INSTITUTO POLITÉCNICO
DE VIANA DO CASTELO

ESTG

An Utility Function for assessing the cost of recovering from ransomware attacks

Luís Filipe dos Santos Pinto

An Utility Function for assessing the cost of recovering from ransomware attacks

Luís Filipe dos Santos Pinto

2024

Escola Superior de Tecnologia e Gestão

Instituto Politécnico
de Viana do Castelo

A Utility Function for assessing the cost of recovering from ransomware attacks

Autor(a)

Luís Filipe dos Santos Pinto

Trabalho orientado por

Prof. Pedro Filipe Cruz Pinto

Prof. António Alberto dos Santos Pinto

Mestrado em Cibersegurança

13 de Março de 2025

Mestrado em Cibersegurança
Master in Cybersecurity

A Utility Function for Assessing the Cost of Recovering from Ransomware Attacks

a master's thesis authored by

Luís Filipe dos Santos Pinto

and supervised by

Pedro Filipe Cruz Pinto
Professor Adjunto, ISEP/IPP

António Alberto dos Santos Pinto
Professor Coordenador, ESTG/IPP

This thesis was submitted in partial fulfilment of the requirements for the Master's degree in Cybersecurity at the Instituto Politécnico de Viana do Castelo

ipvc

13 March, 2023

Abstract

Ransomware is a type of malicious software that encrypts an organization's data, rendering it inaccessible unless a ransom is paid. The ransom is typically demanded in cryptocurrency. This digital extortion has proven to be highly lucrative for cybercriminals and devastating for organizations. The increasing prevalence of these attacks highlights the need for alternative methods to assess and manage recovery costs effectively.

Existing methods to assess the financial impact of ransomware are often inadequate because they focus on indirect costs such as operational downtime and reputational damage and do not take into account the time needed for recovery.

This thesis introduces a novel utility function designed to quantify the costs associated with recovering from ransomware attacks in terms of the time needed for recovery, as an aspect overlooked by the existing solutions. The proposed utility function provides a structured method to estimate recovery times based on the duration of each recovery activity. By quantifying these times, the function allows for organizations to make informed decisions about resource allocation and enhance their preparedness against potential ransomware attacks.

Keywords: ransomware, recovery time, estimation, utility function.

Resumo

O ransomware é um tipo de *software* malicioso que encripta os dados de uma organização, tornando-os inacessíveis a menos que seja pago um resgate. O resgate é normalmente exigido em criptomoeda. Esta extorsão digital provou ser altamente lucrativa para os cibercriminosos e devastadora para as organizações. A crescente prevalência destes ataques realça a necessidade de métodos alternativos para avaliar e gerir eficazmente os custos de recuperação.

Os métodos existentes para avaliar o impacto financeiro do ransomware são muitas vezes inadequados porque se concentram em custos indiretos, como tempo de inatividade e danos à reputação, e não consideram o tempo necessário para a recuperação.

Esta tese introduz uma nova função utilidade projetada para quantificar os custos associados à recuperação de ataques de ransomware em termos da necessidade de tempo para recuperação, um aspeto negligenciado pelas soluções existentes. A função utilidade proposta fornece um método estruturado para estimar os tempos de recuperação com base na duração de cada atividade de recuperação. Ao quantificar esses tempos, a função permite que as organizações tomem decisões informadas sobre a alocação de recursos e melhorem a sua preparação contra possíveis ataques de ransomware.

Palavras-chave: ransomware, tempo de recuperação, estimativa, função utilidade.

Aknowledgements

First, I would like to thank Prof. Pedro Pinto and Prof. António Pinto for having the patience and courage to accompany me through all this journey without giving up. I know it was not an easy challenge. Your persistence, guidance and wisdom was always very welcomed and the main reason this thesis is completed.

I would like to thank IPVC - Instituto Politécnico de Viana do Castelo, for creating the conditions for this master's degree to be possible.

I would like to thank all my colleagues who, directly or indirectly, contributed to making this thesis a reality, my sincere and profound gratitude. This work is also a reflection of the help, understanding, and encouragement I received throughout this academic journey.

I would like to thank all my close friends, and family members who, with words of support, suggestions, or simply by their presence, made this journey lighter and less lonely.

I would like to thank my reason for living, for her love, patience, and understanding throughout this entire process. Her presence by my side, both in moments of joy and in more challenging times, was essential for me to move forward and complete this journey. Her constant support and daily encouragement were crucial for me not to give up, even when the obstacles seemed insurmountable.

Finally, I would like to specially thank and dedicate this thesis to my daughters and son, whose affection and joy gave me the necessary motivation to continue fighting for my dreams. Even without understanding the scope of the work I was undertaking, they were an inexhaustible source of inspiration and happiness, allowing me to face each day with renewed energy.

Contents

List of Figures

List of Tables

List of Abbreviations

AD Attack Detection

AF Application Functional Tests

AI Artificial Intelligence

AV Aditional Variables

CASBs Cloud Access Security Brokers

CC Crisis Management and Comunication Measures Time

CE Contention and Eradication

CI Contention Implementation

CM Communication Plan Preparation

CP Contention Points Identification

CS Cloud Service

CV Cloud Service / Virtual Computer Recovery

DA Damage Assessment

DBMS Database Management System

DC Direct Costs

DI Detection and Initial Analysis

DR Disaster Recovery

DV Data Validation

EC External Communication

EDR Endpoint Detection and Response

EE Eradication Execution

EP Eradication Planning

ePHI Electronic Protected Health Information

GDPR General Data Protection Regulation

HIPAA Health Insurance Portability and Accountability Act

IC Internal Communication

II Improvements Implementation

IoT Internet of Things

IP Security Improvements Planning

IR Initial Response

IT Information and Technology

MA Communication Adjustments and Monitorization

MC Crisis Management Coordination

MD Mobile Device Recovery

ML Machine Learning

MS Mitigation and Security Improvements

NA Number of Assets

NE Network Equipment Recovery

NGFWs Next-Generation Firewalls

NS Number of Servers

NW Number of Workstations

PA Preliminary Analysis

PR Printer Recovery

RC Root Cause Analysis

RM Response Team Mobilization

RSSD Ransom-aware Solid State Drives

RT Recovery Time

SA Server and Enterprise Apps or Server and DBMS or Server and Email or Server and Backup Recovery

