reflects a different perspective than a purely business and practical one but leans more towards the legislative wording of risk management in the context of cybersecurity. When this authority emphasises that this should include the development of documentation or methodology for risk assessment, risk management plan, etc. The decree that the authority cites is the now still effective Decree No. 82/2018 Coll. on Cybersecurity, which in Article 2(i) states, similarly to the above, that it is an activity that

includes the assessment of risks, the selection and application of measures to manage the risks and the subsequent monitoring and review of the risk. In addition, it includes the need to share information about the risk.

The decree is also loosely linked to resources from ISO 27005:2022 (ISO, 2024), where clause 3.2.1 says that the risk management process should be systematic, applying policies and procedures to practice, communicating, consulting the context of actions, and traditionally then analysing, addressing risks, and then monitoring and reviewing these.

Tayllorcox (2024) in turn provides a view of risk management associated with an information security management system (ISMS), considering it to be a process that identifies, then assesses and reviews how a company's revenue or capital may be at risk.

I believe that all these definitions lead to the conclusion that risk management is an ongoing activity that is based on the subjective beliefs and needs of a company, where, crucially, what it considers to be the risks that threaten its existence and success in the marketplace. However, it is not only based on the company's opinion, but must also be based on objective elements and best practice methodologies and procedures (Assurancelab, 2023).

2.3.1 Risk

A key concept in risk management is the concept of risk and how it is calculated. Jirásek, Novák, Požár (2015, p.99), consider it as a certain danger or possible damage or loss, but also the uncertainty of achieving the goal or the possibility that the threat will exploit the vulnerability of the asset and thus cause damage to the company. The authors thus provide basic definitions of risk (MVČR, 2024).

The Home Office then commented on this concept by stating that it is the possibility that an event which is undesirable will occur with a certain probability. According to Ministry of Foreign Affairs Security Strategy of the Czech Republic (2003, p. 9), a risk is here derived by the Department from a specific threat, where its level is calculated as the probability of negative consequences arising from that threat and from vulnerability, all of which is then reflected in the risk analysis.

Tayllorcox (2024), then states that a risk is a possible event that may cause a company to lose or jeopardize its ability to achieve its objective. As a calculation of risk here, Tayllorcox chooses the probability of threat, the vulnerability of assets to the threat and the potential impact on the company.

The risk under Article 6(9) of the NIS II (2024) Directive is the potential loss or disruption due to an incident, and this risk is then expressed as a combination of the magnitude of the overall loss or disruption and the likelihood of the incident occurring.

NIS II (2022, annex No. 2 to Decree No. 82/2018) on cyber security, uses risk calculation as a multiplication of impact, threat, and vulnerability. Compared to the new proposed legislation, i.e. the draft Decree on security measures of a regulated service provider under the regime of higher obligations, there is a slight difference in the possible calculation of risk, where in Annex 2 of this Decree the risk is expressed as a multiplication of the value of the asset, threat, and vulnerability. However, multiplication is not the only possible approach, but it is the recommended approach in the proposed Order. ISO 27005 (ISO, 2024) then defines risk in clause 3.1.3 as "the *effect of uncertainty on targets"*, and these are generally associated with a negative outcome.

Kolouch (2019, p. 68) then goes on to state that risk is the probability of an event occurring that we do not want to happen, and the degree of this probability is expressed through risk analysis. An alternative view of risk can be found in the literature, where Půjček, Páleníková (2022, p. 10) define it as a future event that is the counterpart of an opportunity and is associated with negative impacts.

Thus, it can be summarised that risk is a future negative situation, that a threat will exploit a vulnerability and cause damage to the company, its probability is then determined by one of the calculations outlined.

2.3.2 The Threat

Jirásek, Novák, and Požár (2015, p. 52), say that a threat is a possible cause of an unintentional incident where there is a possibility of damage to the system or to the company. The Home Office then states that a threat is anything that has the capacity to cause damage to the values and interests protected by the state, and its magnitude is determined by how much damage it can cause over time. This is one perspective on assessing the magnitude of a threat.

Tayllorcox (2024) then states that a threat is primarily a condition or activity that has the potential, either intentionally or accidentally, to cause loss or even alteration, disclosure, or unavailability or other damage to information and the resources to process it, all of which can cause loss to society.

ISO 27005:2022 considers the threat view in the context of ISMS, where a threat is a possible cause of an information security incident that, as mentioned above, can cause damage to a system, or even damage the company as a whole. This standard also provides examples of typical threats in its Annex A.2.5.1. Examples include flooding, supply system failure, social engineering, media theft and even staff shortages. These are just a few of more than 50 example threats (ISO, 2024).

Interesting is also the viev of the draft cyber law on portal ODok (2024) on the definition of a threat, the one in Section 2(1)(c), where a threat is not only a circumstance or event but also actions that may cause a cyber security event or incident and may also cause damage or disruption or adversely affect asset or other persons. However, examples of threats as in the ISO are not found here, these are listed in Annex 3 of the draft Decree on security measures of a regulated service provider under the regime of higher obligations. There are far fewer examples of potential threats, such as dependency on a supplier, malicious code or loss, theft, or damage to an asset.

Threat is thus one of the basic concepts of risk management and can generally be understood as something that threatens a company and that must be dealt with in risk assessment. Thus, it can simply be considered as something that causes risk management to be concerned with because it is the threat that can cause harm to the company (Puzder D., 2023).

2.3.3 Vulnerability

Vulnerability is another concept found in risk management. Jirásek, Novák, and Požár (2015, p. 136) states that it is a weakness that can be exploited by one or more threats. This is almost identical to the definition given in the draft of the new Cybersecurity Act on Portal ODok (2024).

As with threats, we find a definition within ISO 27005:2022, specifically in clause 3.1.10, which states that it is a vulnerability that can be exploited in such a way that a negative consequence occurs. In the annex to Table A.11, we also find examples of typical vulnerabilities, which include uncontrolled copying, poor password management, absence of staff, lack of security training, location of the site in an area prone to flooding, or no continuity plans (ISO, 2024).

The same vulnerabilities are also found in ISO (2022, annex 3) of the draft decree on security measures of a regulated service provider under the regime of higher obligations, which, like the threats, are fewer than those listed in the ISO standard. Specifically, these include, for example, a lack of staff with the necessary level of expertise, insufficient protection of assets or, for example, inappropriate security architecture. According to Tayllorcox (2024) then states that a vulnerability is a weakness that can be exploited specifically by a threat and gives the example of never changing a password.

Kolouch (2019, p. 72) then categorises vulnerabilities into known and unknown vulnerabilities, i.e. whether the public knows about them because they have been published or not.

The negative of vulnerability exit depends on the presence or absence of a threat. If a company has vulnerabilities but the threat does not exist it does not move within risk management but already change management. If there is both a vulnerability and a threat, this must be addressed within risk management because it is the threat that can cause harm to the company despite the vulnerability, and the likelihood of this happening or not is the risk in question. Thus, we can see a close relationship between these concepts, which in effect form the basis of risk management as such (Tayllorcox, 2024).

2.3.4 Risk Analysis

Regarding the concept of risk analysis Jirásek, Novák, Požár (2015, p. 18) states that it is a process of understanding what the nature of the risk is and determining its level. Tayllorcox (2024) then states on it that it is the process of determining the risk, the likelihood of its occurrence, the subsequent impact, and the adoption of measures to mitigate it, where he considers it to be synonymous with risk assessment.

The National Cyber and Information Security Authority states on its website (2024, annex 14) to the Cybersecurity Decree that, a risk analysis includes an assessment of the combination of vulnerability and threat relative to assets and a calculation of a final risk value.

Zapletalová (2020) in her lecture on risk management at Silesian University presents two basic approaches to risk analysis as such - qualitative and quantitative methods. According to the author, the qualitative method is determined by the fact that risks are expressed in terms of a range, and this method is simpler, more subjective, and faster, but it lacks an unambiguous financial expression of risks. The qualitative method, according to Zapletalová, is then focused on the mathematical calculation of risk and the probability of occurrence of a threat, which can include the impact in financial terms, most often in the form of an assumption of financial loss per year. This method is more accurate, but more time-consuming and uses special programmes and databases.

Zapletalova's (2020) view is shared and developed by the author Evrin (2021) relating to the issue of qualitative and quantitative methods. They stress that quantitative data is very difficult to obtain and very expensive and can be misleading, compared to qualitative risk analysis, which is much faster but more subjective. And that is why the authors on this page recommend using qualitative assessments in most cases and investing in qualitative analysis at most for critical issues.

On Portal ODok (2024, annex 2) of the draft Decree on security measures for the provider of a regulated service under the regime of higher obligations also specifies the risk assessment scale. Based on this scale, the risks are divided into four categories of low, medium, high, and critical risk. Based on the risk analysis, the scale is used to determine the threshold of risk acceptability, which risk is considered by the company to be low and therefore acceptable. As this draft decree states, if a company has any risk that meets this threshold of acceptability methods must be in place to manage the risk. These methods, according to the decree in question, include risk acceptance, risk reduction and elimination, risk avoidance, or risk transfer or risk sharing.

The Ministry of Labour and Social Affairs of the Czech Republic (2024) on the concept of risk management states that the method of risk management depends on the selection of the best method of managing a given risk, i.e. reducing its impact or the degree of probability with which it may occur. The Ministry then, similarly to the proposed decree above, lists risk avoidance, risk acceptance, risk reduction and risk transfer among these methods, and emphasises that these methods are intended to help the company become aware of the options for dealing with the identified risk and then select the most appropriate specific measure for each method.

Kolouch (2019, p. 71) then states that risk analysis as such is extremely challenging and not only requires knowledge of the company's assets, threats but also requires practical experience in this area. Based on the risk analysis, the author then states that it is only possible to determine the measures that should lead to the reduction or elimination of risks.

The view of the authors mentioned above is agreed upon, stating that for most cases in companies, the qualitative method of risk analysis is considered more appropriate. It is acknowledged that the choice of the method for addressing the identified risk always depends on the circumstances of the specific case, and therefore, it is not presumed to judge here which method should prevail.

2.4 Strategy in Crisis Conditions

Integrating crisis management into the strategic planning of an organization is essential for mitigating potential risks and ensuring long-term success and sustainability (Mehr, K, M. and Jahanian, R., 2016). Crisis management should be a top-down mandate, driven and implemented by all key business functions in collaboration with organizational leaders (Abrashi, G., 2018).

Proactive crisis management is imperative for organizations to anticipate, prepare for, and respond to various crises effectively (Sapriel, C., 2016). Developing and implementing crisis communication strategies (Mudalal, W, M., 2021). Implementing crisis management strategies to mitigate the effects of a crisis and maintain business continuity (Mudalal, W, M., 2021). Organizations should have a predefined crisis management plan in place to effectively respond to crises (Elzaanin, A., Ahadiat, A. and Jimad, H., 2020). Organizations should establish a coordinated response to a crisis, including implementing the crisis management plan and taking immediate action to mitigate the impact of the crisis (Alzatari, A, A, M. and Ramzani, R, S., 2019).

Integrating Crisis Management into Organizational Strategy Process

Integrating crisis management into the strategic planning process involves aligning it with the organization's overall goals and objectives. This ensures that crisis management becomes an integral part of the organization's operations, allowing seamless coordination during

challenging times (Mudalal, W, M., 2021). Leaders should emphasize the integration of crisis management, not only as a reactive measure but as a proactive approach to safeguard the organization's interests and longevity (Elzaanin, A., Ahadiat, A. and Jimad, H., 2020).

Implementing a comprehensive crisis management process as outlined above is crucial for organizations to effectively navigate through turbulent times. It allows them to not only respond to crises but also to emerge stronger and more resilient (Bundy, J. et al., 2016).

The integration of crisis management into an organization's strategy processes is essential for fostering a proactive and resilient business environment (Mudalal, W, M., 2021). By embedding crisis management into strategic planning, organizations can identify potential vulnerabilities, develop preemptive strategies, and build a culture of preparedness throughout the entire organization (Elzaanin, A., Ahadiat, A. and Jimad, H., 2020).

2.5 Theoretical Frameworks in Crisis Management

Comprehensive analysis of crisis management theories relevant to LINET Group. Exploration of models such as the Three Stages of Crisis Management Model and their application to the healthcare technology sector (Cole, T. A., Verbinnen, P, 2022).

We can have this type of models:

Crisis Management Lifecycle Model: This model divides the crisis management process into several stages, typically including pre-crisis, crisis response, and post-crisis phases. It emphasizes the importance of preparedness, response, and recovery activities throughout the lifecycle of a crisis (Porot, G., 2024).

Situation Crisis Communication Theory (SCCT): Developed by Coombs (2015), SCCT focuses on how organizations communicate during crises. It emphasizes the role of reputation, crisis responsibility, crisis type, and crisis response strategies in shaping public perceptions and organizational outcomes.

Sensemaking Theory: According to Weber, K. and Glynn, M.A. (2006, p. 1636-1642) Sensemaking theory, proposed by Karl Weick, suggests that individuals and organizations create meaning out of complex and ambiguous situations, such as crises. It emphasizes the importance of information processing, interpretation, and sensemaking processes in crisis management.

Organisational Resilience Framework: Organizational resilience frameworks focus on building adaptive capacity and robustness to withstand and recover from crises. These frameworks often incorporate elements such as risk management, organisational learning, flexibility, and agility to enhance resilience (ICOR: Resilience framework, 2024).

High Reliability Organizing (HRO): HRO theory, derived from studies of high-risk industries like aviation (Biedermann, M., Papatheodorou, A., Prowle, M., Bulatovic, I., 2024, p. 1-2) and nuclear power, emphasizes the importance of mindful organizing, preoccupation with failure, sensitivity to operations, reluctance to simplify, and deference to expertise in managing complex and high-risk environments (Cantu, J., Tolk, J., Fritts, S., Gharehyakheh, A., 2020, p. 399-401).

Complexity Theory: Anderson, P. (1999, p. 216-217) states, complexity theory views organizations as complex adaptive systems that interact with their environment in non-linear and unpredictable ways. It emphasizes the interconnectedness, emergent behavior, and self-organization of systems, which have implications for crisis management strategies.

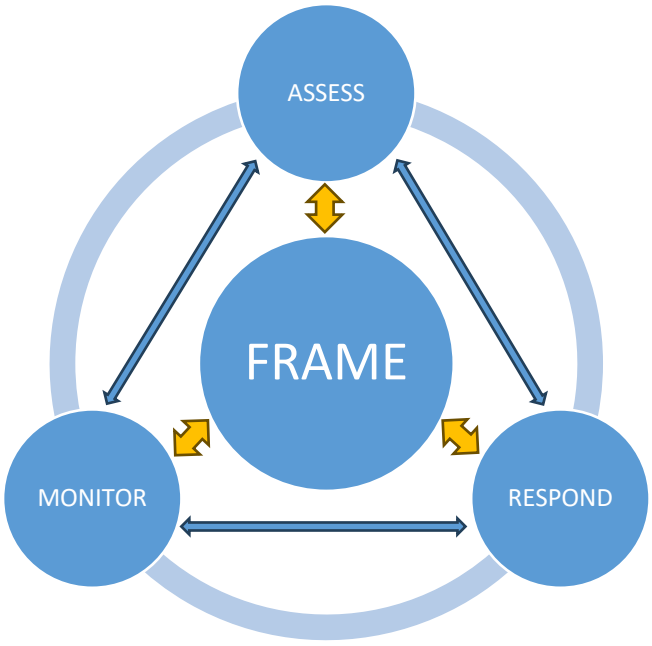
Social Network Theory: According to Scherer, C. W., Cho, H. (2003, p. x) social network theory explores the role of social relationships, networks, and interactions in crisis communication, coordination, and resilience. It examines how information flows, social capital, and network structures influence organizational responses to crises.

Integrated Risk Management Frameworks: Integrated risk management frameworks integrate risk assessment, mitigation, and response strategies across various types of risks, including financial, operational, technological, and reputational risks. These frameworks aim to provide a holistic approach to managing uncertainties and vulnerabilities in organizations.

2.6 Risk Management Approaches

The risk management processes are broken down into 4 categories, as shown in the figure below: (I.) framing risk; (II.) assessing risk; (III.) responding to risk; and (IV.) monitoring risk.

Picture 2 Risk management process



Source: own processing, Cybrela (2023)

Picture 2 represents a diagram illustrating a cyclical process involving four steps: frame, assess, respond, and monitor. This diagram is used to represent a process where each step feeds into the next, creating a cycle of continuous improvement.

To accomplish comprehensive risk management, a variety of approaches are used, each with advantages and uses. This thesis focuses on the risk assessment component of risk management.

Based on the NIST (National Institute of Standards and Technology) Special Publication 800-30 (2012, p. 6-7), a risk assessment methodology typically includes: (I.) risk model, defining key terms and assessable risk factors and the relationships among the factors; (II.) assessment approach (the aforementioned quantitative, qualitative, or semi-qualitative), defining the range of values that those risk factors may take during the risk assessment and the process by which

combinations of risk factors are found and examined in order to enable the functional combination of those factors' values to assess risk; and (III.) analysis approach (e.g, threat-oriented, asset/impact-oriented, or vulnerability-oriented), explaining the process of identifying and analysing combinations of risk factors in order to guarantee sufficient coverage of the issue space at a constant level of detail.

Organisations define risk assessment techniques, which are part of the risk management plan created at the risk framing stage of the risk management process. The corporate risk management strategy has a significant impact on risk assessment techniques. However, depending on the goal and scope of the assessment as well as the particular inputs that organizations choose to make regarding the risk assessment process, risk model, assessment technique, and analytic strategy, risk assessment methodologies can be tailored for each risk assessment (NIST, 2012, p. 4-7).

2.6.1 Risk Model

By NIST (2012, p. 8-9) risk models play a central role in risk assessment. They define the factors to be assessed (e.g., threat, vulnerability, impact) and their interrelationships. These factors serve as inputs for determining risk levels and are also crucial for effective communication of risk.

The organisation should clearly define these factors before conducting risk assessments. Precise definitions ensure consistency and effectiveness in evaluating threats, vulnerabilities, impacts, and other key aspects of risk (NIST, 2012, p. 8-9).

2.6.2 Assessment Approaches

As already mentioned above, organizations can choose from quantitative, qualitative, or semi-quantitative methods, each with its own advantages and limitations (NIST, 2012).

- **Quantitative Assessments:** employ numerical data and excel at cost-benefit analyses. However, interpreting results and accounting for uncertainty can be challenging.
- **Qualitative Assessments:** utilize descriptive categories like "high" or "low" for easier communication but offer limited ability for prioritization and comparison.
- **Semi-Quantitative Assessments:** combine qualitative and quantitative elements by using bins, scales, or representative numbers. This approach provides a balance between communication clarity and relative risk comparison.

Regardless of the chosen methodology, clear definitions and meaningful examples associated with each value scale are crucial for accurate and consistent assessments. Additionally, all methods should explicitly consider the temporal element of risk factors, incorporating timeframes into assessments of likelihood and impact (NIST, 2012, p. 14).

By understanding the strengths and weaknesses of each approach, organizations can select the most appropriate method for their specific needs and context.

2.6.3 Analysis Approaches

A risk assessment's orientation or starting point, degree of detail, and strategy to handling risks arising from similar threat scenarios are among the differences across analysis approaches (NIST, 2012).

- **Threat-oriented:** starts with identifying threats and scenarios, then vulnerabilities and impacts.
- **Asset/impact-oriented:** starts with critical assets and potential impacts, then threat events and vulnerabilities.
- **Vulnerability-oriented:** starts with vulnerabilities, then threat events and potential consequences.

Regardless of the starting point, all approaches consider the same risk factors. However, a combined approach (e.g., threat-oriented with asset/impact-oriented) can improve the analysis's rigor and effectiveness (NIST, 2012, p. 15).

Furthermore, advanced techniques can be employed to account for complex relationships between threat sources, vulnerabilities, and consequences. These techniques offer a more nuanced understanding of potential risks by considering:

- Multiple threat sources contributing to a single event.
- A single vulnerability exploited by multiple threats.
- A single threat event impacting several assets or causing various consequences.

By selecting the appropriate orientation and utilizing rigorous analysis techniques, organizations can achieve a comprehensive and unbiased risk assessment (NIST, 2012, p. 15).

2.6.4 Culture Effects

NIST Special Publication 800-39 (2012, p. 16) describes how organizational culture can influence risk management. For a variety of reasons, organizations may differ in the risk models, assessment methodologies, and analysis approaches that they favor. Cultural issues, for instance, may lead firms to use risk models that assume a constant value for one or more potential risk factors, leaving out those aspects that are included in models used by other organizations. Organizations may be more likely to use risk models (such as nuclear safety) that call for in-depth examinations utilizing quantitative evaluations due to cultural factors. Organisations may also favour semi-quantitative or qualitative methods of assessment. Organisational disparities can also occur within an organisation in addition to differences between them. For instance, early in the system development life cycle, companies might pick security policies using coarse or high-level risk models. Later, more detailed models can be used to evaluate risk to specific missions or business processes. Depending on the situation, organizational risk frameworks specify the risk models, assessment approaches, and analysis approaches to apply.

2.7 Integration of Crisis Management and Risk Assessment

Risk assessment and crisis management integration are essential elements of organisational preparation. As already outlined in the previous chapters, risk assessment serves as the cornerstone by pointing out potential dangers and weak points that might lead to a crisis. It provides vital information for proactive planning by analysing each risk's likelihood and potential impact. The development of comprehensive plans and procedures for handling recognised emergencies is how crisis management subsequently expands on this framework. Its main goals include mitigating damage, ensuring business continuity, and restoring things to normal after an incident (Lam, J., 2014, p. 150-185).

The following breakdown of this integration makes use of strategies from Enterprise Risk Management (Lam, J., 2014, p. 150-185):

Scenario Planning: Using the risks that have been identified as a basis, this technique creates a variety of crisis scenarios. Organizations can test and improve their reaction plans by visualizing possible scenarios, which will ensure a better-coordinated and efficient response during a real crisis (PWC, 2023), (Fotr J., Souček I., 2019)

Communication Procedures: It is critical to have well-defined communication procedures in place for times of crisis. These procedures guarantee accurate and timely information sharing between the company and its external stakeholders (such as the media and clients). A clear communication plan reduces uncertainty and promotes openness in crucial situations (Manley B., McIntire D. 2021).