SE Security Appliance Recovery

SI Server Integrity Tests

ST Storage Appliance Recovery

TR Training

TV Test and Validation Time

VM Virtual Machine

WA Workstation and Apps Recovery

WI Computer Security Verification

Chapter 1

Introduction

When considering cybersecurity threats, ransomware attacks have emerged as a great challenge confronting organizations across the globe [6]. These attacks perform unauthorized data encryption, demand payment in exchange for the decryption keys [22], and commonly have relevant operational, financial, or reputational impacts [4]. Beyond the immediate impact to an entity blocked from accessing its information, the full impact analysis must include the recovery effort, the financial loss due to downtime, and potential legal liabilities [17]. The complexity and frequency of ransomware incidents have underscored the urgent need for sophisticated risk management strategies and recovery planning.

The global impact of ransomware is staggering. Ransomware attacks have increased in frequency and sophistication over the past few years [15]. The annual "Cost of a Data Breach Report" by IBM found that the costs associated with ransomware have reached unprecedented levels, often totaling millions of dollars per incident. These costs are not merely the ransoms paid but also include lost productivity, legal fees, the cost of mitigating the breach, and more long-term costs associated with brand damage and lost customers.

Furthermore, the World Economic Forum has identified cyberattacks, including ransomware, as one of the top five risks to global stability. The threat of ransomware is a concern for private enterprises and public institutions, healthcare facilities, and critical infrastructure. For example, recent attacks on healthcare systems during the COVID-19 pandemic have underscored the vulnerability of essential services to these cyber threats.

The economic repercussions of ransomware extend beyond the immediate financial impact of the ransom demands. Organizations often face extensive operational downtime

while they work to decrypt data and restore systems, leading to significant productivity losses. The recovery process can be prolonged and complex, especially when backups are either unavailable or also compromised, which is increasingly common as ransomware attacks become more sophisticated.

The direct costs associated with managing a ransomware incident include hiring external cybersecurity experts, purchasing new hardware, and acquiring software tools needed for forensic analysis and system restoration. Indirect costs can be even more substantial. They involve business disruption, reputational damage, and lost opportunities during the downtime. Moreover, organizations may face regulatory fines and litigation costs if the ransomware breach involves sensitive customer data, adding layers of financial liability.

The significance of understanding the economic impact of ransomware attacks cannot be overstated. It informs strategic decisions about investments in cybersecurity technologies and services. Organizations that accurately assess the potential costs and impacts of ransomware attacks can allocate resources more effectively, prioritize security initiatives, and develop comprehensive business continuity plans that minimize financial and operational disruptions.

Through an evaluation of ransomware recovery times, this thesis proposes a utility function for enhancing organizational preparation and mitigating the impacts of cyber-attacks. By assessing the average duration of each factor and evaluating their relative contributions to the ransomware recovery process, this work aims to develop a formula to better estimate the total recovery time for a ransomware attack. With the proposed approach, by using data that is directly related to the time needed to recover from these cyber attacks, such a utility function will be capable of helping organizations assess the importance of preemptive measures to minimize the time needed for recovery.

The following sections present the problem statement and motivation, the objectives, the contributions of this work, and the organization of this document.

1.1 Problem Statement and Motivation

In the realm of cybersecurity, ransomware has swiftly escalated from a potential threat to a prevalent and devastating reality for organizations globally. Despite extensive security

measures, the rapid evolution of ransomware tactics has outpaced many existing defenses, leaving even well-prepared organizations vulnerable to attacks. The core of the problem lies not only in the frequency and sophistication of these attacks but also in the inadequate predictive tools available to estimate the economic impact and recovery costs associated with them.

Current approaches to managing ransomware risks are often reactive rather than proactive. Many organizations find themselves unprepared for the aftermath of an attack, struggling with decisions about whether to pay ransoms, how to recover lost data without significant downtime, and how to prevent future incidents. The financial models and tools currently available are insufficient for several reasons:

- Existing models often fail to capture the full spectrum of direct and indirect costs associated with ransomware attacks, such as lost business opportunities, long-term reputational damage, and the psychological impact on employees and stakeholders.
- Many risk management plans are based on outdated threat models that do not account for the modern tactics used by ransomware criminals, such as double extortion schemes and the targeting of backups.
- Data on ransomware incidents is often siloed within individual organizations, leading to a lack of shared knowledge that could be used to develop more effective recovery strategies.

These gaps in knowledge and tools limit the ability of organizations to plan effectively for ransomware incidents, resulting in increased vulnerabilities and potentially catastrophic financial impacts.

The motivation for this research stems from the need to enhance organizational resilience against ransomware attacks by developing a utility function capable of accurately estimating recovery costs and economic impacts. This tool aims to transform ransomware risk management from a reactive to a proactive discipline, enabling organizations to anticipate potential losses and effectively allocate resources for prevention and recovery.

1.2 Objectives

This work addresses a gap in cybersecurity risk management: a utility function to estimate the cost of recovering from a ransomware attack using the time needed for the recovery. The development of such a function represents a new approach in this field. This function aims to quantify the manpower necessary for effective recovery from ransomware incidents, thus allowing organizations to better understand the time associated with ransomware attacks. By quantifying the time and resources required for recovery, this tool aims to be a representation of reality.

The objective of this thesis is to present the ransomware recovery utility function and detail the formulation and application of the utility function, by providing a dive into the utility function's development, fine-tuning, and application. This involves a review of the mathematical constructs that form its base, and an analysis of the assumptions underlying the model, such as the linearity of certain costs or the independence of specific recovery activities. Each variable integrated into the utility function is described, including its significance.

Moreover, this section explores the data sources that were instrumental in formulating the utility function. It details the process of data collection, including the challenges encountered in gathering accurate and representative data.

Exploring the practical applications of the utility function in use-case scenarios is another objective of this thesis. This involves case studies where the utility function is applied to estimate the time needed to recover from ransomware in different types of organizations. Each case study is chosen to illustrate how various factors, such as the size of the organization, and the type of equipment that exists, can influence the outputs of the utility function.

1.3 Contributions

This thesis makes several contributions to the field of cybersecurity, particularly in the domain of ransomware recovery and recovery time assessment. By developing a utility function and providing a tool that allows for the calculation of ransomware recovery times, the research contributes to the understanding of ransomware impacts and recovery pro-

cesses. The discussion below elaborates on the specific contributions made by this thesis, highlighting their significance and potential applications.

1. Development of a Utility Function for Estimating Ransomware Recovery Times. The main contribution in this thesis is the development of a utility function designed to estimate the time associated with recovering from ransomware attacks. This function is a different approach from existing models because it incorporates time as the main factor for calculation and is adaptable to various organizational contexts. Unlike traditional models that often focus solely on direct and indirect costs such as ransom payments, reputational damage, legal consequences, and immediate IT remediation, this utility function integrates real calculated recovery times. It is also designed with the flexibility to be applied to organizations of varying sizes and industries.

2. Validation of Restored Systems in Ransomware Recovery. Another contribution of this thesis is the fact that the function takes into account the time needed for the validation process for restored systems following a ransomware attack. This process is crucial for ensuring that systems are not only operational post-recovery but also secure from future attacks. The mention of validation needs that include hardware, software, network, and data integrity checks ensures that all aspects of an organization's IT infrastructure are evaluated after a ransomware incident.

The utility function to be developed is expected to become a practical tool for organizations to understand ransomware impacts. Collectively, these contributions not only advance academic knowledge but also offer benefits in the field of cybersecurity. Future research can build upon these foundations, exploring additional cost factors, refining validation processes, and further integrating theoretical and practical insights.

1.4 Publications

The work carried out herein enabled the author to achieve the following list of peer-reviewed published works:

- "On the Path to Develop a Recovery Cost-Utility Function for Ransomware At-

tack", Symposium of Applied Science for Young Researchers (SASYR), 3 July 2024, Bragança Portugal

- "Utility function for assessing the cost of recovering from ransomware attacks", 4th International Conference on Optimization, Learning Algorithms and Applications (OL2A), 24-25 July 2024, Tenerife Spain

1.5 Organization

This thesis is organized in the following chapters. Chapter 2 reviews existing literature relevant to ransomware attacks and recovery strategies. Chapter 3 describes the methodologies employed in developing and refining the ransomware recovery utility function. It details the data collection process, including the sources of the data and the criteria for data selection. Chapter 4 analyses the ransomware recovery utility function. It examines the mathematical structure of the function, discussing how it was constructed and the assumptions upon which it is based. Following the analysis, Chapter 5 presents the results obtained from applying the utility function to different data sets and scenarios, and presents a discussion on them. Finally, Chapter 6 summarizes the key insights gained from the research, highlighting the contributions of the thesis to the field of cybersecurity.

Chapter 2

Related Work

The development of a utility function for estimating the recovery time of ransomware attacks is a new field of study within cybersecurity. The proliferation of ransomware attacks and the subsequent need for effective recovery strategies have allowed for some literature, dedicated to the economic quantification of these incidents, to arise. Often, the cost of recovery exceeds the initial ransom demand [23] and some efforts in this domain aim to create a utility function that assists in forecasting the financial aftermath of ransomware attacks on organizations.

The sources mentioned in this chapter have been chosen based on their relevance, actuality, and contribution to the field of cybersecurity. Priority has been given to studies published in the last ten years to ensure they reflect the most recent developments in ransomware attack tactics and defensive mechanisms. However, other important works and foundational texts are also included to provide historical context and depth to the analysis.

Researchers such as [11] provide a critical analysis using the Global Cost of Cyber Risk Calculator, forecasting potential costs in Lithuania, Latvia, and Estonia, and proposing that sectors like public business and defense are at heightened risk.

2.1 Historical Overview of Ransomware Attacks

The ransomware phenomenon represents one of the most significant cybersecurity threats modern organizations face [18]. This section traces the historical development

of ransomware, highlighting key changes in attack methodologies, technological advancements, and the shifting landscape of cyber threats.

Ransomware attacks, which encrypt the victim's data and demand payment for decryption, have evolved significantly since their inception. The concept of ransomware is not new; the first known incidence of ransomware was the AIDS Trojan in 1989 [20]. It spread through floppy disks and involved a relatively primitive form of file locking. However, the real proliferation of ransomware began in the mid-2000s with the advent of cryptocurrencies, which provided a secure and anonymous method for attackers to receive payments.