Resource Allocation: According to Farrel, Gebre eds. (2013, p. 2-16) In order to integrate effectively, resources must be set aside for both crisis management and risk reduction. This may entail allocating funds for emergency response teams, staff training initiatives, and security measures. Organizations show their commitment to disaster preparedness by allocating resources to both proactive and reactive actions.

Frequent Reviews and Updates: As Broomes (2023) notes, crisis management plans and risk assessments are dynamic documents. It is imperative to conduct periodic reviews and updates of these plans to guarantee their continued relevance and adaptability to altering operational environments and organisational contexts. The organization's overall resilience is strengthened by this process of constant development.

Integration with Business Continuity Planning: Combining business continuity and crisis management plans is necessary for a thorough approach to crisis preparedness. This guarantees a smooth transition between emergency response and rehabilitation activities (Flinders, 2024)

This research contributes to the understanding that businesses can develop a strong and proactive strategy for crisis preparedness by combining risk assessment with crisis management. Organizations can develop a strong and proactive approach to disaster preparedness by smoothly integrating the processes of risk assessment and crisis management. This enables proactive planning and the development of effective reaction mechanisms to mitigate the impact of unforeseen crises in the future, predict possible risks, create efficient response plans, and lessen the negative effects of crises on their business and reputation (Flinders, 2024).

2.8 NIS II and Crisis Management

Regarding to Vandezande, N. (2024, p. 4) the NIS II Directive brings a more robust view of cyber security in companies, and compared to NIS I, it will affect many more companies in the EU. In its NIS II (2022, article 9) on national cyber crisis management frameworks, it states in point 4(c) that Member States must adopt national plans for responding to large-scale cyber incidents and crises, which must, among other things, consider cyber crisis management practices, including incorporation into national crisis management frameworks. NIS II therefore has implications not only for companies but also for Member States' crisis management.
By its very nature, the Directive does not directly bind companies as such, but it does provide a framework that Member States must implement in their national legislation, which they will then have to follow. In the Czech Republic, this will be a new cyber law, which is currently only in draft form.
NIS II (2022, article 21) of the NIS II Directive lays down measures to manage cyber security risks, listing in its point 2(c) the measures that will have to be put in place and, apart from business continuity management, backup management, disaster recovery, it does not forget crisis management as such.
In NIS II (2022, recital 55), the NIS II Directive goes even further, stressing the need for public-private partnerships, which are essential for sharing expertise and will also impact on crisis management as such.

2.8.1 NIS II Measures to Support Companies' Crisis Preparedness

Measures to manage cyber security risks are set out in Vandezande (2024). The emphasis here is clearly on risks, not on the crisis per se, i.e. the aim of the Directive is to prevent crises where possible through the measures mentioned, or to be prepared for them when they occur.

PECB (2023) highlights, that NIS II requires that the companies affected take appropriate but proportionate measures to address the security risks they face. These measures are to be not only technical, but also operational and organisational.

The minimum that each Member State must require companies to do includes the ten areas listed in Vandezande (2024) in connection with PECB (2023). These areas are the need for documentation - specifically a risk analysis policy and an information systems security policy. It is already apparent from the first point that risks are given extreme emphasis in NIS II. Furthermore, companies must deal with incidents, have the aforementioned business continuity management and crisis management as such. To deal with supply chain security, to ensure the acquisition, development and maintenance of networks and information systems, which should include the disclosure of vulnerabilities and their resolution.

Other documents required of companies include policies and procedures to assess the effectiveness of cybersecurity risk management measures, basic cyber hygiene procedures, and even cybersecurity training NIS II (2022, article 21). Here, the NIS II reflects that it is the human factor that is one of the most key in cybersecurity. Further documentation is to be provided on the use of cryptography and encryption. Companies must also not forget about human resource security, include access control procedures and asset pairing, and consider multi-factor authentication solutions. Finally, secure communications, including emergency communications within the entity NIS II (2022, article 21)

From the perspective of crisis management and the NIS II area, the emphasis on preparation and thus risk management (the requirement to analyse and manage assets, address vulnerabilities, and assess the effectiveness of risk management measures) must be considered

key. From a crisis management perspective, the necessary parts included in NIS II, ranging from business continuity management and crisis management itself, through incident management to emergency communications within the company, are acknowledged. Thus, it is believed that the NIS II Directive is an appropriate step not only to support the cybersecurity of companies but also to strengthen the crisis preparedness of society in general (NIS II, 2022), (Cole, T. A., Verbinnen, P., 2022).

2.8.2 Draft Czech Legislation Transposing the NIS Directive II

The new cyber phase bill is still in the legislative process. However, already from its draft and the draft accompanying decrees we can infer the future concept of cybersecurity in the Czech Republic, which is already very close (ODOK 2024).

The draft law on cybersecurity regulates the basic concepts, obligations of entities and the designation of regulated services and their regimes. Specific information, for example, on risk management can only be found in the draft of decree on security measures of a provider of a regulated service under the higher obligation's regime. (ODOK 2024, annex 5 of the draft of decree on security measures of a provider of a regulated service under the higher obligation's regime) to this decree contains the content of security policies and security documentation. From the perspective of crisis management, it is also worth mentioning the obligation for companies to have in the policy for the management of the continuum of activities as well as the methods of crisis communication and reporting (ODOK, Annex 5, p. 1.14, d, 2024) of the draft of decree on security measures of a provider of a regulated service under the higher obligation's regime) to have a communication matrix with key persons for each service (ODOK, Annex 5, p. 1.14, 1.14, e, 2024) of the draft of decree on security measures of a provider of a regulated service under the higher obligation's regime), to regulate escalation procedures for crisis situations, and even to have a catalogue of crisis scenarios. This is all part of business continuity management. According to ODOK (Annex 5, p. 2.12 a, 2024) of the draft of decree on security measures of a provider of a regulated service under the higher obligation's regime, the business continuity plan should include not only the conditions for activating the plan, specification of the persons to be governed by it, but also, according to point c) of this point, the temporary solution, and procedures for activating a crisis scenario (ODOK 2024).

There is no provision specifically dealing with crisis management within the draft Decree and the security measures of the regulated service provider under the subordinate obligation's regime, but entities must also deal with business continuity management under Section 7 of the Decree. When the Business Continuity Management Policy in ODOK (Annex 2, p.3, d, 2024) has the same obligation with entities in the higher duty regime, namely, to have a communication matrix with key persons for each service (ODOK 2024).

Risk management can only be found in the draft decree on security measures of a regulated service provider in the higher obligation regime, the draft decree in the lower obligation regime does not explicitly include risk management in the current draft and thus focuses more on crisis management. I believe that to some extent, but not in such a formalised way, risk protection will be addressed by those in the lower regime through other measures designed for them (ODOK 2024).

As mentioned above, risk management in its entirety can now only be found in the Decree for entities falling under the regime of higher obligations. In the draft of this Decree, specifically in Article 4(2), it is stated that companies will have to, inter alia, draw up a statement of applicability, a risk management plan considering significant changes and vulnerability scanning and will have to implement security measures in accordance with this plan. This is

followed up by the provisions of Section 9 of the draft Order on security measures for regulated service providers under the enhanced obligations regime, which details the various steps that companies will need to follow. These obligations are then also elaborated in the annexes to this Decree. As part of risk management, companies will thus have the necessary policies, methodologies, and documentation in place, identify risks with respect to their assets and identify relevant threats and vulnerabilities to these risks and assess these risks on a regular basis, at least annually (ODOK 2024).

Although different opinions and some controversy in society have been aroused by the draft of the new cyber law and its decrees, it is beneficial for the protection of companies. It is believed that it will help them to set up risk management and possibly crisis management so that they are protected to the greatest extent possible (ODOK 2024).

2.9 Crisis Management Roles and Responsibilities

Roles of crisis managers and teams in developing and implementing crisis management plans.

Skills and competencies required for effective crisis management and compliance with regulatory directives like NIS 2 (especially under the new cybersecurity proposal), some parts can be taken from ISO (2024) Crisis management - Requirements for capacities and competencies at the level of local government and organisations, and ISO 22316:2017 - Guide to enhancing organisational resilience.

Crisis management involves a variety of roles and responsibilities to effectively handle and mitigate crises. Here are some key roles and their respective responsibilities:

Crisis Management Team (CMT)

By Kaschner (2021, p. 17-18) and UIC Additional Global Security Programme (2017, p. 53-60) the CMT is responsible for overall crisis management, decision-making, and coordination of response efforts. Their Responsibilities are in particular:

- Activate and lead crisis response efforts.
- Establish communication channels and protocols.
- Assess the crisis situation and determine appropriate actions.
- Coordinate with relevant stakeholders, including internal teams, external agencies, and authorities.
- Allocate resources and manage logistics during the crisis.
- Monitor the progress of response efforts and adjust strategies as needed.
- Ensure the safety and well-being of employees, customers, and other stakeholders.

Communication Coordinator

The communication Coordinator is responsible for managing internal and external communications before, during, and after a crisis, his/her responsibilities include (Kaschner, H. (2021) and (Moh Heng Goh, 2024):

- Develop crisis communication plans and protocols.
- Establish communication channels and tools for disseminating information.
- Draft and distribute crisis messages to stakeholders, media, and the public.
- Coordinate media relations and spokesperson duties.
- Monitor public perception and media coverage of the crisis.
- Provide regular updates and instructions to employees and stakeholders.
- Manage rumors, misinformation, and social media communications.

Operations Manager/Crisis Manager

According to UIC recomendation (2017, p. 18) and Vašíčková (2019, p. 61-63) a crisis manager is an individual or team member who is responsible for managing and coordinating an organisation's response to a crisis. His or her main objective is to minimise the negative impact of the crisis on the organisation and to ensure that appropriate measures are taken to protect employees, customers, assets, and the company's reputation. Sometimes the crisis manager may also be referred to as the crisis team leader or crisis management director. His or her responsibilities include:

- The crisis manager is responsible for developing crisis management plans and procedures to be used in the event of a crisis. This includes identifying potential risks and threats, analysing the organisation's vulnerabilities, and developing strategies for a rapid and effective response.
- During a crisis, the crisis manager is responsible for leading and coordinating the organisation's response. This includes mobilising the crisis team, making real-time decisions, allocating resources, and coordinating with external stakeholders such as authorities, media, or suppliers.
- The crisis manager has a key role in managing communication during a crisis. This includes ensuring the flow of information between internal teams, providing updates and guidance to staff and stakeholders, and managing media and public relations.
- Once the crisis is over, the crisis manager is responsible for analysing and evaluating the course of the crisis, identifying the strengths and weaknesses of the organisation's response, and recommending actions for future improvement.
- The crisis manager also plays a key role in planning and implementing business continuity measures in the event of a crisis. This includes creating business continuity plans, regular testing, and exercises, and updating procedures in line with new threats and developments in the organisation.

Human Resources (HR)

Regarding to Vardarlier (2016, p. 464-469) and UIC (2017) the HR focuses on addressing the human aspects of the crisis, including employee welfare, support, and organizational resilience. Their main duty is to:

- Provide support and guidance to employees affected by the crisis.
- Coordinate employee assistance programs and support services.
- Address staffing issues, including absenteeism, scheduling, and workload management.
- Communicate policies and procedures related to employee safety and well-being.
- Facilitate communication between employees and management.
- Assess and address the long-term impact of the crisis on workforce morale and productivity.

Legal and Regulatory Advisor

According to Moh Heng Goh (2016) the Legal and Regulatory Advisor provides guidance on legal and compliance issues related to the crisis, including risk management and liability. Importantly, they provide the following activities in the context of the crisis:

- Assess legal risks and obligations arising from the crisis.
- Advise on compliance with relevant laws, regulations, and industry standards.
- Coordinate with external legal counsel, regulators, and authorities.
- Manage documentation and record-keeping related to the crisis.
- Address liability concerns and potential litigation.
- Ensure transparency and accountability in crisis response actions.

Kaschner (2021, p. 99-100) states, that these roles may vary depending on the size and nature of the organisation, as well as the specific requirements of the crisis at hand. Effective crisis management relies on clear roles, responsibilities, and coordination among all stakeholders involved in the response effort. For this reason, it is important for the company to develop a matrix of responsibilities, together with clearly stated details. Kaschner (2021, p. 183) recommended to use the RACI matrix methodology.

2.10 Methodology

In the methodology adopted for this thesis, a multifaceted approach was employed, systematically integrating the requirements of the NIS II Directive into the LINET Group's crisis management framework. Each component of the methodology was detailed in this chapter, with an emphasis on regulatory compliance, empirical research, and practical implementation. Like the process of building a house (as explained on page 38, *written italic*), where each phase from foundation laying to the final construction must be meticulously planned and executed, the methodology here was constructed to ensure robust compliance and effective crisis management. The initial groundwork, analogous to laying a foundation, involves a comprehensive analysis of regulatory requirements, while the structural development mirrors the empirical research and integration of practical measures. This analogy, revisited in the analytical part of the thesis, helps illuminate the essential steps taken in developing a resilient crisis management strategy, akin to constructing a durable and reliable house.

For better readability and clarity, all tables that extend over one or more pages was included directly in the text of the document rather than being placed in the appendices.

Regulatory Analysis: The provisions of the NIS II Directive relevant to LINET Group's operations in the healthcare technology sector were extensively examined. Legal texts, guidelines, and regulatory expectations were analyzed, focusing on risk management, incident reporting, and security measures. This analysis aimed to map the directive's implications comprehensively and establish a foundational understanding of the compliance landscape.

Literature Review: A comprehensive literature review was conducted, involving an in-depth examination of existing literature on crisis management theories, risk management methodologies, and cybersecurity best practices. Scholarly articles, books, and other relevant academic sources were scrutinized to extract pertinent concepts and strategies that align with the objectives of LINET Group and the NIS II requirements.

Stakeholder Interviews: Interviews were carried out with key stakeholders within LINET Group, including senior management, IT security teams, and operational personnel. The aim was to ascertain the current state of crisis management practices, identify gaps in compliance with the NIS II Directive, and gather insights on perceived challenges and opportunities.

Case Study Analysis: The practical application was primarily conducted using a case study approach, focusing on LINET Group. The case study was designed to demonstrate the issues related to crisis management, with a particular emphasis on cybersecurity incidents. The disruption vector chosen by the author for this study was a hypothetical scenario. This choice was motivated by the fact that similar types of cybersecurity incidents are currently quite frequent, and their number and sophistication are rapidly increasing.

Empirical Research: Empirical data were collected through a series of structured interviews and surveys conducted with professionals experienced in crisis management. Participants were selected from among professionals experienced in crisis management, ensuring a diverse and relevant pool of insights. This phase was focused on the gathering of both qualitative and quantitative insights to assess the implementation and effectiveness of existing crisis management strategies.

Risk Assessment and Scenario Planning: Customized risk assessments were conducted to identify specific vulnerabilities and potential crisis scenarios that could impact LINET Group post-NIS II integration. Scenario planning was utilized to anticipate and prepare for these scenarios, enhancing the strategic planning and decision-making processes.

Framework Development: Drawing on insights from the regulatory analysis, literature review, stakeholder interviews, and empirical research, a comprehensive crisis management framework was developed. This framework was specifically tailored to incorporate the directives of NIS II, addressing identified gaps, and leveraging industry best practices.

Data Analysis: Data collected from interviews, surveys, and case studies were meticulously analyzed using thematic and statistical analysis techniques. This analysis facilitated an in-depth understanding of the themes, challenges, and opportunities relevant to crisis management implementation.

Implementation Roadmap: An actionable implementation roadmap was outlined, specifying the steps, timelines, resource allocation, and responsibilities required to integrate the developed crisis management framework effectively.

Evaluation and Feedback Mechanism: A systematic evaluation methodology was established to assess the effectiveness of the implemented framework in enhancing crisis management capabilities and meeting NIS II requirements. Feedback mechanisms were also set up to enable ongoing refinement and adaptation of the framework based on stakeholder input and emerging challenges.

Research Ethics: All research activities were conducted in accordance with ethical standards appropriate to the academic and professional context. Confidentiality and anonymity of the participants were strictly maintained throughout the study.

3 Analytical Part

3.1 LINET and the Simulated Incident

Disclaimer: For LINET's protection, all sections, except section 3.1.1 which describes information about LINET, are based on fictitious data and practices that do not reflect LINET's actual operations. As such, however, they are factually correct.

3.1.1 Description of LINET and its Production

Founded in 1990, LINET set out from the outset to improve working conditions for healthcare workers, specifically to address the myriad problems of period medical beds. The company's motto was: "To be an object of desire, not of choice" and is: “Designed to help you care”. The beginnings of the company are closely linked to the name of Zbyněk Frolik, who founded it from scratch and was the key man of the three Czech founding entrepreneurs. Zbyněk Frolik's goal from the beginning was to make LINET a world leader, so he invested not only in research and development but also in his own sales network and unique bed design.

In 2011, the LINET Group was established after a merger with Wissner-Bosserhoff, a company with many years of experience in the production of innovative quality beds and furniture with a focus on homes for the elderly. LINET Group SE, of which LINET spol. s.r.o. is the Czech company, is then based in Dordecht in the Netherlands. The LINET Group now consists of several subsidiaries and prioritises corporate ESG management (Environmental, Social, and Governance), corporate transparency, and overall business efficiency. Nor does it forget about the environment and improving safe working conditions. This is evidenced by the QMS (Quality Management System) and EMS (Environmental Management System) certifications and the international standards ISO 14001, ISO 9001, ISO 13485, MDSAP (Medical Device Single Audit Program) and MDR (Medical Device Regulation EU 2017/745). Now LINET has as one of its key priorities the analysis of climate and energy measures aimed at carbon neutrality, where it aims to reduce energy consumption and natural resources and waste and wants to use renewable resources as much as possible.

As part of its social responsibility, it holds the Healthy Company and Family Friendly Company certificates. It has also passed a gender audit to assess equal opportunities and is therefore a holder of the Gender Audit Certificate.

LINET worked with practitioners, hundreds of nurses from 17 countries, to develop the first product. Interestingly, the company's first production took place in an old barn that used to be a cow barn, but now has 4 very modern facilities and operates globally.

LINET has a long-standing commitment to improving the conditions of not only patients but also those in care roles such as nurses, doctors, and other healthcare professionals by creating and manufacturing products that help them care. It can help these professions through a very wide range of products that not only include the aforementioned beds – for intensive care, but also standard beds for hospital settings, as well as special beds for nursing homes and beds for long-term care. However, the product portfolio is much broader and includes beds, including transport beds and chairs, as well as special mattresses, asisstance systems, medical furniture, and other accessories. Innovative solutions are meant to be designed by nurses for nurses, and LINET's never-ending efforts make it the No. 1 manufacturer of advanced care beds.

The company thus operates in seven basic systems. The intensive care segment, the acute care segment, the transport beds and chairs segment, the gynecology, obstetrics and childcare

segment, the mattress segment, the assist systems segment and finally the beds, mattresses, tables, and seating segment.

In the **intensive care segment**, the premium Multicare X, Eleganza 4 and 5 and Multicare beds are important products. The beds' lateral inclination helps in faster recovery of patients as well as reducing the burden on healthcare professionals. For example, the premium Multicare X beds designed for intensive care units reduce the effort required to move a patient from bed to bed by up to 33%. The Eleganza 5 bed then helps to maintain the patient's vital signs, allowing them to be treated safely and with minimal effort.

The **acute care segment** focuses on a wide range of beds for any hospital ward and for all levels of care. There are 8 key products here, which are Elegnaza 1 & 2, Essenza 300 & 300 LT, Image 3 & 3 Bariatric, Laterna Acute and Praktika 1 & 2.

Within the **transport beds and chairs**, the focus is on easy and safe patient transport, with features such as IV&Drive and exceptional ergonomics. The multi-functionality of the chairs is essential here, which, like other beds, provides the necessary comfort and flexibility for medical procedures. The products in this segment are the Sprint 200, Sella, Pura, and Sprint 100 transport beds.

Production in the field of **gynaecology, obstetrics and childcare** offers the AVE2 birthing bed, the Gracie and Graciella products for ergonomic solutions in the gynaecology department and the TOM2 children's bed.

The **mattress area** offers solutions that prevent pressure ulcers in patients, mattresses are active, hybrid and passive and include products Air2Care 10,20, Air2Care 4,5,6(IN),8(IN), Clinicare 100 HF, Effectacare, Hybrimatt 100 (IN), 200, Medimatt and others.

The penultimate segment is **assistance systems**, which are digital solutions to improve the functionality of beds and allow healthcare professionals to obtain more essential data on patient safety and the functioning of these beds. Assistive systems then include Linis SafetyPort, which among other things enables visualisation of bed management and maintenance data, and SafeSense 3, which combines motion monitoring and moisture detection with other smart technologies. These are thus important systems in the field of smartcare.

The **beds, mattresses, tables, and seating furniture segment** focus on the care sector and plays a key role not only due to the aging population but also due to the increase in chronic diseases. These adaptable, digital, and other nursing beds, along with mattresses and special bedside or dining tables and seating furniture, enhance the comfort of patients and caregivers alike.

These segments thus allow a total and comprehensive coverage of patient care, the product list is constantly expanded and innovated, above, is only an example of the current production of LINET products. At present, the company has installed over 1.2 million beds for global care, produces over 130,000 units per year, and provides its products and services to more than 70,000 customers worldwide in 120 countries.

3.1.2 Description of the Cyber Security Issue That Caused the Linet Production Outage

On Friday, November 10, 2023, the manufacturing company LINET was the target of a sophisticated cyber attack. A hacker managed to penetrate the company's VPN network and encrypt data on critical servers, crippling production, storage, and supply for 3 weeks. The total impact of the incident was estimated at £5 million, and the company also faced a reputational breach and loss of confidential data.

Cause Identified:

The attacker exploited a weak password "password123" used by an external vendor to access the VPN. In addition, the VPN was not protected by multi-factor authentication, making it an easy target for the hacker. After penetrating the network, he performed scans and targeted critical systems. He exploited a vulnerability in the RDP protocol and used a blank password to log into servers with systems and data essential for production, warehousing, and supply. He then installed the WannaCry ransomware, which encrypted all data and made it unusable. He demanded 1000 Bitcoin for decryption.