Early forms of ransomware often merely locked the user out of their system or displayed threatening messages to coerce payment. However, as security measures improved, ransomware attacks became more sophisticated. By the 2010s, ransomware like CryptoLocker had begun using robust encryption methods that made it infeasible to recover files without the decryption key, which significantly shifted the dynamics of cybersecurity defense [28].

The escalation of ransomware attacks is closely tied to technological advancements. The development of Bitcoin and other cryptocurrencies in the early 2010s, as outlined by [28], has been crucial because it allows attackers to receive payments anonymously, reducing the risk of apprehension [28]. Additionally, the proliferation of high-speed internet globally has facilitated the rapid spread of ransomware across geographic boundaries.

Encryption technology has also advanced, with ransomware increasingly using sophisticated algorithms to lock data. Techniques such as asymmetric encryption, where the decryption key is different from the encryption key and kept private by the attacker, have made it challenging to recover data without giving up to ransom demands. This shift has required new approaches in cybersecurity, focusing more on prevention and robust backup solutions.

As detailed in the studies from [7], ransomware attacks have seen a dramatic rise in frequency and impact over recent years. The average cost of recovery from a ransomware attack has more than doubled, indicating not only the increasing severity of attacks but also the greater value of the data being targeted. Organizations of all sizes have been affected, from small businesses to large governmental agencies, each facing substantial

financial losses, operational disruptions, and damage to reputation. The increasing digitalization in businesses has also expanded the attack surface for ransomware. With more critical data being stored digitally without adequate backup or security measures, the potential impacts of ransomware attacks have magnified. The interconnectivity of modern business systems, while increasing efficiency, also poses risks of widespread damage from a single ransomware infiltration.

Different sectors have demonstrated varying levels of vulnerability to ransomware attacks, largely influenced by their cybersecurity preparedness and the nature of the data they handle [16]. The healthcare sector, for example, has been particularly targeted, as highlighted in multiple studies [9, 1]. The urgent need for access to patient records and the lifesaving nature of medical services make healthcare institutions more likely to pay ransoms, making them attractive targets for ransomware attacks. Nevertheless, recent advances in blockchain technology offer new approaches to ensuring data integrity, especially in IoT applications, as discussed by [9]. Additionally, [1] explores layered security frameworks to mitigate ransomware in the healthcare sector.

Organizations with robust IT infrastructure and advanced cybersecurity measures, such as in financial services, have been better equipped to defend against ransomware. However, no sector remains entirely immune, and the evolving tactics of ransomware attackers continue to pose a significant challenge across all areas of industry.

The evolution of ransomware has required a parallel evolution in mitigation and recovery strategies. Traditional cybersecurity measures such as firewalls and antivirus software have proved inadequate against sophisticated ransomware attacks [14]. This has led to an increased emphasis on cybersecurity awareness, employee training, and the implementation of more sophisticated cybersecurity measures, such as network segmentation and real-time intrusion detection systems.

Backup strategies have also evolved. The emphasis has shifted from merely backing up data to ensuring these backups are secure, regularly updated, and segregated from the main network. This ensures that they remain untouched in the event of a ransomware attack, allowing organizations to restore data without paying the ransom.

2.2 The Economic Impact of Ransomware

Sophos research indicates [23] that the cost of ransomware attacks has been steadily increasing over the years. The average total cost of remediation from a ransomware attack more than doubled between 2019 and 2020, going from $761,106 to $1.85 million. Interestingly, the average ransom paid was comparatively much lower, at just $170,404 in 2020. The high cost of recovery is attributed to the complexity of advanced ransomware attacks, which combine automation with hands-on human hacking. These complex attacks require more complex recovery processes, contributing to an overall increase in ransomware remediation costs [7, 23]. Recovery costs differ from sector to sector and are influenced by a range of factors. For instance, outdated and fragmented IT systems contribute to high remediation costs. Organizations often have to completely rebuild their systems after a ransomware attack, costing time and money. Investing upfront in defenses can cut down remediation costs. For instance, upgrading systems before they come under siege from cyber-criminals is one way to minimize costs [7, 23].

Regarding economic impacts, it is necessary to explore both direct and indirect financial consequences that businesses face when dealing with ransomware attacks.

The most immediate financial repercussions of a ransomware attack are the direct costs, which include ransom payments, expenditures on technical remediation, and emergency IT services. These costs can vary widely depending on the specifics of the attack and the targeted organization's preparedness and response capabilities. Ransom payments are often the most obvious direct cost associated with ransomware attacks. The decision to pay a ransom is complex and filled with both ethical and practical considerations. According to a report by IBM, the average cost of ransom payments has been rising, reflecting the increasing sophistication of attacks and the critical nature of the data held hostage [13]. Organizations must weigh the immediate cost of the ransom against the potential long-term costs of data loss and operational downtime. Beyond the ransom itself, organizations must invest in technical remediation to remove the ransomware from their systems and restore data integrity. This process often requires the expertise of external cybersecurity professionals. The costs include forensic analyses to understand how the breach occurred, repairs to damaged software and hardware, and enhancements to cybersecurity measures

to prevent future attacks. The report on the state of ransomware by IT Security Portugal highlights how these remediation efforts can often exceed the cost of the ransom itself, particularly when significant system overhauls are required [21] [25].

Indirect costs, though less apparent than direct costs, can be more significant and longer-lasting[24]. These include operational downtime, reputational damage, and potential legal liabilities. One of the most crippling indirect costs of ransomware is operational downtime. As systems are taken offline and data becomes inaccessible, organizations face significant disruptions to their normal business operations. The duration of downtime can vary widely but often depends on the organization's preparedness and the complexity of the ransomware attack. According to WatchGuard, businesses on average experience substantial operational interruptions, with downtime costs often surpassing the ransom payments themselves [2]. The impact on an organization's reputation following a ransomware attack can be profound and must also be taken into account. Customers and partners may lose trust in the organization's ability to safeguard data, which can lead to lost business opportunities and a long-term decrease in revenue. This aspect is particularly damaging for sectors where trust and data integrity are foundational, such as in financial services and healthcare. The sustainability of these impacts is discussed in detail by Connolly et al., who explore how reputational damage can affect organizational sustainability long after the initial attack has been resolved [28]. Other indirect costs include legal and compliance costs. Ransomware attacks often put organizations at risk of non-compliance with data protection regulations such as General Data Protection Regulation (GDPR), in Europe, or Health Insurance Portability and Accountability Act (HIPAA), in the United States. The legal ramifications can include fines, penalties, and the costs associated with litigation and compensating affected parties. The complexity of these legal challenges is examined in the study by Connolly et al., which considers the broader implications of ransomware attacks within various regulatory frameworks [28].

The economic impact of ransomware varies significantly across different sectors, influenced by the nature of the data held and the criticality of continuous operations. Healthcare and Public Health Sectors are some of the more targeted sectors. In healthcare, for instance, ransomware can paralyze critical systems that are essential for patient care, leading to life-threatening situations. The direct costs in healthcare can include ransom

payments to regain access to patient records and systems, but the indirect costs such as lawsuits and regulatory fines for data breaches can be even more substantial. Schools and universities are also frequent targets, often due to less robust cybersecurity measures. The direct costs may involve paying ransoms to unlock research data or administrative records, but the indirect costs such as the disruption to educational services and the loss of prospective students can also be significant. At last, the government and infrastructure sectors are also in the top of the more targeted sectors. Ransomware attacks on government systems can cripple essential public services and lead to significant financial and operational disruptions. The case studies provided by Sergio Valente and others illustrate these impacts in detail, showcasing how public sector organizations manage and mitigate these challenges [27] [28].

2.3 Review of Existing Models for Estimating Ransomware Costs

Several models and approaches have been developed to estimate the costs associated with ransomware attacks. By examining literature, industry reports, and studies, this section aims to assess the methodologies used, their effectiveness, and the challenges they face in accurately estimating the economic impact of ransomware.

There is a need for cost estimation models which is driven by the increasing frequency and severity of ransomware attacks, which impose substantial financial burdens on affected organizations. These models vary widely in their approach, complexity, and focus, ranging from simple cost calculators to sophisticated economic models that incorporate a broad spectrum of direct and indirect costs.

Many existing models primarily focus on direct costs associated with ransomware attacks, such as ransom payments, immediate IT response costs, and the expenses related to system recovery and data restoration. These models often use historical data and industry benchmarks to provide baseline estimates. For instance, the Sophos report provides insights into average ransom payments and associated IT costs, which serve as critical data points for these models [13]. Other models attempt to quantify indirect costs, such as operational downtime, lost business opportunities, and reputational damage. These mod-

els are inherently more complex due to the difficulty in quantifying non-tangible impacts. The academic papers by [27] and [25] offer methodologies for estimating these broader economic impacts, emphasizing the long-term effects on organizational performance [28].

The methodologies used in existing models often involve a combination of quantitative and qualitative data analysis, econometric modeling, and scenario-based simulations. These methods are designed to accommodate the variability and uncertainty inherent in cyber incidents. Many models employ quantitative methods to analyze ransomware cost data, using statistical and econometric techniques to identify patterns and correlations. The research from [28], explores the use of machine learning algorithms to predict the cost outcomes based on various attack parameters and organizational characteristics. Given the unpredictable nature of ransomware attacks, some models use scenario-based simulations to explore a range of possible outcomes. These simulations allow organizations to understand potential cost impacts under different conditions, such as varying levels of cybersecurity preparedness or different ransomware strains. The utility of scenario-based simulations is particularly highlighted in the [2] and [25] studies, which discuss the application of these techniques in understanding cybersecurity risks.

Despite the development of various models, accurately estimating the costs of ransomware attacks remains challenging. These challenges stem from several factors that complicate the economic analysis of cyber incidents starting with:

- **Data Availability and Quality:** One of the primary challenges is the lack of reliable and comprehensive data on ransomware incidents. Many organizations are reluctant to disclose details about attacks due to reputational concerns or regulatory implications. This data scarcity affects the accuracy and reliability of cost models, as noted in [13] which discusses the implications of underreporting on cost estimations.

- **Evolving Nature of Attacks:** Ransomware attacks are constantly evolving, with attackers developing new strategies to evade detection and maximize their payouts. This evolution makes it difficult for existing models to remain relevant and accurate over time. Continuous updates and adaptations of models are necessary to keep pace with the changing tactics of attackers, as discussed in the [25] and [2].

- **Complexity of Indirect Costs:** Estimating indirect costs such as reputational

damage and lost customer trust is particularly challenging. These costs are often context-specific and can vary widely depending on the organization's industry, customer base, and the nature of the data affected. The need for models that can better capture these complex, indirect costs is emphasized across several studies, including those by Connolly and others [28].

2.4 Ransomware Online Calculators

There are multiple ransomware cost calculators online, most of them free. This is due to the need for tools that can estimate the potential financial impact of such incidents. This section examines online ransomware calculators that aim to help organizations gauge the potential costs associated with ransomware attacks. These online tools are designed to provide organizations with quick estimates of potential financial impacts resulting from ransomware attacks. These tools typically consider various factors, including downtime, data recovery costs, ransom amount, and more, to provide a comprehensive cost impact. None of these tools takes into account the time needed to recover from a ransomware attack.