The Company's Response and the Impact of the Incident:

The incident was not discovered until Monday, November 13, when a helpdesk user reported a production system outage. During weekends, production does not run, and IT supervision does not run to the full extent as during normal working hours. The IT department immediately isolated the compromised systems and started a forensic analysis. Attempts to decrypt the data failed, and the company had to resort to reinstalling and reconfiguring all the compromised systems. The data was recovered from backups, but it is unclear whether the attacker made a copy before encrypting it and will later blackmail the company by threatening to disclose the leaked data. In addition to a 3day production outage and another 2 days of partial operation, the company faces financial losses, reputational damage, and loss of confidential data. It will take another 3 weeks to repair and recover from the incident.

Steps to Remedy and Prevent:

The company's management has established a crisis staff and approved funding to remediate the incident. Authorities were contacted and a forensic analysis was conducted. After the investigation of the crisis was completed, the company further planned the implementation of corrective technical and organizational measures:

- Implement strong passwords and multi-factor authentication.
- Regular software and firmware updates.
- Deploy VPN access monitoring.
- Implementation of security solutions for detection and prevention of cyber attacks.
- Regular staff training in cyber security.
- Creating a cyber incident response plan.
- Consideration of Zero Trust architecture implementation.
- Regular data backup to offline storage.

Detailed Report on the Course of a Security Incident:

On Friday, November 10, 2023, at 18:00, unauthorized access to the LINET manufacturing company's VPN network was detected via the Fortinet FortiGate 60F VPN server. The attacker exploited a weak password "password123" used by one of the external vendors to access the VPN. The VPN was not secured by MFA at the time because accesses were passed between multiple users of the vendor. After penetrating the corporate network, the attacker performed a network scan using Nmap and identified critical systems that were accessible on that network segment. The attacker gained access to the production, warehousing, and supply servers to which the production line was connected.

Subsequently, the attacker exploited the CVE-2022-22015 vulnerability in the RDP protocol to access these servers. The vulnerability consists of a flaw in user authentication that allows an attacker to bypass authentication and gain access to the system. The attacker logged into the servers with the username "administrator" and a blank password.

After accessing the servers, the attacker installed the WannaCry ransomware malware. The malware encrypted all data on the servers, making them unusable. The attacker also left a message demanding a ransom of 1000 Bitcoins.

Other technical details of the attack vector used:

- VPN protocol: IPSec
- VPN port: 500
- RDP protocol: TCP port 3389
- Server operating system version: windows server 2019 Build 1809
- Malware name: WannaCry
- Malware version: WannaCry 2.0

Stages of the Incident:

Friday, November 10, 2023:

- 18:00 - Unauthorized access to VPN network via Fortinet FortiGate 60F VPN server.
- 18:30 - Network scanning with Nmap and identification of critical systems.
- 19:00 - Exploiting the CVE-2022-22015 vulnerability in RDP to access servers.
- 19:30 - WannaCry ransomware installed on servers.
- 20:00 - Encrypting data on servers and making them unusable.
- 23:30 - Leaving a message demanding a ransom.

Saturday, November 11, 2023:

- Day-long ongoing data encryption and systems disruption.
- Not recorded by the IT department, IT department hours are 9am-5pm on weekdays only. No production on weekends.

Sunday 12 November 2023:

- Day-long ongoing data encryption and systems disruption.
- Not recorded by the IT department, IT department hours are 9am-5pm on weekdays only. No production on weekends.

Monday, November 13, 2023:

- 07:00 - Incident discovered by a helpdesk user after reporting a production system outage.
- 08:30 - Verification of the incident by the IT department.
- 09:00 - Isolating infected systems by disconnecting them from the network connection.
- 10:00 - Start of forensic analysis using FTK Imager and Wireshark tools.
- 12:00 - Contacting the police and the National Office for Cyber and Information Security and the Office for Personal Data Protection of the Office for Personal Data Protection.

Afternoon:

- An attempt to decrypt the data using the WannaCry Decryptor tool failed.
- Decision to reinstall and reconfigure all compromised systems.
- The decision not to pay the ransom.
- Start data recovery from backups from external storage.

Tuesday, November 14:

- Full-time work on installation and configuration of systems.
- Evening: completion of installation and configuration of systems

Wednesday, November 15:

- Morning: Completing data recovery from backups.
- Afternoon: Testing and commissioning of systems.
- Evening: resumption of production, storage, and supply.

Impact of the incident:

- Total disruption of production, storage, and supply for 3 days.
- Next 2 days only partial operation and gradual rebooting of systems.
- Data encryption on systems (approx. 20 TB of data).
- Financial losses due to production outage and incident recovery costs (estimated at CZK 5 million).
- Damage to the company's reputation.
- Loss of confidential data, it is unclear whether the data was merely lost or whether the attacker made a copy before encrypting it.

- Remediation and elimination of the reputational and operational impact of the incident for the next 3 weeks (clearance of delayed orders, stocking and tracking of inventory, emergency inventory of stock levels).
- The cost of implementing corrective and technical measures to prevent future crises is estimated at CZK 2 million.

Next Follow-up Steps:

- Completion of forensic analysis.
- Evaluation of the overall impact of the incident – not only financial.
- Implementation of technical and organisational corrective measures.
- Increasing the company's cyber security (e.g. penetration tests).

Recommended Action by the NUKIB:

- NUKIB recommended that the company conduct an in-depth analysis of the incident and identify its causes.
- NUKIB recommended that the company implement technical and organisational measures to prevent similar incidents in the future.
- NUKIB recommended that the company train its employees in cybersecurity.
- NUKIB recommended that the company revise its supplier contracts and anchor the safety rules in the supplier contracts. The application of the sanction from the incident is at the discretion of the company's management.

Types of Lost Data:

- Business data including invoices, orders and contracts were lost.
- Personnel data was lost, including names, addresses, and contact details of employees or suppliers.
- Technical data was lost, including source code and configuration files for production lines and servers.
- The data was restored from backups, but it could not be verified whether it was leaked.

Company Management Actions:

- The company's management set up a crisis staff consisting of IT specialists, managers, and lawyers.
- The Crisis Staff met daily to monitor the situation and coordinate the response to the incident.
- The company's management has approved funding for incident remediation, including the cost of forensic analysis, data recovery and implementation of security measures.
- Management communicated with clients, partners and employees about the incident and its impact.
- The management of the company reported the incident to the NUKIB and the Office for the Protection of Competition within the legal deadlines.
- Management is assessing the filing of a criminal complaint against an unknown perpetrator and cooperating with the Police Department.

- Management has commenced negotiations on the application of a contractual penalty from the contract with the supplier for non-compliance with the security requirements of the service provided.

Information Communicated to Clients and Staff:

- Clients and employees were told that there had been a cyber-attack and that their data may have been lost.
- Clients and staff were forced to change their passwords.

Newly Introduced Corrective Measures:

- Implement strong passwords and multi-factor authentication.
- Regular software and firmware updates (introduction of automatic updates).
- Deploy VPN access monitoring, review, and restrictions.
- Implementation of security solutions for detection and prevention of cyber attacks (e.g. EDR system).
- Regular staff training in cyber security.
- Creating a cyber incident response plan.
- Revision of BCP and DRP plans.
- Review of cybersecurity supply contracts.
- Revision of internal documentation for crisis communication.
- Consideration of Zero Trust architecture implementation.
- Regular data backup to offline storage.

Forensic Analysis Techniques Used:

- Server and network device log files were analyzed using ELK Stack and Splunk.
- Malware samples and ransomware messages were analyzed using VirusTotal and Cuckoo Sandbox tools.
- Forensic copies of the compromised systems were made using the FTK Imager tool.
- Outside forensic firms have been contacted for assistance, and forensic copies will be forwarded to the Police Department.

3.1.3 Current Weaknesses in Crisis Management

The crisis that took place at LINET on 10 November 2023 revealed several weaknesses in management and communication. These weaknesses led to the prolongation and deepening of the impact of the cyber-attack, causing the company to suffer significant financial losses, reputational damage, and loss of confidential data.

Shortcomings in Management

Weak security policy: the use of weak passwords ("password123"), the absence of multi-factor authentication (MFA) for VPNs, the sharing of access between vendor users and the lack of access control to servers represent a serious disregard for basic security principles.

Ineffective response to the incident: the delay in detecting the incident (48 hours) and isolating the compromised systems led to an increase in the amount of time the attacker was able to operate on the company's network. The failed attempt to decrypt data and the delayed decision to restore data from backups exacerbated the impact of the incident.

Lack of a cyber crisis plan: the absence of a cyber incident response plan led to a chaotic and ineffective response from the company's IT department and management.

Inadequate preparedness for cyber attacks and the lack of an incident response plan led to a chaotic and ineffective response from the company's IT department and management. Delays in isolating compromised systems and restoring data from backups extended the time an attacker could operate on the company's network and cause damage.

Communication Deficiencies

Lack of transparency: information about the type of data lost was not communicated to clients and staff, even after a long time since the incident. The lack of clarity about the data leak and the delayed information about management's actions caused confusion and concern among clients and employees.

Lack of empathy: Information about the incident was not communicated in a way that was understandable to clients and staff. There was a lack of expression of regret for the situation and an offer of support for those affected by the incident.

Recommendations

- Establish a strong security policy with an emphasis on access control and authentication.
- Create and regularly test a cyber incident response plan that clearly defines the roles and responsibilities of each department and company management.
- Improving communication with clients and staff in crisis situations. Incident information should be communicated transparently, clearly and in a timely manner, with an offer of support.
- Providing support for clients and staff affected by the incident.
- Consider conducting an independent cybersecurity audit to help the company identify and address remaining cybersecurity weaknesses.

Effective management of crisis situations such as cyber-attacks, natural disasters or other emergencies is a significant challenge for company management. Weaknesses in management and communication in such situations can lead to deepening the impact of the crisis, loss of

trust and damage to the company's reputation. For companies to better deal with crises, it is essential to have robust security policies and procedures in place. This includes implementing strong passwords, multi-factor authentication (MFA), strong access controls, and regular software and firmware updates to minimize security risks. It is also important to conduct regular security audits and penetration tests to identify and eliminate system weaknesses and educate employees on cybersecurity, thereby increasing their awareness of security risks.

It is also crucial to develop and regularly update a crisis response plan that clearly defines the roles and responsibilities of the individual members of the crisis staff and sets out procedures for dealing with different types of crises. The plan should include guidelines for communicating with clients, staff, and the media in the event of a crisis and should be tested and updated regularly to ensure it remains relevant and effective.

Improving communication with clients and staff in crisis situations is another important step. There is a need to share information about the crisis in a timely and transparent manner, to communicate clearly and empathetically, and to provide support and information on how to deal with the impact of the crisis. Providing psychological support for clients and staff is essential as crisis situations can have a significant impact on people's psyche. Once a crisis has been resolved, it is important to carry out a thorough analysis, identify and learn from mistakes and based on this analysis, put in place corrective measures to prevent similar crises from recurring in the future.

In addition to these general rules, it is important for companies to focus on specific aspects of crisis prevention and management relevant to their industry. For example, they should have plans for managing accidents and minimising environmental impacts. Implementing these recommendations will help companies to better prepare for, effectively manage and minimise the impact of crisis situations. An emphasis on prevention, robust planning and effective communication is key to protecting corporate assets, reputation and the trust of clients and employees.

3.2 Preparing for the Crisis

Disclaimer: For LINET's protection, all sections, except section 3.1.1 which describes information about LINET, are based on **fictitious** data and practices that do not reflect LINET's actual operations. As such, however, they are factually correct**.**

3.2.1 Business Impact Analysis

Imagine that a house is being planned for construction. Before the first brick is laid, a thorough assessment of the construction plan must be carried out—not just to predict the appearance of the house but to understand how each part of the construction impacts the overall structure. This preliminary analysis can be likened to a Business Impact Analysis (BIA) in the context of crisis management.

A BIA is seen as the foundation for any organization, like the foundation that supports a house. Just as potential risks such as soil stability, material quality, and design robustness are assessed by architects to ensure that the house can withstand various stresses—be it natural disasters or regular wear and tear—critical operations and processes are identified, potential threats are evaluated, and the impacts of disruptions on these operations are determined through a BIA by businesses.

In this foundational stage, each element is scrutinized: the load-bearing walls (critical business functions) and the electrical wiring (IT infrastructure) are examined. The role of each component is defined not just by its immediate function but by its impact on the overall integrity and livability of the house. Similarly, the interdependencies between different business areas are mapped out in a BIA, illustrating how disruptions in one area could lead to cascading effects throughout the organization.

As this narrative is continued across subsequent chapters, it will be seen how the initial assessments influence decisions during the construction phase (crisis response) and how they aid in the recovery and reinforcement of the structure post-crisis (business continuity planning).

(next metaphor of house building on page 93)

The BIA has been developed according to the established methodology to be consistent with the NIS 2, the draft new law on cyber security and the draft decree on security measures of a regulated service provider under the regime of higher obligations, as well as with the practical functioning of LINET.

The issue of information security covers the entire structure of LINET, in all locations of its operations, including cooperating companies that meet LINET's secure information. Information security then affects all identified information assets to the extent and scope appropriate to the importance of the asset. The methodology for conducting the impact analysis shall be followed by all employees and its implementation shall be monitored by senior employees within the scope of their defined authority and responsibility. Information security control activities are methodically guided by the role of the **Cyber Security Manager**, who is also responsible for keeping the policy up to date.

The methods for assessing the impact of cyber security incidents on continuity and assessing the associated risks were carried out according to the following procedure.

In the business impact analysis, LINET evaluated and documented the potential impact of cyber security incidents on its operations, i.e., on ensuring the operation of its primary assets. In the case of the impact analysis, in addition to the basic attributes of information security (confidentiality, integrity and availability), the attribute of loss (if data would be lost) is also assessed. The impact analysis and subsequent risk analysis were then used to develop a business continuity management strategy.

Therefore, to develop the impact analysis, the key assets of the organisation were first identified according to a specific methodology for asset assessment described in accordance with the rules outlined in the theoretical section and the assets were recorded in the asset and risk assessment framework outlined in the following subchapter.

This subchapter addresses only the primary asset of the bed manufacturing process, which is the asset that was affected by the incident described in Section 3.1.2.

Primary Asset Impact Assessment:

Primary asset name: bed manufacturing process
Guarantor of the primary asset: Michal Písař
Date of evaluation: 10 March 2023

Table 2 Primary asset impact assesment

	Availability									Loss									Confidentiality			Integrity	
Areas of impact	Unavailability 15 min.	Unavailability 1 h	Unavailability 4 h	Unavailability 8 h	Unavailability 1day	Unavailability 2 days	Unavailability 1 week	Unavailability 14 days	Unavailability for a month or more	Data loss from backup (15 min)	Data loss from backup (1 h)	Data loss from backup (4 h)	Data loss since backup (8 h)	Data loss since backup (1 day)	Data loss since backup (2 days)	Data loss since backup (1 week)	Data loss since backup (14 days)	Complete loss of data	Disclosure within the organisation	Disclosure to contractors	Disclosure outside the organisation	Small-scale data modification	Large-scale data modification
Data protection - impact on data subjects	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Data protection - financial harm to data subjects	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Trade secrets	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	4	3	3	4	3	3
Legal and contractual obligations	0	0	0	1	1	1	1	2	2	0	0	0	0	0	0	0	0	4	3	3	4	3	3
Disruption of internal management and control activities	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	4

Public order	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Financial losses	0	0	0	1	1	1	1	2	2	0	0	0	0	0	0	3	3	4	0	0	0	0	0	0
Provision of essential or basic services	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Disruption of normal activities	0	1	1	2	2	2	3	3	4	0	0	0	0	0	0	3	3	4	1	1	1	2	3	3
Loss of credibility	0	0	0	1	1	1	1	2	3	0	0	0	0	0	0	0	0	0	0	1	2	3	3	3
Safety and health of persons	0	0	0	0	0	0	0	1	2	0	0	0	0	0	0	0	0	1	0	0	1	2	2	2
Impact on IS or CS users	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
International Relations	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Criminal law proceedings	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Source: own processing, Cybrela (2024)

Table 2 presents LINET's completed Business Impact Analysis (BIA) for primary asset: bed manufacturing process. The BIA is used to evaluate the potential impacts of various business scenarios on areas such as personal data protection, financial losses, human safety, and health, among others. The top row of the table indicates different levels of unavailability timeframes, data loss timeframes, and levels of confidentiality and integrity. In Chapter 2.2.1 is located the theoretical template illustrated in Picture 1. The rating that was used is described below.

The Resulting Rating of the Primary Asset (maximum of each attribute):

- Availability: 4
- Loss: 4
- Confidentiality: 4
- Integrity: 4

Business Continuity Indicators:

- **RPO** (determined from the Loss): 30 days.
- **RTO** (determined from Availability): 30 days.
- **SLA**: 45 days.

To assess impact, LINET uses the **Business Impact Analysis Impact Matrix**, which provides guidelines for assessing individual areas on a 0-4 rating scale, i.e. no impact to critical impact:

Data protection – impact on data subjects:

- **1/low level**: May lead to discomfort for the data subject (irritation, short time requirements for re-entering data, need for further communication with the organization)
- **2/medium level**: May lead to minor harm (stress, discomfort, minor physical inconvenience, lack of understanding, limitations in accessing services from the organisation or other actors, time demands associated with dealing with impacts)
- **3/high level**: May lead to serious harm (assault, adverse health, depression, hardship, economic disadvantage (blacklisting), identity theft, summons by investigating authorities)
- **4/ critical level**: May lead to very serious harm, direct threat, or loss of life (death, disability, long-term adverse health condition and incapacity, loss of employment, extreme difficulty of employment, exclusion, restriction of rights)

Personal Data Loss – Financial Loss to the Data Subject:

- **1/low level**: no financial harm
- **2/medium level**: Estimated financial damage up to 5000 CZK/data subject
- **3/high level**: Estimated financial damage from CZK 5,000 to CZK 50,000/data subject (misuse of data subject's funds, damage to property)
- **4/ critical level**: Estimated financial damage from 50 000 CZK/ data subject (inability to repay debt, loss of property)

Trade Secrets:

- **1/low level**: no clue
- **2/medium level**: May have a negative impact on business, production or technical facts related to the enterprise that have actual or at least potential tangible or intangible value.
- **3/high level**: May have a material impact on facts of a commercial, production or technical nature related to the enterprise that have actual or at least potential tangible or intangible value.
- **4/ critical level**: It may have a significant impact on facts of a commercial, productive, or technical nature related to the enterprise that have actual or at least potential material or immaterial value.

Legal and Contractual Obligations:

- **1/low level**: May cause violations of internal policies and procedures, but not violations of legal and contractual obligations.
- **2/medium level**: May result in administrative or civil proceedings leading to fines or damages.
- **3/high level**: May cause a breach of the law leading to prosecution.
- **4/ critical level**: no clue

Disruption of Internal Management and Control Activities:

- **1/low level**: no clue
- **2/medium level**: May cause limitations in operations and critical activities, with associated potential for financial loss.
- **3/high level**: May cause temporary shutdown or significant interference with the operation of the organization, significant financial losses associated with restoration of operations.
- **4/ critical level**: It can cause a serious interference with the functioning of the whole organisation, stopping the organisation from running.

Public Order:

- **1/low level**: no clue
- **2/medium level**: May cause protests limited in scale, form, or location (localised riots).
- **3/high level**: It may cause protests limited in scope, form, or location at the level of a significant part of the administrative territory of the municipality with extended jurisdiction, the resolution of which may require activation of crisis management at the level of the region.
- **4/ critical level**: Could cause mass disorder, e.g. a general strike, or otherwise seriously disrupt public order with national implications.

Financial Losses:

- **1/low level:** May directly or indirectly lead to losses of less than 0.05% of the annual budget or turnover of the organisation (depending on the type of organisation).
- **2/medium level**: May directly or indirectly lead to losses of between 0.05% and 2% of the organisation's annual budget or turnover (depending on the type of organisation).
- **3/high level**: May lead directly or indirectly to losses greater than 2% and less than or equal to 10% of the organisation's annual budget or turnover (depending on the type of organisation).
- **4/ critical level**: May lead directly or indirectly to losses exceeding 10% of the annual budget or turnover of the organisation (depending on the type of organisation).

Provision of Essential or Basic Services:

- **1/low level**: There is no disruption to the provision of essential or basic services.
- **2/medium level**: May cause severe limitation or disruption of essential or basic services to a small number of people; may cause short-term disruption of organizational services.
- **3/high level**: May cause severe limitation or disruption of essential or basic services to many people, long-term limitation, or prevention of access to services.
- **4/ critical level**: May cause widespread restriction, disruption, or unavailability of essential or basic services to many people, may cause harm e.g. lawsuit, liquidation, incurring unpayable debt etc.)

Disruption of Normal Activities:

- **1/low level**: There is no disruption to normal activities, at most increased time demands in carrying out normal activities.
- **2/medium level**: May restrict the conduct of normal activities, disrupt the proper management or functioning of part or all the organisations.
- **3/high level**: May cause temporary cessation or substantial disruption of the organization's normal activities or impair the development or furtherance of the organization's goals and interests.
- **4/ critical level**: May seriously and long-term affect relations with other organisations or the public, resulting in national or transnational negative publicity, with long term effects and demands for political accountability.

Loss of Credibility:

- **1/low level**: May negatively affect relationships with other parts of the organization, other organizations, or relationships with the public, but negative publicity will be limited to the immediate environment and will not be long lasting (e.g., for personal data – inconvenience with data subjects, having to deal with other data subjects, having to deal with other data subjects, negative sometimes public reaction from data subjects, etc.).

- **2/medium level**: May adversely affect relations with other organisations or the public, but negative publicity will be limited to a limited interest group or will be widespread but short-lived. E.g. for personal data - 10% loss of data subjects for the organisation, short-term restriction of access to services used by the controller, negative but short-term media coverage.
- **3/high level**: May seriously affect relations with other organizations or the public, resulting in national negative publicity. E.g. for personal data - 10-50% loss of data subjects at the organisation, massive negative but short-term media coverage).
- **4/ critical level**: May seriously and long-term affect relations with other organisations or the public, resulting in national or transnational negative publicity, with long term effects and demands for political accountability. E.g. for personal data – loss of data subjects above 50% at the organisation, blacklisting, loss of competitiveness, massive negative long-term media coverage including foreign).