The BullWall's Cost of Downtime Calculator [5] is an online ransomware calculator that aims to calculate ransomware costs by taking into account the number of affected users of the organizations and whether they will be unavailable to work or not. All the answered questions are about the hour value of the employees and how many hours they will not be able to do their work. On the other hand, Cyber Risk Calculator from At-Bay [3] takes a more simplistic approach where the only two questions are the business industry and the annual revenue of the organization. At last, the CFC's Ransomware Cost Calculator [26], also takes an approach by industry sector and revenue but, it also takes into account the number of employees of the organization.

In Table 2.1 it can be seen a simple comparison of the three online calculators. Each line of the table represents the input that each of the online software needs to do the calculations. For example, At-Bay's Cyber Risk Calculator only uses the industry sector and the organization's annual revenue. It doesn't use the number of employees of the organization neither the cost that employees represent, nor the number of hours that the

business will be offline, or other costs. As it can be seen in the *Value returned* line, the returned values are so disparate that they cannot be considered reliable.

Table 2.1: Input Required by Online Ransomware Cost Calculators

	Bullwall	**At-Bay**	**CFC**
Number of employees	Yes	No	Yes
Employees cost	Yes	No	No
Number of offline hours	Yes	No	No
Other costs	Yes	No	No
Industry sector	No	Yes	Yes
Annual revenue	No	Yes	Yes
Value returned	**11 600 000 €**	**23 286 $**	**387 500 €**

2.5 Ransomware Recovery Strategies

This section reviews the current strategies for mitigating ransomware risks and recovering from attacks, drawing from academic literature, industry reports, and studies. The effectiveness of various recovery strategies is explored and the operational and technical challenges that organizations face during the recovery process are discussed.

Ransomware recovery strategies encompass a range of practices and technologies designed to restore affected systems, retrieve lost data, and minimize downtime. These strategies are crucial for organizations to bounce back from ransomware attacks effectively and to prevent future occurrences.

One of the foundational strategies for ransomware recovery is the maintenance of regular, secure backups. Effective backup strategies ensure that data is not only backed up regularly but also stored in a manner that isolates it from the main network, thus protecting it from being encrypted during an attack. This strategy is emphasized across multiple sources, including the [21], which highlights the critical nature of off-site or cloud-based backups in ensuring data can be restored without having to pay a ransom.

Segmenting networks and implementing strict access controls are essential to contain the spread of ransomware once an attack is detected. By limiting the ransomware's ability to move laterally across a network, these measures can significantly reduce the scope of an attack. The effectiveness of network segmentation is well-documented in the academic literature, including studies by [28], which detail how segmentation can prevent ransomware

from accessing critical systems and data stores.

Enhancing endpoint security measures, including the use of advanced antivirus and anti-malware solutions, coupled with real-time monitoring, plays a vital role in detecting and isolating ransomware attacks as they occur.

The deployment of Endpoint Detection and Response (EDR) systems allows for the continuous monitoring of network and system activities, enabling rapid response to potential threats. This approach is supported by findings in the [25] thesis, which discusses the role of EDR systems in providing granular visibility and control over endpoint activities. The effectiveness of recovery strategies can be influenced by several factors, including the sophistication of the ransomware, the preparedness of the organization, and the speed of the response.

Various case studies, such as those presented in the [27] and [25] documents, provide real-world examples of how organizations have successfully recovered from ransomware attacks using combinations of these strategies. For instance, these studies often cite instances where robust backup protocols allowed organizations to restore their data with minimal loss, thereby avoiding the need to pay ransoms. Despite the availability of effective strategies, there are significant challenges in their implementation.

The [2] paper discusses challenges such as the high costs associated with maintaining state-of-the-art cybersecurity measures, the complexity of configuring and managing advanced security systems, and the need for ongoing employee training to ensure all personnel are aware of potential cyber threats.

Recent advancements in technology have led to the development of new tools and approaches to enhance ransomware recovery strategies. Innovations in AI and machine learning are being leveraged to predict ransomware attacks before they happen and to automate responses to attacks when they occur.

The [28] study discusses how machine learning models are trained to detect unusual patterns of behavior that may indicate a ransomware attack, allowing preemptive action to be taken.

According to [8], to counter ransomware attacks, resilient self-healing schemes like Ransom-ware-Resilient Self-Healing XML Documents need to be implemented, emphasizing the importance of multi-layered security approaches and backup strategies.

Authors in [12] state that leveraging file system characteristics and behavior-based detection mechanisms can substantially improve ransomware defense strategies in Linux systems.

Additionally, hardware-isolated network-storage codesign approaches like Ransom-aware Solid State Drives (RSSD) have shown effectiveness in defending against ransomware attacks with minimal performance overhead, as stated by [19].

Security leaders are prioritizing the implementation of advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) for faster threat detection. Internet of Things (IoT) security and Next-Generation Firewalls (NGFWs) are among the areas where leaders plan to invest [10].

2.6 Legal and Policy Considerations

This section reviews the legal frameworks and policy measures surrounding ransomware, which play a crucial role in shaping how organizations and governments respond to and mitigate the impacts of these cyberattacks. By examining a variety of sources, this review seeks to outline current regulations, identify gaps in legal responses, and discuss the implications of policy on ransomware defense and recovery strategies.

Ransomware attacks not only cause significant economic and operational damage but also raise complex legal issues. These issues revolve around data protection laws, compliance requirements, and the legal ramifications of ransom payments. In many jurisdictions, organizations that suffer data breaches, including ransomware attacks that result in data being accessed or encrypted, must comply with strict data protection regulations.

For example, the GDPR in the European Union imposes stringent requirements on data handlers to ensure the security of personal data. Non-compliance can result in heavy fines and penalties, as has been the case in several high-profile ransomware attacks where organizations were found lacking in their cybersecurity measures [13].

The legality of paying ransoms is a contentious issue. In some jurisdictions, paying ransom to cybercriminals, especially those on international sanction lists, can be illegal. This legal dilemma places affected organizations in a precarious position, having to balance the urgency of recovering their data with the legal implications of ransom payments.

Studies such as those by [28] discuss these legal challenges in depth, highlighting the need for clear legal guidelines regarding ransom payments in the context of ransomware attacks.

Government policies also play an important role in defining the landscape of cybersecurity and specifically, the prevention and mitigation of ransomware attacks. These policies not only aim to protect critical information infrastructure but also to create a proactive cybersecurity culture among private and public entities.

Many countries have developed national cybersecurity strategies that include specific provisions for combating ransomware. These strategies typically emphasize the importance of public-private partnerships, sharing of threat intelligence, and investing in cybersecurity infrastructure. The effectiveness of these strategies, however, often depends on their implementation and the active engagement of all stakeholders involved. In addition to national strategies, sector-specific regulations can dictate how particular industries protect themselves against ransomware. For instance, the healthcare sector in the United States must adhere to the HIPAA, which includes requirements for safeguarding Electronic Protected Health Information (ePHI). Compliance with such regulations not only helps protect sensitive data but also minimizes the risk of legal repercussions in the event of a ransomware attack.

Analyses of policy effectiveness often reveal that while policies are well-intentioned, their implementation can be fraught with challenges. Issues such as inadequate resources, lack of cybersecurity expertise, and slow legislative processes can hinder the effectiveness of policies designed to combat ransomware [2].

Looking forward, there is a need for dynamic legal and policy frameworks that can keep pace with the evolving nature of ransomware and other cyber threats. Innovations in policy could include:

- International Cooperation: Given the transnational nature of cyber threats, international cooperation is crucial. Developing standardized global legal responses and cooperative frameworks can enhance the ability to combat and respond to ransomware attacks effectively.

- Incentives for Improved Cybersecurity Measures: Policies that provide incentives for

adopting advanced cybersecurity measures can encourage organizations to enhance their defenses. This could include tax breaks, subsidies, or other financial incentives for businesses that invest in robust cybersecurity infrastructures.

2.7 Technological Innovations and Future Directions

When mentioning technological innovations and emerging trends it is necessary to find what is shaping the landscape of ransomware defense and recovery and the impact of these technologies on improving cybersecurity measures and predicting future directions in the fight against ransomware. The rapid evolution of ransomware attacks has required corresponding advancements in detection and response technologies.

Organizations are increasingly turning to sophisticated cybersecurity tools that can not only prevent ransomware but also minimize its impact if an attack occurs. EDR systems represent a significant advancement in endpoint security. These systems continuously monitor and collect data from endpoints to detect cyber threats and provide automated responses. The capabilities of EDR systems to identify suspicious activities and mitigate threats in real time are critical in preventing the spread of ransomware within an organization's network. The utility of EDR systems in combating ransomware is well-documented in the academic paper by [28], which discusses their effectiveness in detecting ransomware signatures and anomalies before they can cause significant damage.

AI and ML technologies are increasingly being integrated into cybersecurity tools to enhance their predictive capabilities. These technologies can analyze vast amounts of data to identify patterns and predict potential ransomware attacks, thus allowing preemptive action. Studies by [27] and [25] highlight the role of machine learning in developing predictive models that can anticipate ransomware attacks based on historical data and recent trends.

Blockchain technology offers a promising solution to ensure data integrity and security, particularly in the context of ransomware attacks. By decentralizing data storage, blockchain can prevent the kind of single-point failures that ransomware exploits. Implementing blockchain for data storage involves creating a distributed ledger where data is stored across multiple nodes, making it nearly impossible for ransomware to encrypt the

entire dataset. The immutability of blockchain also ensures that any unauthorized changes to the data can be easily detected and reversed.

The potential applications of blockchain in enhancing data security are explored in the [2] paper, which provides an analysis of how blockchain technology can mitigate the risks associated with ransomware. Beyond data storage, blockchain can facilitate the use of smart contracts that automatically execute responses when certain conditions are met, such as the detection of unauthorized data encryption. This proactive approach can significantly reduce the response time to a ransomware attack, potentially limiting its impact.

As more organizations move their operations to the cloud, securing cloud environments has become paramount. Cloud security innovations are continually being developed to address the unique challenges posed by cloud computing, including vulnerability to ransomware. Cloud Access Security Brokers (CASBs) are security policy enforcement points that sit between cloud service consumers and cloud service providers to ensure that the security policies of the enterprise are followed. CASBs help control access to cloud resources and can provide additional security measures such as encryption and device profiling, which are crucial in preventing ransomware attacks.

Cloud platforms are also increasingly offering advanced backup and recovery options that can be pivotal in ransomware incidents. These solutions often include automated backups that are regularly updated and can be quickly restored in the event of data encryption by ransomware. The importance of robust backup solutions in cloud environments is discussed in the [28] paper, which emphasizes the role of cloud backups in reducing downtime and data loss during ransomware attacks.

Looking ahead, the ongoing development of cybersecurity technologies promises new ways to combat ransomware. The integration of IoT devices into cybersecurity frameworks, the use of quantum cryptography for enhanced data security, and the continuous evolution of AI and ML models are expected to play fundamental roles in future ransomware defense strategies.