Personal Safety and Health:

- **1/low level**: no clue
- **2/medium level**: May result in harm (threat to personal safety, liberty, or injury) to one or more persons.
- **3/high level**: May result in harm (threat to personal safety, liberty, or injury) to a large group of persons or threat to the lives of individuals.
- **4/ critical level**: May lead to direct threat or loss of life of a group of persons.

Impact on IS (information system) and CS (communication system) users:

- **1/low level**: May cause short-term inconvenience when using IS or CS (delay and irritation to users, no other health effects).
- **2/medium level**: May negatively affect the performance of an internal or external user of the IS or CS (user stress, minor physical and health problems).
- **3/high level**: May cause severe short-term limitation of the performance of an internal or external user of the IS or CS (deterioration of users' health, short-term incapacity to work).
- **4/ critical level**: It may cause serious long-term limitation of the performance of the internal or external IS or CS user (attacks on users, departure of employees, long-term disability, death).

International Relations:

- **1/low level**: E.g. for personal data – may necessitate negotiations between the organisation and the foreign partner on the characteristics of the processing of personal data.
- **2/medium level**: May create a negative image in one territory or state. E.g. for personal data – may lead to temporary limitation of foreign participation in the processing of personal data.

- **3/high level**: Can create a negative image in the world. E.g. for personal data - may be associated with permanent or long-term restrictions on foreign partners' participation in the processing of personal data.
- **4/ critical level**: May adversely affect or damage diplomatic relations and thus cause a disadvantage to the interests of the Czech Republic. E.g. for personal data - long-term or permanent restriction of participation of foreign entities or even states in the processing of personal data.

Criminal Proceedings:

- **1/low level**: no clue
- **2/medium level**: May create the conditions for the commission of crime or make it difficult to investigate.
- **3/high level**: May lead to disruption of criminal investigations or court proceedings (minor crime, short-term, on a case-by-case basis).
- **4/ critical level**: May lead to serious, long-term impairment of the ability to investigate criminal activity, or to the questioning of judicial proceedings and decisions (serious crime, general questioning of the system).

Evaluation of the Primary Asset, the Bed Manufacturing Process, in a Business Impact Analysis:

The business impact analysis was conducted on 10 March 2023 with Mr. Michal Písař, who is the guarantor of the primary asset of the bed production process. It has been determined that this asset has no impact on the protection of personal data, either in terms of impact on data subjects or on the financial detriment of the data subject. Similarly, this asset has no impact on public policy, the production of beds as such has no impact on IS or CS users or on international relations and criminal proceedings. Thus, these lines are only filled with a zero value.

Further, Mr. Písař identified assets in terms of, for example, if information is not available to operate a regulated service and systems are unavailable and LINET is unable to operate that primary asset, when there is an impact at that scale.

However, if unavailability of one week or more were to occur, the impact on trade secrets would be critical with complete loss of the asset, and the impact on the confidentiality and integrity of trade secrets would be equally high. The impact on the availability part of the disruption of internal command and control systems occurs after the first hour, the integrity disruption also has a high and critical level of impact as it would lead to a disruption of the functionality of the production system. Financial losses will occur when production is unavailable for 8 hours or more, with backup losses being high to critical from 1 week. The availability of routine activities is impacted by an incident from as little as 1 hour, where critical unavailability would occur after a month or more, where there would be a comprehensive breakdown of production and its system of organisation and delivery, the impact would also be in this category for loss (from 1 week), to confidentiality and integrity. The next part is trustworthiness, which is impacted by availability, confidentiality, and integrity, which reach the highest level of impact. The last line where impact was determined is the safety and health of people, due to the fact that LINET not only manufactures the beds themselves, but part of this process is logically the production of spare parts, which if they were to go down for more than 14 days, or there was a

complete loss of data or modification of integrity, the safety and health of patients using these beds could be compromised. This in the event of a potential failure of the beds in question.

Based on the above business impact analysis, the asset of the bed manufacturing process within the CIA triad (Confidentiality, Integrity, and Availability) was then evaluated with the values 4 confidentialities, 4 integrities and 4 availabilities, i.e. the asset is evaluated as very critical for the functioning of LINET.

The RPO value is determined from the loss and assumes that the highest value occurs when there is a complete loss of data and therefore a critical level of impact, and according to best practice this is a value of 30 days or more. And so, it was determined to be 30 days.

The RTO value is determined from availability, and the highest value occurs when unavailability is a month or more, so the RTO value was also set at 30 days.

The SLA identified within the manufacturing process asset, was evaluated in the context of the supplier SLAs affecting that asset, and the highest delivery value was found to be 45 days in the supplier contract.

3.2.2 Risk Impact Analysis

The risk impact analysis was developed in accordance with the established asset identification and assessment methodology and the risk identification and assessment methodology. This thesis focuses mainly on the primary asset that was affected by the incident and therefore became part of the crisis management, i.e. the bed manufacturing process asset.

A table has been created that contains the primary asset records and is listed on the primary asset records tab. The confidentiality, integrity and availability ratings are carried forward from the values obtained according to the business impact analysis.

Table 3 Risk impact analysis – evidence of primary assets

ID	Primary asset	Confidentiality	Integrity	Availability	Asset description	Asset guarantor
PR 01	The process of making beds	4	4	4	A process that involves the selection of materials, manufacturing itself, finishing and inspection to create the finished bed	Michal Písař
PR 02	Storage process for beds	2	3	4	A process that involves storing manufactured beds before selling it to customers.	Veronika Cingrošová
PR 03	The process of selling beds	3	3	3	A process that includes presenting beds to customers, providing product information, closing the sale, and coordinating delivery.	Lucie Halakucová
PR 04	Process of after-service of beds	4	3	4	Procedure including follow-up maintenance and repairs of beds including professional IT service	Štěpánka Velíšková

Source: own processing, Cybrela (2024)

Table 3 illustrates part of the risk impact analysis – evidence of primary assets. The table has seven columns: ID, Primary Asset, Confidentiality, Integrity, Availability, Asset Description, and Asset Guarantor. It includes four primary assets and rates them in confidentiality, integrity, and availability. Each primary asset has an associated asset guarantor.

Table 4 Primary asset linkages, how the primary assets are linked to each other was noted:

	PR01	PR02	PR03	PR04
PR01				
PR02	X			
PR03	X			
PR04	X			

Source: own processing, Cybrela (2024)

Table 4 description: Primary Asset Linkages is used to show how different primary assets, labeled as PR01 to PR04, are linked to each other. The cells marked with an "X" indicate a linkage between the corresponding assets. For example, there's an "X" at the intersection of PR02 and PR01, indicating that these two assets are linked. The table serves as a visual guide to understand the relationships between different primary assets.

The primary asset of bed production is not dependent on any other asset, but all other assets are dependent on it. An asset cannot be dependent on itself; therefore, these boxes are coloured black. These primary asset links are then relevant for the subsequent Business Continuity Plan and Disaster Recovery Plan.

In the next step, the supporting assets were defined in the section of the supporting assets register, here only the supporting assets related to the primary asset of the bed production process, which is the subject of this thesis, are listed.

The primary asset of the bed manufacturing process is linked to the supporting assets, these have been identified as: the production line, the IT system controlling the line, employees, and suppliers.

Table 5 Risk impact analysis – evidence of supporting assets.

ID PR	Primary asset		Supporting asset	Confidentiality	Integrity	Availability	Asset description	Asset guarantor
PR01	The process of making beds	PO 01	Production line	2	4	4	Bed making lines at location A.56	Daniel Přibyl
PR01	The process of making beds	PO 02	IT system for production line	2	4	3	Systems Xline expert and Linka 1000 lite.	Veronika Forgotname
PR01	The process of making beds	PO 03	Staff	2	2	2	Internal staff including agency staff	Vilibald Malý
PR01	The process of making beds	PO 04	Suppliers	2	2	2	LINET suppliers	Marek Novotný

Source: own processing, Cybrela (2024)

Table 5 describtion: Risk Impact Analysis – Evidence of Supporting Assets is used to evaluate the potential impacts of various business scenarios on different supporting assets involved in the process of making beds – connected to the primary asset. The table has eight columns: ID

PR, Primary Asset, Supporting Asset, Confidentiality, Integrity, Availability, Asset Description, and Asset Guarantor. It includes four supporting assets related to the process of making beds (PR01), each with their respective risk ratings in confidentiality, integrity, and availability. The supporting assets are production line (PO01), IT system for production line (PO02), staff (PO03), and suppliers (PO04). Each supporting asset has an associated asset guarantor who evaluated this asset in terms of confidentiality, integrity, and availability.

Table 6 Confidentiality of supporting assets were addressed based on the scale's confidentiality rating scale.

Confidentiality rating scale		
#	**Level**	**Description**
1	**Low**	The assets are publicly available or have been designated for publication. A breach of the confidentiality of the assets does not jeopardise the legitimate interests of the obliged person.
2	**Medium**	The assets are not publicly available and constitute the know-how of the obliged person, the protection of the assets is not required by any legal regulation or contractual arrangement.
3	**High**	Assets are not publicly available, and their protection is required by law, other regulations, or contractual arrangements (e.g. trade secrets, personal data).
4	**Critical**	Assets are not publicly available and require a higher level of protection than the previous category (e.g. strategic trade secrets, special categories of personal data).

Source: own processing, Cybrela (2024)

Table 6 shows Confidentiality Rating Scale that classifies the confidentiality of assets. It's divided into four levels: Low, Medium, High, and Critical. Low-level assets are public or intended for publication, and their confidentiality breach doesn't harm the owner's interests. Medium-level assets are private and represent the owner's know-how, but they don't require legal or contractual protection. High-level assets are private and need legal or contractual protection, like trade secrets or personal data. Critical-level assets are private and need a higher level of protection than the High level, including strategic trade secrets and special categories of personal data.

Table 7 Integrity of supporting assets were addressed based on the scales for integrity assessment.

Scale for integrity assessment		
#	**Level**	**Description**
1	**Low**	The asset does not require integrity protection. A breach of the integrity of the asset does not compromise the legitimate interests of the obligor.
2	**Medium**	The asset may require integrity protection. A breach of the integrity of an asset may lead to damage to the legitimate interests of the obligor and may result in less severe impacts on the primary assets.
3	**High**	The asset requires integrity protection. A breach of the integrity of the asset leads to damage to the legitimate interests of the obligor with significant effects on the primary assets.
4	**Critical**	The asset requires integrity protection. A breach of integrity leads to very serious damage to the legitimate interests of the obligor with direct and very serious effects on the primary assets.

Source: own processing, Cybrela (2024)

Table 7 serves as an Integrity Assessment Scale, categorizing the integrity of supporting assets into four levels: Low, Medium, High, and Critical. Low-level assets do not require integrity protection and their breach doesn't compromise the legitimate interests of the obligor. Medium-level assets might require integrity protection, and their breach could lead to less severe impacts on the primary assets. High-level assets require integrity protection, and their breach could lead to significant effects on primary assets. Critical-level assets require intense protection, and their breach could lead to very serious damage to the legitimate interests of the obligor with direct and very serious effects on the primary assets.

Table 8 availability of supporting assets were addressed based on the scales below.

Availability rating scale		
#	**Level**	**Description**
1	**Low**	Disruption to the availability of the asset is not important and in the event of an outage, a longer recovery period (up to approximately 1 week) is normally tolerated.
2	**Medium**	The disruption of the availability of the asset should not exceed the duration of the working day, a longer outage leads to a possible threat to the legitimate interests of the obliged person.
3	**High**	Disruption to the availability of an asset should not exceed a few hours. Any outage must be dealt with immediately as it leads to a direct threat to the legitimate interests of the obliged person. Assets are very important.
4	**Critical**	Disruption of the availability of an asset is not permissible, and even a short-term unavailability (within a few minutes) leads to a serious threat to the legitimate interests of the obliged person. Assets are considered critical.

Source: own processing, Cybrela (2024)

Table 8 serves as an Availability Rating Scale, categorizing the availability of supporting assets into four levels: Low, Medium, High, and Critical. Low-level assets can tolerate a disruption up to approximately one week. Medium-level assets should not have their availability disrupted for more than the duration of a working day, as a longer outage could threaten the legitimate interests of the obliged person. High-level assets should not have their availability disrupted for more than a few hours, and any outage must be dealt with immediately as it leads to a direct threat to the legitimate interests of the obliged person. Critical-level assets cannot tolerate any disruption, and even short-term unavailability (within a few minutes) leads to a serious threat to the legitimate interests of the obliged person. These assets are considered critical.

The risk analysis then assessed the links of the primary asset under consideration to the supporting assets, according to the table below assessing the degree of dependence. This dependency is then reflected in the prioritisation in the risk management plan.

Table 9 shows the dependency between primary (PR) and supporting (PO) assets.

Dependency ratio PR x PO	Time without PO
	Does not affect
1	More than a week
2	Day to week
3	Max. 8 hours
4	Max. 4 hours
5	Cannot operate

Links between primary and supporting assets (*sample part of the table)*		Production line	IT system for production line	Staff	Suppliers	Storage system	IT system for inventory tracking
		PO01	**PO02**	**PO03**	**PO04**	**PO05**	**PO06**
The process of making beds	**PR01**	5	5	4	1		
Storage process for beds	**PR02**			3	1	4	3
The process of selling beds	**PR03**			3	1		2
Process of after-service of beds	**PR04**			5	1		

Source: own processing, Cybrela (2024)

Table 9 shows the dependency between primary (PR) and supporting (PO) assets. The table is accompanied by a legend that explains the dependency ratio ranging from 1 (does not affect) to

5 (cannot operate). The table lists four processes related to beds: making, storage, selling, after-service. These processes are evaluated against six types of supporting assets including production line and staff. For instance, a dependency ratio of 5 indicates that even a short-term unavailability (within a few minutes) leads to a serious threat to the legitimate interests of the obliged person, and these assets are considered critical. This table provides a clear visual representation of how different processes depend on various supporting assets. The degree of dependency was determined by consultation with the guarantors of primary assets and the employees of the IT department.

In the next part of the risk analysis, the risks of the primary assets were identified, and the vulnerabilities and threats within the primary asset on which this thesis focuses were identified from the catalogue of vulnerabilities and threats. The CIA values were transferred from the primary asset tab, where it is still the same value, I was obtained from the business impact analysis. Then their values were added to the vulnerabilities and threats, where they were based on scales to determine the likelihood of the threat and vulnerability. It was considered in determining vulnerabilities and threats that no precautions are taken so as not to introduce bias. Subsequently, for each vulnerability, a risk level was calculated according to the given scales.

Table 10 Threat and vulnerability probability rating scale

Threat probability rating scale		
#	**Level**	**Description**
1	**Low**	The threat is non-existent or unlikely. The threat is not expected to be realised more than once every 5 years. To realise the threat, it is necessary to: - have equipment that is not normally available; - have significant financial resources; - have knowledge that is not normally available. The length of preparation to implement a threat is in the order of months.
2	**Medium**	The threat is unlikely to probable. The threat is expected to be realised in the range of 1 to 5 years. To realise the threat, it is necessary to: - have superior equipment, - have financial resources equal to the average annual salary, - have superior knowledge. The length of preparation for the implementation of the threat is in the order of weeks.
3	**High**	The threat is likely to very likely. The threat is expected to be realised in the range of 1 month to 1 year. To realise the threat: - normally available resources are sufficient, - average knowledge is required, - resources equal to an average monthly salary are sufficient. The length of preparation for the implementation of the threat is in the order of days.

4	**Critical**	The threat is very likely to certain. The threat is expected to occur more than once a month. No resources are required to carry out the threat: - basic knowledge is sufficient, and it can be carried out by anyone, - almost no financial resources are required. The duration of preparation of a threat is more than once a month.
Vulnerability probability rating scale		
#	**Level**	**Description**
1	**Low**	The vulnerability does not exist, or exploitation of the vulnerability is unlikely. Security measures are in place to detect potential vulnerabilities or possible attempts to exploit them early. There is no evidence of any defects or failures in security measures.
2	**Medium**	Exploitation of the vulnerability is unlikely to likely. Security measures are in place and regularly checked for effectiveness. The ability of the security measures to detect potential vulnerabilities or possible attempts to overcome the measures in a timely manner is limited. There is evidence of a small number of security failures or malfunctions.
3	**High**	Exploitation of the vulnerability is likely to be very likely. Security measures are in place, but their effectiveness does not cover all necessary aspects and is not regularly monitored. There is evidence of a higher number of defects or failures of security measures.
4	**Critical**	Exploitation of the vulnerability is very likely to certain. There is evidence of widespread vulnerabilities or no security measures in place.

Source: own processing, Cybrela (2024)

Table 10 serves as a Threat Probability Rating Scale and Vulnerability probability rating scale, categorizing the probability of threats and vulnerabilities into four levels: Low, Medium, High, and Critical. This table provides a clear visual representation of how different threats are categorized based on their probability and the resources required to carry them out. Vulnerability rating provides a clear visual representation of how different vulnerabilities are categorized based on their probability and the resources required to exploit them.

Table 11 Vulnerability and Threat Catalogue

Vulnerability Catalogue	
Z1	Inadequate maintenance of assets,
Z2	Obsolescence of assets,
Z3	Insufficient perimeter protection,
Z4	Lack of security awareness among users, administrators, security role holders, suppliers, and senior management,
Z5	Insufficient backup,
Z6	inappropriate access permission settings,
Z7	Insufficient procedures and processes for detecting cyber security events and identifying cyber security incidents,
Z8	Inadequate monitoring of user and administrator activity and failure to detect activity that may affect the security of the regulated service,
Z9	Insufficient establishment of security rules and procedures, inaccurate or ambiguous definition of rights and obligations of users, administrators, security role holders, contractors, and top management,
Z10	Insufficient asset protection,
Z11	inappropriate security architecture,
Z12	Insufficient independent scrutiny,
Z13	Failure to detect misconduct in a timely manner by users, administrators or those in security roles, suppliers, and senior management,
Z14	Lack of staff with the necessary level of expertise,
Z15	location of the asset outside physical control (e.g. in a foreign country),
Z16	the location of the asset in the territory of a State of which the obligor has insufficient knowledge of the legal environment,
Threat Catalogue	
H1	Violation of security policy, unauthorized activities, misuse of privileges by users, administrators, security role holders, contractors, and senior management,
H2	damage or failure of technical and/or software equipment,
H3	identity abuse,
H4	use of the software in violation of the license terms,
H5	malicious code,
H6	physical security breaches,
H7	interruption of electronic communications services or electricity supply,
H8	misuse or unauthorised modification of information,

H9	loss, theft, or damage to the asset,
H10	failure by the supplier to comply with a contractual obligation,
H11	misconduct by users, administrators, security roles, suppliers, and senior management,
H12	misuse of internal resources, sabotage,
H13	prolonged interruption in the provision of electronic communications services, electricity supply or other essential services,
H14	staff with insufficient professional knowledge,
H15	Targeted cyber attack using social engineering, use of espionage techniques,
H16	misuse of removable technical data carriers,
H17	electronic communication hacking (interception, modification),
H18	dependence on suppliers,
H19	abuse of state power to access assets,
H20	disclosure or transfer of assets at the request of a State

Source: own processing, Cybrela (2024)

Table 11 serves as a catalogue for vulnerabilities and threats, each labeled with a unique identifier. The vulnerabilities range from inadequate maintenance of assets to failure to detect misconduct in a timely manner. Each vulnerability is concisely described, highlighting specific areas where security or management may be lacking or insufficient. The threat catalogue identifies issues such as violation of security policy and damage or failure of technical and/or software equipment.

Table 12 Scale for assesing the level of risk

Scale for assessing the level of risk		
Level	**Risk level**	**Description**
1-13	**Low**	The risk is considered acceptable – tolerable.
14-31	**Medium**	The risk can be reduced by less demanding measures, or in the case of more demanding measures, the risk is acceptable subject to the approval of the KB Committee.
32-47	**High**	The risk is unacceptable in the long term and systematic steps must be initiated to eliminate it.
48-64	**Critical**	The risk is unacceptable, and steps must be taken immediately to eliminate it.

Source: own processing, Cybrela (2024))

Table 12 shows categorizing the level of risk into four levels: Low, Medium, High, and Critical. This table provides a clear visual representation of how different levels of risks are categorized based on their severity and the actions required to mitigate them.

Table 13 Risk assessment matrix with formula, Risk Level = Asset (Impact) × Vulnerability × Threat

Vulnerability X Threat										
Asset		**1**	**2**	**3**	**4**	**6**	**8**	**9**	**12**	**16**
	1	1	2	3	4	6	8	9	12	16
	2	2	4	6	8	12	16	18	24	32
	3	3	6	9	12	18	24	27	36	48
	4	4	8	12	16	24	32	36	48	64

Source: own processing, Cybrela (2024)

Table 13 describes a risk assessment matrix that calculates the risk level based on the formula: Risk Level = Asset (Impact) x Vulnerability x Threat. The matrix is color-coded to represent different levels of risk, with red indicating higher risk and green indicating lower risk. The rows are labeled “Asset” with numbers 1 to 4, representing different asset ratings (based on CIA triad). The columns are labeled “Vulnerability X threat” with numbers 1 to 16, representing the product of vulnerability and threat levels. Each cell within the table contains calculated values of risks ranging from 1 to 64, providing a clear visual representation of the risk associated with each asset given its vulnerability and threat levels.

The bed manufacturing process as a primary asset was identified in the risk assessment as follows.

Table 14 risk assesment of primary asset – the process of making beds.

Primary asset	Value confidentiality	Value integrity	Value availability	PR vulnerability	Vulnerability value	The threat of PR	Threat value	Specific risk/situation	Risk level
The process of making beds	4	4	4	insufficient maintenance of assets	2	damage to or failure of technical and/or software equipment	3	no regular check of process settings	24
	4	4	4		2	loss, theft, or damage to the asset	2		16
	4	4	4		2	long-term interruption of the provision of electronic communications services, electricity supply or other long-term services	2	machines susceptible to sudden power outages	16
	4	4	4	Lack of security awareness among users, administrators, security role holders, vendors and senior management	3	Violation of security policy, unauthorized activities, misuse of privileges by users, administrators, security role holders, contractors, and senior management,	2		24
	4	4	4		3	misconduct by users, administrators, security role holders, vendors, and senior management	2		24

	4	4	4		3	Targeted cyber attack using social engineering, use of espionage techniques	3		36
	4	4	4	inappropriate access permission settings	4	misuse or unauthorised modification of information	3	no regular review of access permissions, no overview of permissions	48
	4	4	4		4	Targeted cyber attack using social engineering, use of espionage techniques	3		48
	4	4	4		4	Violation of security policy, unauthorized activities, misuse of privileges by users, administrators, security role holders, contractors and senior management,	2		32
	4	4	4	lack of staff with the necessary level of expertise	3	misconduct by users, administrators, security roles, vendors, and senior management	2	Lack of staff substitutabilit y, overloading of staff can result in errors	24
	4	4	4		3	staff with insufficient professional knowledge	2		24

Source: own processing, Cybrela (2024)

Table 14 shows risk assesment of primary asset it contains different types of vulnerabilities and threats in a security or risk management context. The table is divided into rows and columns, with each cell containing text describing specific vulnerabilities, threats, or risk levels. Each column contains numerical values or descriptive text. The cells are color-coded in shades of red, orange, and yellow to possibly indicate the severity or importance of the respective entries. This table provides a clear visual representation of various vulnerabilities and threats, serving as a useful tool for understanding and addressing potential security risks of primary asset. The values of vulnerabilities and threats were filled in after discussions with the guarantor of primary asset, the CIA triad was transferred from the record of primary asset which is from BIA. The risk level was calculated according to the formula stated in Table 13.

In the next step of the risk analysis, the vulnerabilities and threats of the supporting assets were identified and assessed according to the same methodology outlined for the primary asset.

Table 15 risk assesment of Supporting assets

Primary asset	Supporting asset	Value confidentiality	Value integrity	Value availability	Vulnerability of the PO	Vulnerability value	Threat of PO	Threat value	Specific risk/situation	Risk level
The process of making beds	**Production line**	2	4	4	insufficient maintenance of the asset	2	damage to or failure of technical or software equipment	3		24
		2	4	4		2	loss, theft or damage to the asset	2		16
		2	4	4	insufficient asset protection	3	breach of physical security	2	lack of monitoring by security cameras	24
		2	4	4		3	loss, theft or damage to the asset	2		24
	IT system for	2	4	3	insufficient backup	3	misuse or unauthorised	3		36

	production line						modification of information			
		2	4	3		3	dependence on suppliers	2	backup and IT system solved by contractors	24
		2	4	3	inappropriate access permission settings	4	Violation of security policy, unauthorized activities, misuse of privileges by users, administrators, security role holders, contractors and senior management,	2	No access records are kept, persons have redundant and extensive permissions	32
		2	4	3		4	misconduct by users, administrators, security role holders, vendors and senior management	2		32
		2	4	3		4	Targeted cyber attack using social engineering, use of espionage techniques	3		48
	Staff	2	2	2	lack of staff with the necessary level of expertise	3	misconduct by users, administrators, security roles, vendors and senior management	2		12

		2	2	2		3	staff with insufficient professional knowledge	2		12
		2	2	2	Lack of security awareness among users, administrators, security role holders, vendors and senior management	3	Violation of security policy, unauthorized activities, misuse of privileges by users, administrators, security role holders, contractors and senior management,	2		12
		2	2	2		3	misconduct by users, administrators, security role holders, vendors and senior management	2		12
		2	2	2		3	Targeted cyber attack using social engineering, use of espionage techniques	3		18
	Suppliers	2	2	2	Lack of security awareness among users, administrators, security role	3	Violation of security policy, unauthorized activities, misuse of privileges by users, administrators, security role	2	Suppliers are not trained	12

					holders, vendors and senior management		holders, contractors and senior management,			
		2	2	2		3	misconduct by users, administrators, security role holders, vendors and senior management	2		12
		2	2	2		3	Targeted cyber attack using social engineering, use of espionage techniques	3		18

Source: own processing, Cybrela (2024)

Table 15 shows risk assesment of supporting assets, it contains different types of vulnerabilities and threats in a security or risk management context. The table is divided into rows and columns, with each cell containing text describing specific vulnerabilities, threats, or risk levels. Each column contains numerical values or descriptive text. The cells are color-coded in shades of red, orange, and yellow to possibly indicate the severity or importance of the respective entries. The values of vulnerabilities and threats were filled in after discussions with the guarantors of supporting assets as well, the CIA triad was filled from the evidence of supporting assets. The risk level was calculated according to the formula stated in Table 13.

From the risk analysis performed, it was found that in the process of bed production as a primary asset, most of the risks are at a medium level, two risks at a high level and two risks at a critical level. The most critical impact on the bed manufacturing process is the vulnerability of inappropriate access permission settings, which can be exploited by the threat of misuse or unauthorised modification of information or by a targeted cyber-attack through social engineering or the use of espionage techniques. A particular risk is that permissions are not reviewed, nor is it known which employees or contractors have what permissions and what they can do with those permissions.

Within the support assets, the risk level ranges from low to critical, with the highest risk level of 48 identified for the support asset IT system to the production line, which is vulnerable to inappropriate access rights settings, and the most significant threat is a targeted cyber attack using social engineering and espionage techniques.

An acceptable level of risk has been determined. LINET has established the following criteria for accepting a level of risk where the level of risk has been determined to be low (i.e. a level of risk where the estimated damages are so small that LINET is able to cope with them in day-to-day operations). Or there would be great difficulty in implementing or operating the security measures. Unavailability of resources (financial, human or time) to implement security measures or the implementation of security measures is not in line with the priorities of the activities or the environment.

Subsequently, a risk management plan has been developed that includes all risks that have not been accepted. Based on the selected risk management option, a decision was made on how each risk would be managed (corrective action) and who would be responsible for managing it (risk owner). The plan was drawn up based on a discussion between the responsible persons on the appropriateness of the individual safety measures and the exact way in which the risks would be managed, and the specific persons responsible for managing the risks concerned and the date by which the risks would be managed were identified. The risk management plan shall include all risks with a risk level of medium, high, and critical. In this thesis, only some of the identified risks have been highlighted in the risk management plan.

Table 16 Risk Management Plan:

Risk Management Plan (Sample of the Table)									
				Measures				Check	
Risk	**Value at risk**	**Asset**	**Source of findings**	**Priority**	**Measures**	**Responsible person**	**Completion date**	**Deadline**	**Status**
cyber attack on the system due to improperly set access permissions	48	IT system for production line	risk analysis	1	a review of access rights and removal of redundant	Veronika Forgotname	20.04.2024		
modification of information due to inappropriately set permissions	48	the process of making beds	risk analysis	1	protection of the system against unauthorised modification	Michal Písař	01.02.2024		
damage to the company by a cyber attack due to inadequately trained employees	36	the process of making beds by employees	risk analysis	2	introduction of regular training and testing of employees	Michal Písař and Vilibald Malý	30.08.2024		
access rights broader than needed allows sabotage by employees	32	the process of making beds	risk analysis	3	removal of redundant rights and increased control over employees – introduction of logging	Michal Písař	15.09.2024		

backups of the production line IT system are permissible for modifications	36	IT system for production line	risk analysis	4	improvement of IT system protection	Veronika Forgotname	10.10.2024		
employees may accidentally damage the IT system they have unnecessary access to	32	IT system for production line	risk analysis	5	removal of access, introduction of training	Veronika Forgotname	15.10.2024		
untrained contractors can be targeted in a cyber attack and harm LINET	18	Suppliers	risk analysis	6	introduction of supplier training and knowledge test	Marek Novotný	01.12.2024		
lack of monitoring by security cameras	24	Production line	risk analysis	7	purchase of a camera system	Daniel Přibyl	01.06.2025		

Source: own processing, Cybrela (2024)

Table 16 is Risk Management Plan. It details various risks, their values at risk, sources, priorities, measures to mitigate them, responsible persons for these measures, completion dates, deadlines, and statuses. The values were obtained from tables 15 and 14, the priority was determined also considering the data from table no. 9. During discussions with the guarantors of the assets, the responsible persons were determined and after consultation with the management, the expected completion dates were set.

3.2.3 Responsibility Matrix and Incident Response Plan

A responsibility matrix, also abbreviated as a RACI matrix, is a model used most in project management, but it is a valuable tool in crisis management as well. Usage of such a matix will be enforced by the new cybersecurity law and it is a part of the ISO 27001 standard. It helps define which company members are responsible for which tasks. When drafting a RACI matrix, it is important to have a good understanding of roles and responsibilities in your team. Part of the matrix should also be focused on dealing with possible incidents. This matrix will help your team to deal with an incident swiftly and without confusion. It shows who to consult, who should be responsible for dealing with the accident etc.

The RACI matrix does not have a standardized look, its main requirement is that it needs to be easily readable and understandable. A possible look for a RACI matrix could be as shown below. The matrix shown below is a special metrix regarding cybersecurity management, and it was made according to the recommendations of the draft of new cybersecurity law, which is currently in a legislative session.

Vital part of establishing this matrix is the understanding of how it works. Usual RACI matrix contains two parts - description of which areas need to be managed and identification of roles potentially responsible for those areas. Inside of the matrix are the 4 letters - R, A, C, and I. One role can be responsible/accountable etc. for more than one activity.

- **R** - stands for "**Responsible"** (does the job) - This role performs the task alone or in cooperation.
- **A** - stands for "**Accountable"** - This role is responsible for the task. Sometimes, this can also be found in the variant "**Approver**".
- **C** - stands for "**Consulted**" - Solutions for potential problems or tasks within this category need to be consulted with this role.
- **I** - stands for "**Informed**" - This role needs to be informed about the solution and the progress of the work on the problem.
- **S** - stands for "**Supported**" - Sometimes, part of the matrix can also be "S", however it is not standard. This is used for a person who can possibly support performing the task at hand. Usually, "S" is not used.

Table 17 RACI matrix:

Area	Roles							
	Cybersecurity comitee	Cybersecurity manager	Cybersecurity architect	Cybersecurity Auditor	Guarantor of the primary asset	Supporting asset guarantor	Security Manager	Administrator
Cybersecurity management	**A**	**R**	**R/C**	**I**	**R**	**R**	**R**	**R**
Cybersecurity audit	**I**	**C/I**	**C/I**	**A/R**	**C/I**	**C/I**	**C/I**	**C/I**
Design of security measures	**A**	**R**	**R**	**I**	**C**	**C**	**C**	**C**
Implementation of security measures	**I**	**A**	**C**	**I**	**R**	**R**	**A**	**R**
Ensuring the development, use and security of the primary asset	**I**	**C**	**C**	**-**	**A**	**R**	**C**	**R**
Ensuring the development, use and security of the support asset	**I**	**C**	**C**	**-**	**C**	**A**	**C**	**R**
Cybersecurity incident management	**C/I**	**R/A**	**I**	**I**	**I**	**I**	**I/C**	**R**

Source: own processing, Cybrela (2024)

This 17 serves as a RACI matrix that outlines the roles and responsibilities in different areas of cybersecurity management. The roles include Cybersecurity Owner, Cybersecurity Manager, Cybersecurity Architect, Auditor, Guardian of the asset, Supporting Asset Security Manager, and Administrator. Each cell in the matrix contains letters representing Responsible (R), Accountable (A), Consulted (C), or Informed (I). Some cells contain combinations like “R/C” or “C/I”, indicating shared or overlapping responsibilities. The table 17 was filled out by security manager and approved by management of LINET.

If the matrix is investigated, the most important part for the described security incident can be found in the last row. "Cybersecurity incident management" is indicated as telling us which roles are responsible for dealing with this. In the case of a ransomware attack, the most important person will undoubtedly be identified as a cybersecurity manager. Responsibility for starting the process of incident response will be his.

After being informed about the incident, the other roles should be informed by the cybersecurity manager as soon as possible, so that the whole company is aware of what is happening, what to do, and what to expect in the upcoming hours or even days. This is how the importance of the incident response plan is realized.

Incident response plan is a very important guideline, especially during a possible crisis. It is a structured approach outlining the steps an organization takes to address and manage security breaches or other unexpected events effectively. Typically, it encompasses predefined procedures, roles, and responsibilities designed to mitigate damage, minimize recovery time, and maintain business continuity. This plan should be linked to other company documents, such as risk assessment and business continuity plan. This plan is crucial fot containment of possible incidents. It delineates how incidents are reported, investigated, and escalated, specifying communication protocols both internally and externally. Moreover, an incident response plan includes strategies for evidence collection, forensic analysis, and restoration of systems or data. Regular testing and updating of the plan are crucial to ensure its effectiveness in adapting to evolving threats and technologies. That is why the last step should always be implementinog of "lessons learned", topic covered in paragraph 3.4. Ultimately, the goal of an incident response plan is to respond to incidents, reducing their impact and safeguarding the organization's assets and reputation swiftly and efficiently.

The following is an example of an incident response plan, which could possibly be used for LINET.

Table 18 Incident response plan

What needs to be done?	**Who is responsible?**	**When is it necessary to take this action?**	**Notes or other information**
1. First reactions			
If a cyber-attack is detected or suspected, the person who discovers (or merely suspects) the fact shall report to the IT department.	Anyone spotting the mistake or an incident	Immediately	IT department: phone number: *xxxx* Outside of the typical working hours, call: *xxxxx* (cybersec manager) or *xxxx* (hotline)
Conduct an initial spot check of the system with emphasis on the reported problem and its impact on data and systems. The aim is to confirm or refute the attack, or to determine its nature.	Cybersecurity manager, figuratively anyone in the IT department aviable	Immediately	
Depending on the result of the inspection, immediately	Cybersecurity manager, figuratively	Immediately	

suspend/isolate the affected system or restrict related. In the event of a ransomware attack, also immediately: a) disconnect the backup device from the network and turn it off, b) disconnect the company network from the Internet, c) shut down all servers.	anyone in the IT department		
Inform the members of the CZ Crisis Team for these cases (hereinafter referred to as the Crisis Team). This column should contain	Cybersecurity manager, figuratively anyone in the IT department		By phone xxxxx
Inform all employees of LINET about the incident	xxxxxxx		In the manner as specified: An email-message must be sent to with the following parameters: 1. it must be sent with HIGH PRIORITY 2. the message must be sent from a LINET email-address only (emails from your external IT contacts do not work) ATTENTION: please send emails in cause of a high priority security incident only - not just for updates or information. Every email where both conditions (high priority & LINET email-address) are fulfilled/met will trigger emergency information (phone call, sms, email, teams-message) to every person, which is nominated as emergency contact - at every day/nighttime.

2. **Finding out the details**			
Review the logs to the systems concerned in the period since the probable loss/disclosure and, if positive, further review the changes and accesses made to the systems during the period concerned.	Cybersecurity manager, figuratively anyone in the IT department	Immediately	Provide external support as required to identify the impact of the incident and resolve it: Here could be listed some external companies on-call for these specified cases (e.g. because of an service licence agreement)
Perform content analysis of the changed/read data.	Cybersecurity manager, figuratively anyone in the IT department	Immediately	
Carry out checks on movements in bank accounts. Block a company's credit cards in the event of a suspected data leak.	*Here should be a name of a person with prerogatives to control a financial account*		*Here should be a contact of a person with prerogatives to control a financial account*
To summarize the impact of the attack on: - availability of systems and data for staff and clients, - data confidentiality (data leakage), - data integrity (data corruption). Inform the Crisis Team of the outcome.	Cybersecurity manager, figuratively anyone in the IT department		Via email or a dedicated Teams channel
Inform the group of the nature and impact of the attack.	Cybersecurity manager, figuratively anyone in the IT department		In the manner specified - see the above-mentioned procedure for high priority messages.
Inform about the nature and impact of the attack: a) partners of the company b) all employees	Crisis team - member in charge		By email, if possible. Otherwise by SMS through the O2 SMS gateway or by phone, or with the involvement of team leaders.

Also consider the potential impact on employees' private data (e.g. personal credit cards, access to int. banking) if it is suspected that they may have been leaked. Provide everyone within the company with basic information on how to communicate with clients.			A copy of the employee directory shall be maintained in a separate part of the network.
3. Attack recovery			
Initiate work to deal with the aftermath of the attack, selecting a course of action according to the specific situation.	IT		
As part of the solution, consider the possibility of restoring from a backup, both full and partial, if possible.	IT		
4. Informing clients and state authorities			
Prepare information for clients about the attack, describing the impact on: a) client data, b) availability of client applications, c) the provision of services and the fulfilment of deadlines by.	Crisis team - designated member; cooperation with PR agency, internal and external lawyers		Contact *Here should be a list of contacts useful in this situation*
Send/forward information to clients. Consider specific provisions in contracts with certain clients.	Crisis team - designated member; collaboration of managers and staff responsible for clients		By email, if possible. Otherwise by telephone with the involvement of managers and other staff responsible for clients. A copy of the client directory and a list of specific contractual arrangements will be maintained in a separate part of the network.

Instruct management or all staff on how to answer client questions. Prepare and update the Q&A list.	Crisis team - member in charge		
Inform the National Office for Cyber Security (NUCS) and the Police of the Czech Republic. *Note: this section is mandated by law*	Internal and external lawyers		Actively cooperate with the Police of the Czech Republic and provide all required logs and information.
Inform the Data Protection Authority (DPA) in accordance with the GDPR plan if personal data has been leaked.	Internal and external lawyers		Procedure and contacts in the GDPR plan *(if it exist)*
After the incident is resolved, update this plan with possible "lessons learned".	Crisis management team along with every role responsible for cybersecurity		

Source: own processing, Cybrela (2024)

Table 18 outlines an incident response plan for handling cyber-attacks. The table is divided into four columns: What needs to be done? Who is responsible? When is it necessary to take this action? and Notes or other information. The first part of the table addresses initial reactions to a suspected cyber-attack. The next parts of the table include more detailed steps such as finding out the details of the attack, recovery from the attack, informing clients about the incident, and reporting to state authorities. This table was filled by security manager with cooperation of IT and other management roles includede in the table.

While this incident response plan is easy to follow, it is also very important that all the phone numbers and other contact details it contains are regularly updated and checked. It is not important to mark the procedure step-by-step, as many of them can be taken simultaneously, but some baselines should be met.

Regarding the incident described in the section 3.1.2, this incident response plan should be activated as soon as an employee finds out about the incident happening, so in this case, 13.11.2023 at 7:00. Employees can first investigate the RACI matrix, which should be aviable to them as a part of a company policy and which they should be trained to use, and after finding out that the cybersecurity manager is responsible for dealing with a potential cybersecurity incident. Said manager should then activate the incident response plan.

3.2.4 Business Continuity Plan and Disaster Recovery Plan

The Businceess continuity plan (also reffered to as BCP) and Disaster recovery plan (also referred to as DRP) (often, these two plans are referred to jointly as BCDR) were developed in accordance with the established methodology in order to be consistent with NIS 2, the draft new law on cybersecurity, and the draft Decree on security measures of a regulated service provider under the regime of higher obligations, as well as with the practical functioning of LINET.

This diploma thesis presents a sample of the BCP and DRP, in an updated form, as it should have been (ideal state) before the cybersecurity incident.

3.2.5 Business Continuity Management

Business continuity management oversees a business's continuity plan. This type of management determines the potential threats to a company and how each of these threats might impact business functions. Based on these findings, business continuity management can tweak the company's continuity plan to address any new potential hazards. One responsibility that business continuity management team has is planning for disaster recovery. Disaster recovery is a component of the business continuity plan that specifically focuses on product issues. In addition to that, business continuity management also includes crisis management, contingency planning, and emergency management.

The measures resulting from the business continuity management target the LINET Group's ability to respond quickly and effectively to situations related to adverse influences beyond its control (e.g. natural disasters) or cyber security incidents. Failure to prepare for such situations would risk total or partial interruption of the provision of the regulated service for an unacceptably long period of time. All LINET Group employees are obliged to comply with the business continuity management documents thus established. Its implementation is monitored by senior employees within the scope of their defined authority and responsibility.

Business continuity management is perceived as a process that was enabled by LINET to effectively bridge business disruptions and restore key services and processes after a disaster. The aim, therefore, was to mitigate the impact of the service outage and restore functionality as quickly as possible. It was key for LINET that crisis scenarios and partially drawn-up plans were in place to be activated and restore the organization's core functions and services. In hindsight, it can be confirmed that the business continuity management of an organization is not only about rectifying the consequences caused by incidents or accidents but is also about preventing crisis and emergency situations.

As part of business continuity management, for LINET are created:

- Business Continuity Management Policy

The purpose of this policy is to set out the principles of business continuity management and to set out the procedures and rules for back-up. This measure aims at LINET's ability to respond quickly and effectively to situations related to adverse influences beyond its control, e.g. natural disasters, or cyber security incidents. Failure to prepare for such situations would risk total or partial interruption of the regulated service for an unacceptably long period of time.

- Business continuity plan

A plan for responding quickly to an emerging security incident, to maintain uninterrupted processing and delivery of primary assets. It describes the specific resources, activities and tasks that need to be provided to restore processing and provision of primary assets.

- Disaster recovery plan

A plan for rapid response to a security incident to restore functionality of supporting assets. Describes the specific resources, activities, and tasks that need to be provided to restore, e.g., servers, backups, power, etc.

- Business Continuity Management Indicators

RPO (Recovery Point Objective) - the time from the last backup to the occurrence of a cybersecurity incident. Indicator of the amount of data we are willing to lose in that time/period. To recap, for LINET, the RPO was evaluated at 30 days.

RTO (Recovery Time Objective) - the time from the occurrence of a cybersecurity incident to recovery. An indicator of the time by which services or access must be restored after a cybersecurity incident. To recap, for LINET, the RTO was evaluated at 30 days.

MTDL (Maximum Tolerable Data Loss) - an indicator of the acceptable level of information loss due to a cybersecurity incident. An indicator of the frequency of backups.

MTO (Maximum Tolerable Outage) - a time indicator of the acceptable level of service outage due to a cybersecurity incident. Backup frequency indicator. May be the same as MTDL.

MRSL (Minimum Required Service Level) - an indicator specifying the minimum level of service at which the system objective is assured. SLA.

Business Continuity Management Policy

LINET's employees, contractors and third parties who, as part of their employment or business, interact with the part of the company that performs the regulated service and may meet the company's assets on which the provision of the regulated service is dependent are required to comply with the LINET's Business continuity management policy. Its performance shall be monitored by senior employees within the scope of their authority and responsibility.

According to the Decree on security measures of a provider of a regulated service under a higher duty regime, a business continuity management policy shall include:

a) Rights and duties of responsible persons

This section of the LINET's Business continuity management policy states that business continuity processes are managed and documented, including defining the rights and responsibilities of the ICT department and those in security roles.

b) Business continuity management objectives for each service

This section of the Policy mainly states that Methodology for conducting the Business impact analysis (BIA) is established. The assessment of the impact of the cybersecurity incident on continuity and the assessment of the associated risks is part of the impact analysis in the framework of the assessment of the primary assets and their links to the supporting assets. In

determining the value of the assets and the associated risks, the impact on the continuity of the activities of the asset must be considered.

The objective of business continuity management is based on the outputs of the risk assessment and impact analysis:

- Establish minimum service levels for each LINET's agency,
- ensure the security and continuity of ICT service provision in the event of a cybersecurity event or incident, emergency, or disruption of ICT service provision,
- set business continuity management objectives regarding minimum service levels, IS recovery time and data recovery point,
- initiate steps to ensure that services are restored to the required level,
- minimise damage to LINETs property or assets resulting from the emergency.

Each ICT element must have defined recovery time of operation (RTO) and data recovery point (DRP).

To meet business continuity objectives, Business continuity plan and Disaster recovery plan are developed, managed, and regularly updated by the Cybersecurity manager.

The backup, retention, and archiving policies are set and access to backup databases and the functionality of the backups and other vital records will be tested periodically, and a record will be made of this.

As business continuity management depends in many respects also on the interaction and cooperation with suppliers, it is imperative that suppliers are obliged to be familiarised with the Policy when signing the contract, or it is possible that the relevant extract of the Policy is included in the contractual documentation.

c) Prioritisation of individual services

Business continuity plan and Disaster recovery plan define the importance of individual services so that it is clear which parts of the infrastructure need to be restored first in the event of an emergency.

d) Methods of crisis communication and reporting, Communication matrix with key persons for each service, Escalation procedures for crisis situations

The Business continuity plan and Disaster recovery plan set out the procedures and modalities for crisis communication within the LINET, including rules for reporting crises and incidents to those responsible. It should also be defined how, for example, communication towards customers will take place if they are also affected by a service outage. In addition, a communication matrix is established that identifies the key persons and contacts for each defined service. This matrix ensures a quick and efficient involvement of the responsible persons in case of emergencies. Escalation procedures are defined for cases where standard measures are not effective and the emergency requires the involvement of other departments, senior management units, external persons or authorities.

e) Catalogue of crisis scenarios

The Business continuity plan and Disaster recovery plan define a catalogue of different emergency and crisis scenarios that may affect LINET. Each scenario, according to the Policy,

must be accompanied by a plan to respond adequately and minimize the impact on the service being operated.

f) Procedures for starting and stopping system operation, for restarting or restoring system operation after a failure, and for handling error conditions or emergencies.

LINET's Operational Guidelines define procedures and protocols for starting and stopping the system, restarting, and recovering the system after a failure, and for handling error conditions or abnormal events.

g) The method and period for testing each business continuity plan and recovery plan.

As stipulated in the Policy, the ICT department tests Business continuity plans and Recovery plans, i.e. the ability to restore, according to set procedures, the operation of servers, including data recovery. It is not always necessary to test the entire infrastructure, but it is usually sufficient to test the functionality of the set procedures through a mock recovery of one system.

h) Procedures for the implementation of measures issued by the NUKIB.

The NUKIB publishes the currently effective measures on its official website. The Cybersecurity Manager shall inform the Cybersecurity Committee of the issued measure or directly order the IT Administrator or other responsible persons to implement the measure, depending on the scope and content of the measure.

Business Continuity Plan

Business continuity can be defined as the ability of an organisation to continue to deliver products or services at a predefined acceptable level after a disruptive incident. In addition to prevention, the objective is to enable uninterrupted operations before and during the execution of disaster recovery. The term 'strategic resilience' is also now used, which goes beyond resisting a one-off crisis, but rather continuously anticipating and adapting.

Business continuity plan outlines a range of disaster scenarios and the steps the business will take in each specific scenario to return to business as usual. Business continuity plan, which must be developed with input from key staff as well as stakeholders, is a set of contingencies to minimize potential damage to the business during adverse scenarios. Any event that could have a negative impact on operations, such as supply chain disruption, loss, or damage to critical infrastructure (major machinery or computing/network resources) should be included in the plan, and it is necessary to prepare a resolution for each.

The LINET's Business continuity plan as a formal document outlines directions and procedures that the company will follow when faced with a crisis. This plan includes contingencies for business processes, assets, human resources and business partners, actions, processes, and tools for ensuring the organization can continue critical operations after a disastrous event, and other helpful information. The goal of the Business continuity plan is to handle anything from minor disruptions to full-blown threats. It represents all the task and activities required to bring the organization back to normal operations following a disaster.

Here are 6 basic steps that were kept in mind when putting together The LINET's Business continuity plan:

I. Initiation Plan

The process has begun with the initiation of the business continuity planning effort, where the emergency preparedness team was established, key stakeholders were identified, and the scope and objectives of the plan were established.

- Emergency Management Team (EMT)

It is recommended that teams are formed from a diverse cross section of employees such as IT, HR, Public Relations, Operations, and Legal/Regulatory/Compliance.

Description of the tasks: Responsible for coordination on the initial activities of a disaster such as assessing damage and officially declaring the event a disaster which invokes the execution of the plan.

Support activities:

- Assess initial damage & activate the plan.
- Determine recovery actions needed.
- Set the recovery priorities based on the damage.
- Provide status updates to senior leadership.
- Establish Command Center
- Disaster Recovery Team (DRT)

Description of the tasks: A much larger team with a more tactical focus responsible for doing the groundwork to recover and communicating the status on all individual parts during recovery.

Support Activities:

- Execute plan procedures.
- Assist in relocation as needed.
- Provide status updates.
- Replace broken equipment & salvage useful equipment.

II. Identifying Critical Functions and Types of Threats

Critical business functions were identified along with potential threats that could disrupt these functions, such as natural disasters, cyberattacks, or supply chain disruptions.

III. Conducting Risk Assessment Across Each Area Identified

Risks associated with each critical function and potential threats were assessed to determine their likelihood and potential impact on business operations (see Section 3.2.2)

IV. Conducting Business Impact Analysis

The next important step in the business continuity planning was Business impact analysis, within as it was mentioned above this thesis, at LINET, it was identified critical business functions and processes along with the resource requirements necessary to sustain operations. Through risk assessment and business impact analysis, LINET knows the critical services and the supporting assets that enable them to run and knows where it has weaknesses to target with corrective action. Hence, the team creating the Business impact analysis had to look at the organization from many different angles and use information from a variety of sources. It's an ongoing process, as things can and will change over time.

V. Draft of the BCP

A demonstration of the LINET's business continuity plan will be provided below within this thesis.

VI. Testing and Maintaining BCP

Regular testing and maintenance of the Business continuity plan ensure its effectiveness in real-world scenarios and enable timely updates to address evolving threats and business needs.

Table 19 Business Continuity Plan

Business Continuity Plan

ID	Plan name	Description of the emergency situation	Plan owner	Emergency management procedure (individual activities)	Estimated lead time	Responsibility for implementation	Contact	RTO	RPO	Information about backup sources	Testing	Date of update
1	Security breach of IT and OT systems	It can involve a variety of scenarios, including sensitive data leakage, unauthorised access to IS, disruption of industrial equipment, misuse of access credentials, ransomware extortion and physical damage to equipment. These incidents can have serious consequences including loss of credibility, production downtime, financial losses and security threats.	Cybersecurity manager	1) isolating storage/ disconnecting systems from the network/ deactivating accounts 2) inform EMT and stakeholders 3) rapid analysis 4) data storage recovery 5) external communication - media, customers, NUKIB 6) testing 7) taking action to improve procedures	10 hrs	Head of IT/ Cyber Security Manager	70533311 70550039	30 day	30 day	Cloud	Yes	10.3.2024
2	Server security breach	If the security of servers is breached, data can be compromised and can be misused or stolen.	Cybersecurity manager	Informing the responsible person, prioritizing, technically ensuring that the	5-10 hrs	Head of IT/ Cyber Security Manager	705 333 111	30 day	30 day	Cloud	Yes	10.3.2024

				problem is corrected			705 500 390					
3	Communication network security breach	When the security of a communications network is breached, data protection, user privacy, and the stability of network operations can be compromised.	Cybersecurity manager	Informing the responsible person, prioritizing, technically ensuring that the problem is corrected	5-10 hrs	Head of IT/ Cyber Security Manager	705 333 111 705 500 390	30 day	30 day	Cloud	Yes	10.3.2024
4	Network device security breaches	A security breach of network devices such as routers, switches, firewalls, access points, or other network devices can have serious consequences for network security and operations.	Cybersecurity manager	Informing the responsible person, prioritizing, technically ensuring that the problem is corrected	5-10 hrs	Head of IT/ Cyber Security Manager	705 333 111 705 500 390	30 day	30 day	Cloud	Yes	10.3.2024
5	Violation of cabling and structured cabling security	Violation of the physical security of cables used for data transmission and communication between different devices such as computers, servers, switches, routers, etc. It can lead to loss of connectivity, unauthorized access to data, etc., and violation of the protection of network cabling used for data transmission and communication within an organization or building. These can be both physical and logical breaches that	Cybersecurity manager	Informing the responsible person, prioritizing, technically ensuring that the problem is corrected	3-5 hrs	Head of IT/ Cyber Security Manager	705 333 111 705 500 390	30 day	30 day	Cloud	Yes	10.3.2024

		can have serious consequences for network security and operations.										
6	Inaccessibility of objects	Denied physical access to key facilities - flooding, malicious intent	Cybersecurity manager	Informing the responsible person, prioritizing, ensuring that the problem is corrected	5-10 hrs	Operations Manager/ Cyber Security Manager	705 454 111 705 500 390	30 day	30 day		Yes	10.3.2024
7	Unavailability of energy resources	Electricity, gas outage	Cybersecurity manager	Informing the responsible person, prioritizing, ensuring that the problem is corrected	5-10 hrs	Operations Manager/ Cyber Security Manager	705 454 111 705 500 390	30 day	30 day		Yes	10.3.2024
8	Unavailability of utilities	Drinking and wastewater	Operations Manager	Informing the responsible person, prioritizing, ensuring that the problem is corrected	24 hod	Operations Manager	705 454 111	30 day	30 day		Yes	10.3.2024
9	Unavailability of staff	Lack of staff to run primary assets	Operations Manager	Informing the responsible person, prioritizing, ensuring that the problem is corrected	8 hod	Operations Manager	705 454 111	30 day	30 day		Yes	10.3.2024
10	Unavailability of supplier services	A major supplier stops providing its services (service outage)	Cybersecurity manager	Informing the responsible person, prioritizing, ensuring that the problem is corrected	30 day	Operations Manager/ Cyber Security Manager	705 454 111 705 500 390	30 day	30 day		Yes	10.3.2024

Source: own processing, Cybrela (2024)

Table 19 contains a table outlining a businness continuity plan. It details immediate actions, responsible parties, and timing for these actions. The plan was filled out by the guarantors of primary assets and the cybersecurity manager.

Table 20 BCP Communication and substitutability matrix

Communication matrix within BCP			
The role of cyber security	**Person**	**E-mail**	**Phone**
Operation manager	Ing. Pavel Kožený	Pavel.Kozeny@ casestudy.neverforget.grizz	+420 1212 1976 -420 2010 2023
Cybersecurity manager	Manfred Graeber	Manfred Graeber@ casestudy-LINET.com	-420 987 654 321
Asset guarantor (Production line)	Stanislav Ondráček	Standa.Ondrace@ mentor-LINET.com	-420 111 222 333
The matrix of substitutability			
Person	**Who represents the person**	**E-mail**	**Phone**
Operation manager	Rozalie Germiova	Rozalie.Germiova@casestudy-LINET.com	+420 3011 2018
Cybersecurity manager	Jiří Němeček	Jiri.Nemecek@casestudy-LINET.com	+420 2507 1968
Asset guarantor (Production line)	Jonáš Germi	Jonas.Germi@casestudy-LINET.com	+420 2310 2020

Source: own processing, Cybrela (2024)

Table 20 is divided into two sections. The first section lists roles in cyber security, the persons assigned to those roles, and their contact information. The second section indicates who can substitute for each role and provides their contact information. The table was filled out by cybersecurity manager.

Disaster Recovery Plan

A Disaster Recovery Plan is a strategic document that describes how an organization can recover quickly after an unplanned incident. It typically includes an analysis of business processes and continuity needs. The main goal is to have critical information systems brought back online and to minimize downtime for servers, databases, and employee workstations. Strategies for Disaster Recovery Plans vary. However, as has been learned from the experience at LINET, it should always begin at the business level, i.e., by determining which applications are most critical to the operation of the organization and the business.

Due to the predicament, a crucial discovery was being sought. Initially, it was believed that LINET would require only one recovery strategy to rebuild the entire business. However, this proved to be impractical. If there is a single document for enterprise-wide recovery, it becomes so huge and complex that testing or successfully implementing it would be impossible. Not to mention, updating it when the environment changes is also unfeasible. Therefore, it is common for most organizations to have multiple types of continuity and disaster recovery plans, for example for:

- Application-level failures,
- site-level failures,
- infrastructure component failures,
- critical applications,
- development/testing applications.

In the case of the LINET network, one robust Disaster Recovery Plan had been developed for all IT systems, which was identified as the first mistake as explained above. Furthermore, it was not considered necessary to develop a Disaster Recovery Plan for part of the Operational Technology, because OT systems are managed by the supplier and, as such, it was assumed that their disaster recovery plans were also managed only by the supplier. Below, a practical example of the newly developed Disaster Recovery Plan for OT alone will be provided.

Table 21 Header of the Disaster Recovery Plan

DISASTER RECOVERY PLAN	
Crisis (one of the variants)	• Application-level failures • Infrastructure level failures • Failure of the IT due to a cyber security incident • **Failure of the OT due to cybersecurity incident**
Plan owner	Cybersecurity manager

Source: own processing

Table 21 outlines various crisis situations and identifies the plan owner responsible for addressing each situation.

Entry and Exit Criteria

This plan will be activated or deactivated based on the official decision of the authorized escalation contact and senior leadership using input from the various recovery teams. Regardless of disaster circumstances (natural, man-made), the entry and exit criteria will be defined as follows:

Activation (Entry) Criteria:

- Total loss of the communication network
- Total loss of the production line
- Total loss of the main building
- Flooding of the premises

Deactivation (Exit) Criteria

- Total restoration of the communication network
- Total restoration of the production line
- Total restoration of the main building
- Remoal of flooding damage from the premises

Table 22 Measurements in the DRP

MEASUREMENTS		
Chronologically ordered activities in case of plan activation	**Person responsible**	**Max. duration of activity**
1. A) Immediately notify the Emergency Management Team (EMT) Authorized Escalation Contact, Martin at 705-323-875 (24/7) for direction on next steps. B) Convening the research team	Head of IT/ Operations Manager/ Cyber Security Manager	90 min
2. Check and identify the cause	Infrastructure manager/co-operation OT supplier	120 min
3. DRP plan activation and unavailability information	Head of IT/ Head of IT/ Operations Manager	10 min
4. Reporting to the relevant supervisory authorities	Head of IT/ Operations Manager/ Cyber Security Manager	30 min
5. Solution	Head of IT/Infrastructure manager/co-operation OT supplier	180 min
6. Functionality testing and information on the commissioning of the DRP termination, alternatively, there may be a transfer of the production process	Infrastructure manager/Asset guarantors/users	120 min
7. Evaluation	Head of IT/ Operations Manager/ Cyber Security Manager	60 min
End (Total duration, which must ideally be less than the specified RTO)		550 min

Source: own processing, Cybrela (2023)

Table 22 outlines the chronologically ordered activities that should be undertaken in case of a disaster recovery plan activation. It includes the person responsible for each activity and the maximum duration for each activity. The activities listed range from notifying the Emergency Management Team to evaluating the entire process. The table was filled out by the IT manager and was consulted with various business roles and Cyber Security Manager.

Table 23 Solution Activities Performed

SOLUTION

ACTIVITIES PERFORMED			
Activity	**Employee involved**	**Supplier involved**	**Note**
Servers			
1. Closing traffic from the internet	Head of IT/Infrastructure manager	OT supplier	
2. Resetting factory settings	Head of IT/Infrastructure manager	OT supplier	
3. Preparing the image and USB installation disk	Head of IT/Infrastructure manager	OT supplier	
4. Clean installation	Head of IT/Infrastructure manager	OT supplier	
5. Installing antivirus	Head of IT/Infrastructure manager	OT supplier	
6. Setting rules on the local firewall	Head of IT/Infrastructure manager	OT supplier	
7. Online updates of antivirus databases and definitions	Head of IT/Infrastructure manager	OT supplier	
8. Scanning the system with antivirus	Head of IT/Infrastructure manager	OT supplier	
9. Verification of server functionality	Head of IT/Infrastructure manager	OT supplier	
10. Setting intra-network traffic rules and remote access rules	Head of IT/Infrastructure manager	OT supplier	
Hospital bed production information system			
1. Installation of the information system from the image/disk	Head of IT/Infrastructure manager	OT supplier	
2. Setting	Head of IT/Infrastructure manager	OT supplier	
3. Restoring an information system configuration from a backup disk	Head of IT/Infrastructure manager	OT supplier	

4. Verification of the functionality of the information system	Head of IT/Infrastructure manager	OT supplier	
Data recovery			
1. Validating backups, finding the last working backup	Head of IT/Infrastructure manager	OT supplier	
2. Scanning backups with antivirus	Head of IT/Infrastructure manager	OT supplier	
3. Importing data into the restored information system	Head of IT/Infrastructure manager	OT supplier	
Transfer of the production			
1. In case the previous steps have failed or require an immense amount of time at the expense of the production, the next step is to move the production – LINET branch, Novohradska street 82. The restoration at the main site is continuing.	Operations Manager/ Cyber Security Manager/users	OT supplier	
2. Staff redeployment	Operations Manager/ Cyber Security Manager/users	OT supplier	
3. Commencement of production according to established procedures until completion of the defect	Operations Manager/ Cyber Security Manager/Users	OT supplier	

Source: own processing

Table 23 outlines the activities performed related to servers, hospital bed production information systém, Data recovery and transfer of the production. It includes the employee involved in each activity and any supplier involved. The table was filled out by the IT manager and was consulted with various business roles and Cyber Security Manager.

RTO - 30 days

RPO - 30 days

SLA - 45 days

Table 24 Disaster Recovery Plan Activation Priorities

DRP ACTIVATION

PRIORITY OF COMMISSIONING		
Asset (affected components)	**Responsible**	**Target values**
Windows server	Head of IT/Infrastructure manager	Server installed, patched, connected to AD
SQL server	Head of IT/Infrastructure manager	Server installed, patched, connected to AD, connected to backup client
IS operating the production line	Head of IT/Infrastructure manager	Functional IS with user rights
Backups	Head of IT/Infrastructure manager	Backup is available, SQL connected, DB restored, Data return to the last backup point
Production line	Head of IT/Infrastructure manager	Functional
Ordering application and service management	Head of IT/Infrastructure manager	Functional

Source: own processing

Table 24 outlines the priority of commissioning for various assets in the event of a disaster recovery plan activation. It includes the asset affected, the person responsible for each asset, and their target values. The target values indicate the desired state of each asset after the recovery process, such as being installed and patched or functional. The table was filled out by the IT Manager and was consulted with various business roles and Cyber Security Manager

Table 25 Emergency Contact Information

CONTACTS		
Role	**Name**	**Phone**
Infrastructure Manager	Veronika Viková	+420 2202 1983
OT Supplier	Míla Krtek Richard Šubrt	+81 230 230 230
Head of IT	Vojtěch Müller	+420 2210 1990
Operations Manager	Ing. Pavel Kožený	+420 1212 1976 - 420 2010 2023
Cybersecurity Manager	Jiří Němeček	+420 2507 1968

Source: own processing

Table 25 provides the roles, names, and phone numbers of individuals in specific positions related to infrastructure management, IT, operations, and cybersecurity. The table was filled out by the IT manager and was consulted with various business roles and Cyber Security Manager.

Table 26 Other information in DRP

OTHER INFORMATION	
Storage plan	External disk in the safe, printed form in a locked cabinet – room 123, spare keys are at the concierge desk
Testing period	1 year
Date of creation of DRP	10.03.2024
Date last updated	10.03.2024

Source: own processing

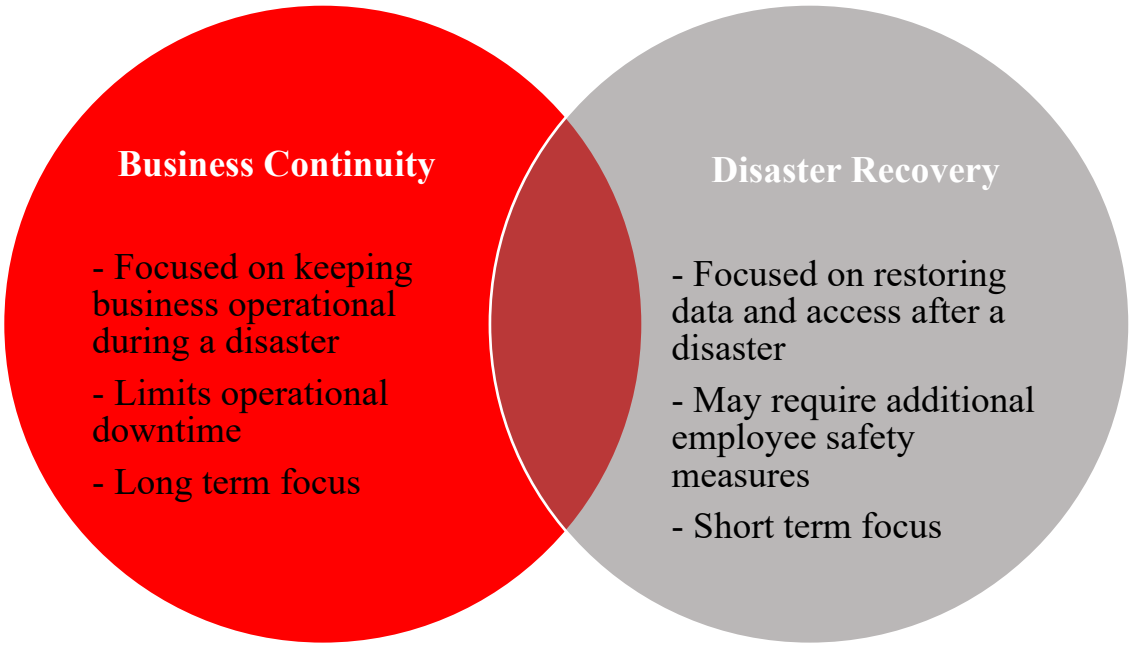
Table 26 provides additional details related to a Disaster Recovery Plan. It indicates where the plan is stored, the frequency of its testing, and the dates of its creation and last update. The table was filled out by the IT manager and was consulted with various business roles and Cyber Security Manager.

Difference between Business continuity plan and Disaster recovery plan and common pitfalls

The difference between Disaster recovery and Business continuity plans as it has been showen in this thesis, lies in that Disaster recovery plans are technical plans focused specifically on recovering from failures, while business continuity plans manage relationships during a crisis. Disaster recovery plans are created as part of an overarching Business continuity plan.

For example, in the case of LINET's crisis - we also lost IT services due to OT failure. So, part of a larger business continuity plan was one or more disaster recovery guidelines that would focus specifically on restoring those IT services.

Picture 3 Differences between Business Continuity Plan and Disaster Recovery Plan



Source: own processing, Cybrela (2024)

Picture 3 represents a Venn diagram. The diagram has two overlapping circles, one representing Business Continuity and the other representing Disaster Recovery. It illustrates the distinct yet interconnected roles of Business Continuity plan and Disaster Recovery plan.

Based on a crisis that was dealt with by LINET, the general common pitfalls in business continuity management when creating disaster recovery plans and business continuity plans can be outlined, which other companies should watch out for:

1) **Not Running and Testing of the Disaster Recovery Plan and Business Continuity Plan.**

It is recommended to test DRP and BCP, including the functionality of backups, at least once a year. However, if a major change impacts operations such as a pandemic which moves the staff to remote work, the plan should be updated and tested more often to ensure it is effective.

2) **Not Obtaining Executive Level Support at the Start.**

It all starts with executive leadership buy-in and support, especially for creating a business continuity plan. Executive leadership commitment permeates throughout the culture and their support is needed throughout the creation of the plan. Once buy-in is officially obtained, a policy can be defined to reflect the company's posture or stance on their business continuity risk tolerance overall.

3) **Not Learning from the Last Disaster or Interruption or Incorporating Those Learnings Back into the Plan.**

The most important finding from LINET's perspective was that the point of the lessons learned meetings should not be to assign blame or find fault with any person, but rather to focus on the question of why a particular process failed.

4) **Clearly, Defining Roles and Responsibilities Would Boost Efficiency.**

Some employees require specialized training to fully understand the roles and responsibilities across teams and how to reduce chaos during an actual disaster.

5) **Not Having Both IT and Business at the Table to Create the Plans, All Key Stakeholders Should Contribute in a Meaningful Way.**

To guarantee that all important stakeholders make a significant contribution to the creation of comprehensive plans, it is imperative that both IT and business representatives be involved in the planning process for Disaster recovery plans and Business continuity plans.

6) **BCP and DRP Need to be in Physical Hard Copy Form, it is not Sufficient to Have Them Stored Within the Network.**

Physical hard copies of the Disaster recovery plan and Business continuity plan are essential. Digital copies maintained on the network alone may not be sufficient in an emergency, such as a cyberattack or network failure.

7) **Making the BCP and DRP too Large.**

It is essential to make sure that the Disaster recovery plan and Business continuity plan are clear and simple. Plans that are too detailed may cause uncertainty and inefficiency in urgent situations, which will impede quick decision-making and efficient action.

3.3 Implementation of Crisis Management During an Incident

Disclaimer: For LINET's protection, all sections, except section 3.1.1 which describes information about LINET, are based on fictitious data and practices that do not reflect LINET's actual operations. As such, however, they are factually correct.

Realization of a crisis management during the incident is a very complex topic, which takes a deep understanding of various internal company documents and strategies, along with a quality training and preparation to execute well. There are many rules and principles to follow. Below written points are those which would be the most important for LINET after an incident as described in

Key to a good incident response plan is also choosing the right communication channel. Using Teams or instant messenger app is not recommended, especially when the company needs to inform a larger group of people (eg. customers or employees), for example in the case of a company-wide announcement of an incident. For interal communication, using a dedicated Teams channel with specific settings is acceptable. However, for an urgent communication, eg. in the first moments after finding out about the incident, calling the person responsible is the best practice.

3.3.1 Communication During a Crisis

Once the foundations of the house were meticulously laid and its construction carefully planned, the actual building commenced. At this stage of the project, it was crucial to ensure that work on the construction could continue even in the face of unexpected weather conditions. Similarly, in the phase of crisis management when an organization faces unforeseen challenges, the construction team needed to be prepared to effectively respond and adapt their plans to changing conditions.

Preparation for Unexpected Weather Conditions: *Construction plans included strategies for quickly adjusting to changes in weather, such as sudden rains or strong winds. In the same spirit, within crisis management, organizations must develop flexible plans that allow rapid adaptation to technological failures or other crisis situations to ensure the continuation of critical operations.*

Team Coordination Efforts: *As with a construction project, where the team needed to constantly communicate and coordinate their efforts to keep the work efficient and safe, crisis management requires strong coordination among various departments. Regular updates, briefings, and strategic planning are essential for managing a crisis effectively.*

Deployment of Backup Resources: *At the construction site, backup materials and tools were prepared in case the main resources suddenly became unavailable. Similarly, in crisis management, organizations must have backup systems and processes ready to be activated to ensure operational continuity.*

Evaluation and Feedback: *Every day, at the end of work, the team assessed progress and any issues that arose due to unexpected weather conditions. This regular evaluation allowed for quick adjustments and optimization of the next steps. In crisis management, it is equally important to conduct ongoing evaluation of the crisis response, ensuring that feedback is integrated into future actions.*

Using this analogy during the phase of implementing crisis management during an incident provides a clear, understandable model of how an organization can navigate crises with foresight and efficiency, ensuring minimal disruption to its operations. This part of the story sets the stage for further analysis and lessons that can be derived from the crisis, just as it prepares the groundwork for the final stages of the construction project.

(conclusion of house metaphor is on page 100)

One of the most important parts considering dealing with a crisis is good communication. To avoid confusion during an incident, it is crucial to be prepared and to have a plan. Referencing the incident description in the section 3.1.2, we can clearly see what communication mistakes were made, and which could be potentially avoided, had LINET set up their incident response plan in section 3.2.3. better.

Communication during a crisis can be seen as an important factor in determining how extensive the damages will be. In this thesis, details on how to communicate effectively with the public to mitigate damage to the company's reputation, or on how to communicate with customers for the same purpose, will not be covered. Focus will be placed on basic communication principles that should be adhered to within the company.

First, it is important to set up which commincation channels to use before the incident occurs. LINET should ensure there are multiple channels through which the roles responsible can communicate with various employees, stakeholders, or members of a crisis management team before the incident, so nobody panics, and everybody knows hwo to inform and how. Communicate promptly and frequently, especially during the initial stages of a crisis.

One of the steps for setting up a proper communication method should be choosing a right channel. While Microsoft Teams can work very well during a usual workday, they may be disabled during an accident. That is why in the first stages of incident response, it is best practice to rely on mobile phone calls, as they are reliable and easy to follow. Then, a special method for alerting the whole company should be setup, for example a special email (as described in the incident response plan), an SMS message or potentially a dedicated Teams channel.

For those set up channels and incident response plans to work properly, it is necessary to regularly train employees on crisis communication protocols and conduct simulated crisis scenarios to ensure preparedness and readiness to respond effectively in real-time situations. Incident response scenarios should be repeated at least once a year, during a cybersecurity training mandatory for all employees.

3.3.2 Activation of Incident Response Rules

This part of the thesis is dedicated to post-disaster recovery efforts and follows up on the Disaster recovery plan (see Section 3.2.4). At the same time, it smoothly builds on lessons learned.

This stage is sometimes referred to other guidelines as reconstruction, resumption, resettlement, rehabilitation, and a few other similar terms. They all refer to returning to normal operations after a stable state has been reached. After stabilization, it is possible to shift the focus and activity levels until you fully restored normal operations, after which you can begin the important step of performing a lesson learned session to incorporate improvements. In LINET's case, this meant that thanks to the rapid activation of our BCP and DRP plans, it was possible to temporarily move the production of hospital beds to another site that was equipped with the necessary equipment within a short period of time.

To resume, following the cyberattack on LINET manufacturing company's IT infrastructure, the management swiftly activated the crisis management team, conducted a forensic analysis, initiated corrective actions, allocated financial resources to mitigate the incident's impact and supervisory authorities were notified. The incident's impacts however included a complete shutdown of operations for three days, partial operation for two additional days, data encryption, financial losses, reputational damage, and data loss.

The company plans to implement corrective technical and organizational measures, including:

- Implementation of strong passwords and multi-factor authentication.
- Regular software and firmware updates.
- Deployment of VPN access monitoring.
- Implementation of security solutions for detecting and preventing cyber attacks.
- Regular employee training on cyber security.
- Development of a cyber incident response plan.
- Consideration of implementing Zero Trust architecture.
- Regular data backups to offline storage.

Next steps also include evaluating the incident's overall impact, implementing technical and organizational corrective measures, enhancing cyber security measures, and continuously reviewing BIA, RIA, BCP, DRP and supplier contracts. Particularly when it comes to the revision of contracts with suppliers, we have discovered a serious shortcoming during the crisis. As already mentioned, the SLA identified within the production process asset, was assessed in the context of the suppliers' SLAs affecting that asset, and the highest delivery value was found to be in the contract with the supplier for 45 days. This period is unreasonably long; therefore, we must initiate as soon as possible an amendment to the contract with the supplier.

3.3.3. Reporting Obligation Under NIS 2 and Draft of Czech Legislation

In certain circumstances, the company LINET may be required to report the cyber incident to the supervisory authority. This obligation is based on Article 23 of NIS 2, which obliges Member States to ensure that regulated entities could report significant security incidents to the supervisory authority without undue delay. This measure is intended to eliminate the impact and prevent the incident's potential spread.

The term "incident" within the meaning of the NIS 2 Directive is "the event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems" (Article 6, para. 6 of NIS 2). As can be seen from the above, regulated entities are not obliged to report every cyber incident, but only those that qualify as *significant*. According to the NIS 2 Directive, a significant incident is the incident that has either (I.) caused or can cause severe operational disruption of the services or financial loss for the entity concerned or (II.) affected or can affect other natural or legal persons by causing considerable material or non-material damage (Article 23, para. 3 of NIS 2). However, as the Czech National Cyber and Information Security Agency (2024), hereafter referred to as "NCISA", notes, individual Member States have the possibility to specify or set stricter criteria for this obligation in the transposition of the Directive into their national legislation.

This is also the case in the Czech implementation, where the current draft of the new Cybersecurity Act and the draft Decree decree on security measures of a regulated service provider in the regime of higher obligations (mentioned above) stipulate that obliged entities falling under the higher regime must report *all* incidents originating in cyberspace, while at the same time intentional culpability cannot be excluded (Section 16, para. 1 of the draft of Cybersecurity Act).

As ESMA (2024) state that the notification of significant incidents must take place in a "multiple-stage approach". If we assume that LINET falls under the stricter, higher-level

regime, it will be necessary for LINET to report the incident described above directly to the NCISA within 24 hours of discovering the incident (so called "early warning"). This notification should include at least identifying information, basic details of the certain cybersecurity incident, and whether the company believes that the cybersecurity incident was caused by unlawful interference or that it could have a cross-border impact (Article 17, para. 1 of the draft of Cybersecurity Act). Subsequently, the NCISA assesses whether the incident may have a significant impact. If the NCISA declares that the incident is not qualified as an incident with a significant impact, the company does not need to take further steps in the reporting process. This obligation is based on Article 23, para. 4, a) of NIS 2.

If NCISA notifies LINET that an incident may be considered significant, LINET will be required to deliver a second notification to the supervisory authority within 74 hours of the discovery of the incident. So, the clock for both notifications (early warning and second notification) start ticking the moment the respective entity becomes aware of the incident. The second notification should contain - initial assessment of the incident, impact of the incident, indicators of compromise (Article 17, para. 3, a) of the draft of Cybersecurity Act; the transposition of Article 23, para. 4, b) of NIS 2).

Furthermore, the NCISA may request an interim report of significant changes in the status of cyber security incident management (Article 17, para. 3, b) of the draft of Cybersecurity Act; the transposition of Article 23, para. 4, c) of NIS 2). No later than 30 days after notification the company has duty to send the NCISA the final report, which includes a detailed description of the incident, its severity and impact, the type of threat, the probable cause of the incident, mitigation measures taken and underway, and the potential cross-border impact of the incident (Article 17, para. 3), c) of the draft of Cybersecurity Act; the transposition of Article 23, para. 4, d) of NIS 2).

It is also worth mentioning that in the event that LINET would fall into the category of the lower regime under the draft Decree on security measures of a regulated service provider in the regime of lower obligations, it can be assumed that the company will also be obliged to report this incident to the supervisory authority, since according to the scope and severity of the model incident described above, it can be assumed that the incident will be assessed as significant. In such a case, the notification procedure would be virtually identical, except that LINET would not make the notification directly to NCISA, but to the national CERT.

In addition to the surveillance authority, LINET is also obliged under NIS 2 (Article 23(2) NIS 2) to contact recipients of its services who may be affected by a significant cyber threat about any actions or remedies that recipients may take in response to the threat, without undue delay.

If the company does not fulfil the reporting obligation, it can be sanctioned. However, penalties are not directly set out in NIS 2. On the contrary, Article 36 of NIS 2 provides that Member States shall lay down penalties for breaches of the national measures adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. Under the Czech legal system, it is expected that, according to the draft of Cybersecurity Act, the NCISA may impose a fine of up to 250 000 000 CZK (approx. 9 835 990 EUR) on an obliged entity for failure to comply with the reporting obligation (Article 60, para. 1), h) of the draft of Cybersecurity Act) or, in the case of an undertaking pursuant to Articles 101 and 102 TFEU, up to 2% of the net worldwide annual turnover achieved by the undertaking in the immediately preceding financial year (Article 60, para. 15, a) of the draft of Cybersecurity Act).

Schmitz-Berndt (2023, p. 6) also draws attention to the fact that, in addition to the above-mentioned reporting obligation, Article 30 of NIS 2 provides regulated entities opportunity to

voluntarily share information about cybersecurity incidents, cyber threats or other significant issues.

3.4 Lessons Learned

Disclaimer: For LINET's protection, all Sections, except Section 3.1.1, which describes information about LINET, are based on fictitious data and practices that do not reflect LINET's actual operations. As such, however, they are factually correct.

Incident Evaluation and Feedback

The incident that affected LINET is a clear example of how disastrous the consequences of inadequate IT infrastructure security can be. The misuse of a weak password and the absence of multi-factor authentication led to an attacker easily penetrating the company network and causing extensive damage.

One of the main lessons learned from this incident is the need to thoroughly protect gateways such as VPNs with both strong passwords and multi-factor authentication. It is also essential to regularly update software and firmware and implement security solutions to detect and prevent cyber attacks.

Communication and collaboration between different departments of the company is also key. The incident wasn't discovered until Monday morning, meaning that a lack of coordination and outage monitoring over the weekends caused delays in responding to the attack.

Another important lesson is the need for regular employee training in cybersecurity. People are often the first line of defense against cyberattacks and must be able to recognize suspicious activity and report it early.

Implementing a Zero Trust architecture and regularly backing up data to offline storage are also steps that should be considered as part of preventing similar incidents in the future.

Overall, the incident provides a hard lesson on the importance of security measures in a cyber environment and highlights the need for continuous improvement and monitoring of security protocols and procedures. Incident evaluation and feedback are key to assessing the effectiveness of protocols and preparation, which did not occur in this case. Moving on to more specific lessons learned steps.

Several factors are important to consider when evaluating an incident.

1) Was the LINET response quick and effective, both at the individual and team level?
2) How effectively were safety procedures and protocols applied in the situation?
3) Was there cooperation and communication between different parts of the organization and possibly with external entities such as emergency services or the authority?

During such an incident assessment, it is important to include all persons who had a role in the incident response. It is important for the future operation of the company and the handling of future potential incidents how the course of the incident is perceived by the persons involved.

To start with, it is therefore advisable to ask each of them what was done well in the incident and where they see a proctor for improvement. Only after this "round" of interviews is it a good idea to move on to a specific discussion of the incident, through the different phases of the incident to the end.

From the fictitious LINET incident, it can be concluded that many mistakes were made, but that many companies make mistakes in crisis management. The following areas that were done wrong were evaluated in the review (which are summarized in the introduction, here we go more in depth):

- RIA, BIA – these parts did not consider the type of attack, the company focused too much on IT, while neglecting OT, which is the most attacked nowadays because management forgets to protect it
    - BIA: RTO/RPO 30 days, SLA with vendor 45 days.
    - RIA: in PR x PO links – suppliers rated low dependency. Risk framework for supporting asset does not consider all vulnerabilities and threats. There could have been more supporting assets – more detail.
- Not running and testing of the Disaster recovery plan and Business continuity plan
- Not having both IT and business at the table to create the plans, all key stakeholders should contribute in a meaningful way, BCP and DRP need to be in physical hard copy form.
- Making the BCP and DRP too large
- DRP only fot IT systems, it was not considered necessary to develop DRP for part of the Operational technology, because OT systems are managed by the supplier and as such it was assumed that they were also, in terms of disaster recovery plans, only managed by the supplier etc.
- Passwords, passwords, and passwords again and basic rules of cyber security. Repetition is the mother of wisdom and employees are the most important and most critical asset of a company.
- Dysfunctional/non-existent communication matrix:
    - the incident happened at a time when IT was not available nor were processes in place to monitor systems during non-business hours.
    - no one was set up on weekend duty to monitor the systems in question, or at least respond to any alerts.

Conclusion of the Crisis and Recommendations for Future Practice

The crisis was not handled as it should have been if everything had worked as it should. It is important to remember, however, that crises cannot be 100% prepared for and it is important to have people involved in crisis and incident management who can vary the various pre-determined scenarios to take account of the current situation. It is important to have adequate preparation for these cases and to test it regularly.

It is not always necessary to test entire plans - DRP, BCP, although it is always a better option, but if it is not economically viable, it is necessary to test at least individual plans and units that build on each other.

The first steps that need to be taken so that a similar incident does not happen again.

1) Establish the individual tasks that need to be improved based on lessons learned.
2) Assign individual task owners and explain their tasks to them and give a time and financial framework for completing the task.

3) Create a functional team - incident response team and cyber security team/crisis management team.
4) Establish regular and practical cyber security training.
5) Prepare new BIAs during #Table 2.
6) Then review the RIA at the BIA and then reflect the results of the BIA in item #Table 2
7) Redesign the new DRP and BCP to include all important assets relevant to the operation of the company (in the case of DRP, BCP, remember to include any newly purchased components such as HW, SW)
8) Testing the knowledge of employees/externs from training
9) Review supplier contracts, include suppliers in the redesign of DRP, BCP if it makes sense.
10) Testing of new DRP, BCP

4 Conclusion

As the construction of the house reaches completion, the builders, architects, and future homeowners come together to inspect the final structure. This moment of reflection is not only a celebration of the project's completion but also a critical evaluation of the building's resilience against both expected and unexpected challenges. This phase corresponds to the conclusion stage in crisis management, where an organization reflects on the crisis management processes it implemented, learning valuable lessons for future endeavors.

Assessment of the Construction's Success: *The house, now standing firm, is scrutinized for its ability to fulfill the expectations set at the beginning of the project. The quality of materials, the stability of the structure, and the effectiveness of the adaptations made due to unforeseen weather conditions are all evaluated. In crisis management, this step involves reviewing how well the organization handled the crisis, including the effectiveness of the communication, coordination, and decisions made under pressure.*

Learning from the Building Process: *Each stage of the construction provided valuable lessons, from the initial ground-breaking to the final touches. The construction team discusses what strategies worked best, what could be improved, and how to better prepare for future projects. Similarly, in crisis management, a thorough review of the actions taken, the resources utilized, and the overall response effectiveness is crucial for strengthening future crisis preparedness and response strategies.*

Planning for Future Improvements*: Based on the insights gained during the construction and the final evaluation, plans for future building projects are adjusted. These adjustments might involve choosing more resilient materials, refining architectural designs, or enhancing coordination protocols. In the context of crisis management, the organization may revise its crisis management plans, implement new training programs for staff, and invest in better technology to improve response capabilities.*

Strengthening the Foundations for the Future*: The house's resilience is a testament to the soundness of its initial design and the effectiveness of the construction team's response to challenges. For the organization, this resilience reflects the robustness of its crisis management framework and its ability to adapt and evolve. Moving forward, both the builders and the organization are better equipped to handle future challenges, ensuring longevity and stability.*

In conclusion, just as the completed house stands ready to provide shelter and security to its inhabitants, the organization emerges from the crisis more prepared and resilient. This narrative throughout the thesis chapters highlights the critical role of proactive planning, effective response, and continuous learning in both construction and crisis management, providing a relatable and instructive story for readers to understand the importance of Business Impact Analysis and crisis management in practical terms.

Strong cybersecurity safeguards are recognized as vital in today's digital environment, as vividly illustrated by the fictional LINET security incident. This incident serves as a stark reminder of the consequences of inadequate security measures for IT infrastructure. Due to weak passwords and the absence of multi-factor authentication, attackers were able to access LINET's network, causing considerable harm. This underscores the crucial nature of protecting gateways, such as VPNs, using multi-factor authentication and strong passwords.

Synthesis and Main Findings: The research conducted demonstrates significant insights into the integration of the NIS II Directive's cybersecurity requirements into the existing crisis management practices of LINET Group. The proactive crisis management strategies developed are shown to enhance the resilience and sustainability of LINET Group significantly. It was found that systematic and proactive crisis management contributes to a more stable and resilient global economy, reduces environmental impacts, and improves the overall quality of life by minimizing the impacts of crises on society and the environment.

Implications for Theory, Method, and Policy: This thesis contributes theoretically by expanding on the models of crisis management to include cybersecurity aspects explicitly, thereby offering a multidisciplinary approach to crisis resilience. Methodologically, the use of extensive case studies and stakeholder interviews provides a robust framework for analyzing and integrating crisis management strategies with cybersecurity needs, which can be replicated in similar studies. The policy implications are vast, suggesting that organizations, especially in healthcare and other critical sectors, must adopt stringent cybersecurity measures to protect against and mitigate the impacts of digital threats.

Limitations of the Research: The primary limitation of this research is its reliance on a fictional scenario within LINET Group, which may not capture all the complexities of a real-world crisis. Additionally, the research focus was narrowly tailored to the context of LINET Group's operations and may not be generalizable to other sectors or smaller organizations without adaptations.

Need for Further Research: Further research is needed to explore the applicability of these findings in different organizational contexts and across various geographical regions. It would also be beneficial to investigate the long-term effects of integrated crisis management and cybersecurity practices on organizational resilience and recovery capabilities.

Conclusion Enhanced: In conclusion, it is recognized that society can be enriched by this thesis. The findings underscore the need for realistic assessments of capabilities and response times to cyber incidents, including regular simulation and exercises to enable staff to gain the necessary skills and confidence to respond effectively. The security of operational technology (OT) is highlighted as an emerging vector of cyber attacks, suggesting that OT security must not be overlooked and should be integrated into the company's overall cybersecurity strategy.

Recommendations: It is recommended that LINET and similar organizations frequently back up data to offline storage, implement a zero-trust architecture, and ensure continuous monitoring and improvement of security protocols and procedures. By implementing robust security measures and adopting the lessons learned from this research, companies can better protect themselves against the evolving cyber threat landscape, thereby securing their assets, reputation, and stakeholders more effectively.

Literature:

Primary Source

COLE, T. A., VERBINNEN, P. *Collaborative Crisis Management: Prepare, Execute, Recover, Repeat.* Chicago: University of Chicago Press, 2022. ISBN 978- 0226821375.

FOTR, J., SOUČEK, I. *Scénáře pro strategické rozhodování a řízení: Jak se efektivně vyrovnat s budoucími hrozbami a příležitostmi.* Praha: Grada, 2019.240 s. ISBN 9788027120208.

FRASER, J. R. S., QUAIL, R., SIMKINS, B. *Enterprise Risk Management: Today´s Leading Research and Best Practices for Tomorrow´s Executives.* New Jersey: John Wiley & Sons, 2021. 944 p. ISBN 9781119741480.

JAN KOLOUCH, PAVEL BAŠTA ET AL. *Cybersecurity.* p. 68, CZ.NIC, z.s.p.o., 2019 ISBN 8088168317, 9788088168317

JIRÁSEK P., NOVÁK L., POŽÁR J., *Cyber Security Glossary.* Praha 2015 ISBN 978-80-7251-436-6, available online https://www.cybersecurity.cz/data/slovnik_v310.pdf

KASCHNER, H. *Cyber Crisis Management the Practical Handbook on Crisis Management and Crisis Communication*. p. 17-18, and p. 63-74, 2021 2021 ISBN 978-3-658-35488-6. Available online at: https://link.springer.com/content/pdf/10.1007/978-3-658-35489-3.pdf

LAM, J., *Enterprise Risk Management: From Incentives to Controls,* p. 150-185. John Wiley & Sons, Hoboken, 2014 ISBN: 978-1118413616

PŮJČEK M. J., PÁLENÍKOVÁ M. *Risk management and exploitation of opportunities as a tool for improving the management and control of public finances. Brno: Masaryk University, Faculty of Economics and Administration*, 2022, p. 10

WENZEL, M., STANSKE, S., LIEBERMAN, M. B. *Strategic responces to crisis.* Strategic Management Journal, 2020, vol. 42, no 2, p. 1-12.

ZUZÁK, R. & KÖNIGOVÁ, M. *Krizové řízení podniku. 2nd ed.* Praha: Grada, 2009, ISBN 978-80-247-3156-8.

Internet Sources

ABRASHI, G. *Organizational Communication-the Importance of Communication Strategy in Times of Crisis for the Organization*. 2018, available at: https://doi.org/10.26417/ejss.v1i2.p21-25 (Accessed: April 25, 2024).

ALZATARI, A, A, M. AND RAMZANI, R, S. *A Review of Crisis Management Strategy and its Influences on the Organizational Performance*. 2019, available at: https://doi.org/10.17148/iarjset.2019.6314 (Accessed: April 25, 2024).

ALZATARI, A, A, M. AND RAMZANI, R, S. *A Review of Crisis Management Strategy and its Influences on the Organizational Performance.* 2019, available at: https://iarjset.com/wp-content/uploads/2019/04/IARJSET.2019.6314.pdf (Accessed: April 25, 2024).

ANDERSON, P. *Complexity Theory and Organization Science.* 1999, available at: https://www.jstor.org/stable/2640328 (Accessed: April 25, 2024).

ASSURANCELAB. *Best Practices: Risk Management*. 2023, available at https://www.assurancelab.cpa/resources/post/implementing-risk-management (Accessed: April 25, 2024).

BASSIM, M. ET AL. *Evaluating Risk Management Readiness of Organizations towards COVID-19: A Case of the Small-scale Boutique Hotels,* CINEC Academic Journal, 2021 5, p. 85-92. Available at: https://doi.org/10.4038/caj.v5i1.76 (Accessed: April 25, 2024).

BIEDERMANN, M., PAPATHEODOROU, A., PROWLE, M., BULATOVIC, I. *High Reliability Organisations in a Changing World: The Case of Air Traffic Control*, p. 1-2. 2024, available at: https://www.sciencedirect.com/science/article/abs/pii/S2210539524000014 (Accessed: April 25, 2024).

BROOMES, L. *Why Regularly Reviewing and Updating Your Risk Management Plan Is Essential for Project Success.* 2023, available at: https://www.manageprojex.com/continuously-monitoring-and-addressing-risks-regularly-reviewing-and-updating-the-risk-management-plan (Accessed: April 25, 2024).

BUNDY, J. et al. *Crises and Crisis Management: Integration, Interpretation, and Research Development, Journal of Management*, 43(6), p. 1661-1692. 2016, available at: https://doi.org/10.1177/0149206316680030 (Accessed: April 25, 2024).

BCMpedia – Business Continuity Management Institute. *Crisis Management. A Wiki Glossary for Business Continuity Management (BCM) and Disaster Recovery (DR).* 2020, available at: https://bcmpedia.org (Accessed: April 25, 2024).

CANTU, J., TOLK, J., FRITTS, S., GHAREHYAKHEH, A. *High Reliability Organization (HRO) systematic literature review: Discovery of culture as a foundational hallmark*. 2020, available at: https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-5973.12293 (Accessed: April 25, 2024).

COOMBS, T, W. *The value of communication during a crisis: Insights from strategic communication research.* 2015, available at: https://www.sciencedirect.com/science/article/pii/S0007681314001505 (Accessed: April 25, 2024).

Crisis Management. *Meaning, Need and its Features*. 2022, available at: https://www.managementstudyguide.com/crisis-management.htm (Accessed: April 25, 2024).

Crisis Management. *What is Crisis Management?* 2014, available at: https://www.tutorialspoint.com/management_concepts/crisis_management.htm (Accessed: April 25, 2024).

CYBRELA *NIS II.* 2024, available at: https://cybrela.com/en/nis2/ (Accessed: April 25, 2024).

DEY, M. *Business continuity planning (BCP) methodology – essential for every business*. 2011. Available at: https://ieeexplore.ieee.org/abstract/document/5752503 (Accessed: April 25, 2024).

ELZAANIN, A., AHADIAT, A. AND JIMAD, H. *Linking Crisis and Emergency Management In Strategic Management Process Of Ngos In Gaza Strip*. 2020, available at: https://doi.org/10.23960/ijebe.v3i2.85 (Accessed: April 25, 2024).

EVRIN V. *Risk Assessment and Analysis Methods: Qualitative and Quantitative*. 2021, available at: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods (Accessed: April 25, 2024).

FARREL, D., GEBRE, B. HUDSPETH, C. AND SELLGREN, A. *Risk-based resources allocation: Focusing regulatory and enforcement efforts where they are needed the most*., p. 18 2013, available at: https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/Public%20Sector/PDFS/MCG_Risk-based%20resource%20allocation-WEB (Accessed: April 25, 2024).

FLINDERS, M. *Business continuity vs. disaster recovery: Which plan is right for you?* 2024, available at: https://www.ibm.com/blog/business-continuity-vs-disaster-recovery-plan/ (Accessed: April 25, 2024).

POROT G. *What are the Three Stages of Crisis Management?* 2024, available at: https://www.internationalsos.com/magazine/what-are-the-three-stages-of-crisis-management (Accessed: April 25, 2024).

HENDARYATNA, H., FIRMANSYAH, G., TJAHYONO, B., WIDODO, A. M. *Performance Evaluation of Business Continuity Plan in Dealing with Threats and Risks in Cilegon Companies Use ISO 22301:2019 & NIST Sp 800-30 R1 Frameworks Case Study*, 2023, p. 1159 at https://www.researchgate.net/publication/374254103_Performance_Evaluation_of_Business_Continuity_Plan_in_Dealing_with_Threats_and_Risks_in_Cilegon_Companies_Use_ISO_223012019_NIST_Sp_800-30_R1_Frameworks_Case_Study_PT_X (Accessed: April 25, 2024).

HEATH, W, R. *Dealing with the complete crisis—the crisis management shell structure.* 1998, available at: https://doi.org/10.1016/s0925-7535(98)00042-3, 24.4.2024 (Accessed: April 25, 2024).

HILES, A. *Servis level agreements and business continuity*., p. 1-9. 2023, available at: https://www.continuitycentral.com/SLAsBCM.pdf (Accessed: April 25, 2024).

ICOR ISO 22320:2018 *Security and resilience, Emergency management, Guidelines for incident management Resilience framework*. 2024, available at: https://www.build-resilience.org/organizational-resilience-framework.php (Accessed: April 25, 2024).

INSTITUTE, F, C. *Crisis Management – Definition, Types, Plan and Steps*. 2020, available at: https://corporatefinanceinstitute.com/resources/management/crisis-management/ (Accessed: April 25, 2024).

ISO *Security and resilience, Emergency management, Guidelines for incident management*. 2024, available at: https://www.iso.org/standard/67851.html (Accessed: April 25, 2024).

JENKINS, R. *Critical assets for business continuity and risk management*. City Security Magazine. 2018, available at: https://citysecuritymagazine.com/risk-management/business-continuity-critical-a (Accessed: April 25, 2024).

MANLEY B., MCINTIRE D. *A Guide to Effective Incident Management Communications*. 2021, available at: https://insights.sei.cmu.edu/documents/1631/2021_002_001_651819.pdf (Accessed: April 25, 2024).

MOH HENG GOH. *Crisis Management Series – Roles and Responsibilities of Communication Coordinator.* BCM Institute, 2024, available at: https://blog.bcm-institute.org/crisis-management/roles-and-responsibilities-of-communication-coordinator (Accessed: April 25, 2024).

LEMONAKIS, C. AND ZAIRIS, A. *Crisis Management and the Public Sector: Key Trends and Perspectives.* IntechOpen eBooks, 2020, available at: https://doi.org/10.5772/intechopen.90855 (Accessed: April 25, 2024).

LEMONAKIS, C. AND ZAIRIS, A. *Crisis Management and the Public Sector: Key Trends and Perspectives.* 2020, available at: https://www.intechopen.com/citation-pdf-url/70824 (Accessed: April 25, 2024).

MEHR, K, M. AND JAHANIAN, R. *Crisis Management and Its Process in Organization*. 2016, available at: https://doi.org/10.5901/mjss.2016.v7n51p143 (Accessed: April 25, 2024).

MILLS, D. *Preparing for a BIA – Understanding RTO and RPO*. 2023, available at: https://www.compassitc.com/blog/preparing-for-a-bia-understanding-rto-and-rpo (Accessed: April 25, 2024).

MUDALAL, W, M. *Integrating Crisis Management into the Strategic Planning Process in the Service Sector Firms*. 2021, available at: https://doi.org/10.6007/ijarbss/v11-i11/11607 (Accessed: April 25, 2024).

MPSV, *Koncepce managementu rizik*, 2024, available at: https://www.mpsv.cz/documents/20142/372813/Koncepce_managementu_rizik_v2%20(1).pdf/d0b28029-ee4c-2ccc-9c00-79197dff5c88 (Accessed: April 25, 2024).

MVČR. *Riziko.* 2024, available at https://www.mvcr.cz/clanek/riziko.aspx#:~:text=Možnost%2C%20že%20s%20určitou%20pravděpodobností,a%20odvozené%20z%20konkrétní%20hrozby (Accessed: April 25, 2024).

Ministry of Foreign Affairs. *Security Strategy of the Czech Republic*. 2003, available at: https://www.databaze-strategie.cz/cz/mzv/strategie/bezpecnostni-strategie-ceske-republiky?typ=download (Accessed: April 25, 2024).

NIS II, *The NIS 2 Directive, Final Text. Article 21, Cybersecurity risk-management measures*. 2022, available at: https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html (Accessed: April 25, 2024).

NIST CSRC Computer Security Resource Center. *Guide for Conducting Risk Assessments. Joint Task Force Transformation Initiative SP 800-30* Rev. 1. 2012, available at: https://csrc.nist.gov/pubs/sp/800/30/r1/final (Accessed: April 25, 2024).

NUKIB, *Supporting materials*. 2024 available at https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/ (Accessed: April 25, 2024).

ESMA European Securities and Markets Authority, *Final report on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554*, 2024, available at: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_83_-_Final_Report_on_draft_RTS_on_classification_of_major_incidents_and_significant_cyber_threats.pdf#:~:text=URL%3A%20https%3A%2F%2Fwww.esma.europa.eu%2Fsites%2Fdefault%2Ffiles%2F2024 (Accessed: April 25, 2024).

ODok Portal. *Návrh zákona o kybernetické bezpečnosti*. 2024, available at: https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/ (Accessed: April 25, 2024).

PECB, *A Comprehensive Guide: Understanding the NIS 2 Directive*, 2023, available at: https://pecb.com/article/a-comprehensive-guide-understanding-the-nis-2-directive (Accessed: April 25, 2024).

PUZDER D., *Vulnerabilities, Threats, and Risks Explained.* 2023, available at: https://informationsecurity.wustl.edu/vulnerabilities-threats-and-risks-explained/ (Accessed: April 25, 2024).

PWC: *Crisis strategy and scenario planning*. 2023, available at: https://www.pwc.com/gx/en/issues/crisis-solutions/crisis-strategy-scenario-planning.html (Accessed: April 25, 2024).

QUINN, S., IVY, N., CHUA, J. (EDS.), *Using Business Impact Analysis to Inform Risk Prioritization and Response.* p. 3-4, p 10-12, 2022, available at https://www.nist.gov/publications/using-business-impact-analysis-inform-risk-prioritization-and-response (Accessed: April 25, 2024).

SAWALHA, I. H. *Views on business continuity and disaster recovery*. 2021, available at: https://www.emerald.com/insight/content/doi/10.1108/IJES-12-2020-0074/full/html (Accessed: April 25, 2024).

SAPRIEL, C. *Effective crisis management: Tools and best practice for the new millennium*. 2016, available at: https://www.emerald.com/insight/content/doi/10.1108/13632540310807485/full/html (Accessed: April 25, 2024).

SCHERER, C. W., CHO, H. *A Social Network Contagion Theory of Risk Perception.* 2003, available at: https://onlinelibrary.wiley.com/doi/epdf/10.1111/1539-6924.00306 (Accessed: April 25, 2024).

SCHMITZ-BERNDT *Defining the Reporting Threshold for a Cybersecurity Incident under the NIS Directive and the NIS 2 Directive*, Journal of Cybersecurity, 9(1), p. 6. Available at: https://doi.org/10.1093/cybsec/tyad009 (Accessed: April 25, 2024).

TANEJA, S., PRYOR, G, M. AND ZHANG, L. *Crisis management: a strategic and tactical leadership imperative for organizational sustainability, International Journal of Sustainable Strategic Management*, 2(1), p. 60-60. 2010, available at: https://doi.org/10.1504/ijssm.2010.032164 (Accessed: April 25, 2024).

TANEJA, S., PRYOR, G, M. AND ZHANG, L. *Crisis management: a strategic and tactical leadership imperative for organizational sustainability.* 2010, available at: https://doi.org/10.1504/ijssm.2010.032164 (Accessed: April 25, 2024).

TAYLLORCOX. *Risk Management*. 2024, available at https://www.tx.cz/slovnik/isms/rizeni-rizik (Accessed: April 25, 2024).

TAYLLORCOX. *Risk*. 2024, available at https://www.tx.cz/slovnik/itil/riziko (Accessed: April 25, 2024).

TAYLLORCOX. *Threat*. 2024, available at https://www.tx.cz/slovnik/pci-dss/hrozba (Accessed: April 25, 2024).

TAYLLORCOX. *Vulnerability*. 2024, available at https://www.tx.cz/slovnik/itil/zranitelnost (Accessed: April 25, 2024).

TAYLLORCOX. *Risk Analysis*. 2024, available at https://www.tx.cz/slovnik/isms/analyza-rizik (Accessed: April 25, 2024).

UIC *Additional Global Security Programme*, p. 53-60; *Recommendations for Crisis Management,* p. 18. 2017, available at: https://uic.org/IMG/pdf/crisis_management_report.pdf (Accessed: April 25, 2024).

VAŠÍČKOVÁ V. *Crisis Management Process: A literature review and a conceptual integration.* p. 61-63, 2019, available at https://aop.vse.cz/pdfs/aop/2019/03/05.pdf (Accessed: April 25, 2024).

VANDEZANDE, N. *Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor,* p. 4. 2024, available at: https://www.sciencedirect.com/science/article/pii/S0267364923001000 (Accessed: April 25, 2024).

VARDARLIER, *P. Strategic Approach to Human Resources Management During Crisis*, p. 464-469. 2016, available at: https://www.sciencedirect.com/science/article/pii/S1877042816315919 (Accessed: April 25, 2024).

WEBER, K., GLYNN, M. A. *Making Sense with Institutions: Context, Thought and Action in Karl Weick's Theory,* pp. 1639-1660. 2006, available at https://journals.sagepub.com/doi/10.1177/0170840606068343 (Accessed: April 25, 2024).

WARD, S. *Approaches to Integrated Risk Management: A Multi-dimensional Framework.* 2003, available at: https://link.springer.com/article/10.1057/palgrave.rm.8240161 (Accessed: April 25, 2024).

WATSON, J. *Application of the Plan-Do-Check-Act (PDCA) cycle for standardized nursing management*. 2022, available at: https://www.alliedacademies.org/articles/application-of-the-plandocheckact-pdca-cycle-for-standardized-nursing-management.pdf (Accessed: April 25, 2024).

ZAPLETALOVA *Š., Rozložení rizika – Risk management*. 2020, available at: https://is.slu.cz/el/opf/zima2020/PEMNPKRI/2209991/KM_PS_20-21_8._prednaska.pdf (Accessed: April 25, 2024).

Topic Addressed

VŠEM

introduction

This thesis integrates the NIS II Directive into LINET Group's crisis management protocols to enhance cyber resilience and ensure continuous operations in healthcare, using a multidisciplinary methodology to improve regulatory compliance and crisis preparedness.

problem

The main problem this thesis addresses is the inadequate integration of NIS II Directive cybersecurity mandates into LINET Group's crisis management, potentially compromising response to cyber threats in healthcare.

approach

The approach uses detailed analysis, stakeholder interviews, and risk assessments to integrate NIS II Directive requirements into LINET Group's crisis management, enhancing cybersecurity resilience.

Solution Approach

source

Legislative documents were reviewed, stakeholder interviews were conducted, and scenario planning exercises were utilized as the basis for integrating cybersecurity measures into the crisis management frameworks.

obtaining

Data were collected through legislative document reviews, stakeholder interviews, and scenario planning exercises. This facilitated the integration of cybersecurity measures into the existing crisis management frameworks.

processing

A multidisciplinary approach was employed, featuring legislative analysis, stakeholder interviews, and scenario planning. This effectively integrated NIS II Directive cybersecurity requirements into existing protocols, enhancing organizational resilience to cyber threats.

Work results

The study demonstrated that the comprehensive methodology employed effectively enhanced LINET Group's resilience and compliance with the NIS II Directive.

→It can be predicted that systematic and proactive crisis management practices will significantly strengthen organizational resilience, mitigate the impacts of crises on society and the environment, and contribute to sustainable global development and well-being

→**Facts can be gleaned from the data:**

→The development indicates that the integration of the NIS II Directive into crisis management practices has significantly enhanced both cybersecurity and operational resilience within LINET Group.

→In the future, it is expected that the continuous updating and testing of cyber incident response plans, along with regular independent cybersecurity audits, will further strengthen the firm’s defense mechanisms against evolving cyber threats.

Recommendation

Based on the results, it can be recommended that strong security policies be established, a cyber incident response plan be created and regularly tested, and improvements in communication during crises be implemented.

1. From the integration of the NIS II Directive's cybersecurity requirements into the existing crisis management practices, it will be profited by the company by more secure and stable operational environment.

2. By focusing on cybersecurity and crisis management integration, compliance with regulatory standards and enhanced operational resilience will be brought.

3. From an economic perspective, significant enhancement in regulatory compliance and operational continuity is meant.

Conclusion

The work brought a very deep insight and understanding of the given topic

The new solution is a comprehensive overview, applicable to a wide range of subjects

The issue was shifted thanks to consultations with doc. Enzo Essenza, D.Phil., M.P.A


VŠEM
VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU
DĚKUJI ZA POZORNOST