Future models may involve more advanced predictive analytics capabilities, where systems not only respond to threats but can anticipate them before they manifest. This proactive approach could fundamentally change how organizations defend against ran-

somware and other cyber threats. With the advent of quantum computing, quantum cryptography could potentially offer unbreakable encryption that would safeguard data against even the most sophisticated ransomware attacks. However, this technology is still in its infancy and presents both opportunities and challenges for cybersecurity.

2.8 Summary and Conclusions

This section synthesizes the findings from the literature review, summarizes key points, reflects on the interconnected themes, and draws some conclusions that underscore the relevance and urgency of advancing ransomware research, policy, and practice.

The review of existing literature on ransomware attacks highlights several areas of concern and interest, ranging from the evolution and proliferation of ransomware, the economic impact it has on organizations globally, to the effectiveness of current mitigation and recovery strategies, and the legal and policy frameworks that guide the response to these attacks. The ransomware landscape has evolved dramatically, becoming more sophisticated and damaging over time.

Advances in technology, including the rise of cryptocurrencies and improvements in encryption methods, have facilitated this evolution, making ransomware a formidable challenge for modern cybersecurity defenses. These developments necessitate ongoing adaptations in cybersecurity tactics and tools to keep pace with increasingly savvy adversaries.

Ransomware attacks impose significant direct and indirect costs on organizations. Direct costs include ransom payments and expenditures on technical remediation, while indirect costs encompass operational downtime, reputational damage, and potential legal liabilities. The economic burden of ransomware is exacerbated by its capacity to affect a wide range of industries, each with unique vulnerabilities and consequences.

The studies reviewed provide a detailed examination of these costs and highlight the critical need for effective economic models to quantify and manage these impacts [13] [2] [25].

Effective ransomware mitigation and recovery strategies are critical in minimizing the impact of attacks. Strategies such as robust backup systems, network segmentation, and advanced threat detection tools like EDR systems have been identified as key components

of a good cybersecurity approach. The effectiveness of these strategies varies, influenced by the organization's preparedness, the resources available, and the specific nature of the ransomware attack.

Innovations in AI and ML are promising developments that could enhance the predictive capabilities of cybersecurity systems, offering new ways to predict and respond to ransomware threats [28].

Robust legal and policy frameworks in managing ransomware risks must also exist. Regulations such as GDPR have set significant precedents in terms of compliance requirements and the legal implications of data breaches.

However, the legality of ransom payments remains a contentious issue, with a clear need for more definitive guidelines and international cooperation to address the global nature of cyber threats. The discussion also points to the potential of emerging technologies like blockchain to enhance data integrity and security, although these are not without their challenges and limitations [28].

The themes explored in this review are deeply interconnected, illustrating the complexity of the ransomware challenge. Technological advancements not only contribute to the effectiveness of cybersecurity measures but also to the sophistication of ransomware attacks, creating a dynamic and ongoing conflict between cybercriminals and defenders.

Similarly, the economic impact of ransomware is linked to the effectiveness of recovery strategies. Organizations that invest in advanced cybersecurity measures may experience lower overall costs in the event of an attack. These interdependencies suggest that no single strategy or solution is likely to be sufficient. Instead, a multi-faceted approach that includes technological innovation, economic analysis, legal considerations, and policy development is required to effectively combat ransomware.

There is a clear need for more sophisticated economic models that can accurately quantify the full spectrum of ransomware costs, incorporating both direct and indirect impacts. Future research should focus on developing these models, incorporating real-world data and case studies to improve their accuracy and relevance. As ransomware continues to evolve, so too must the legal and policy frameworks that govern cybersecurity practices.

Future legislative efforts should aim to clarify the legality of ransom payments, en-

hance international cooperation, and provide clear guidelines for organizations on how to respond to ransomware attacks legally and ethically. Continuous innovation in cybersecurity technologies is essential to stay ahead of ransomware threats. Future research should explore the potential of emerging technologies like AI, ML, and blockchain to enhance ransomware detection, prevention, and recovery strategies.

Several websites state that they calculate the money businesses lose when attacked by ransomware. The approach used by online ransomware recovery calculators is based on estimating the commercial value of the company, the loss of image and position in the market are the main goals. Estimating the time, not cost, needed to recover from a ransomware attack in the form of a utility function is a novel approach, which is pursued in the work herein.

Chapter 3

Methodology

This chapter explains the statistical methods and models used in the analysis, providing a rationale for their choice and describing how they contribute to the reliability and validity of the utility function. This section is crucial as it not only supports the credibility of the research but also provides a replicable methodological framework for future studies.

Although there are many methodologies to use, this work implements a mixed methods research strategy. As the study begins with an inquiry, analyzing data, and integrating known public data, it is employing a quantitative methodology. However, using "use cases" to validate the findings added a practical, application-based dimension to the research, which aligns closely with action research or applied research methods.

The adopted methodology is presented in Fig. 3.1 and was divided into three parts: Data Collection, Utility Function Refinement, and Validation Techniques.

In Data Collection there is an emphasis on data collection, which was used as an element for the utility function. The primary mechanism for data gathering was an online questionnaire, made to obtain responses pertinent to ransomware recovery times. The questionnaire was structured into two main sections: the first addressing the organization's Disaster Recovery (DR) policies and practices, and the second focusing on the recovery times for various Information and Technology (IT) assets.

The Utility Function Refinement details the refinement process of the utility function designed to assess the recovery costs from ransomware attacks. This refinement was based on an analysis of data collected through the questionnaire mentioned. The original utility function underwent some refinement to enhance its relevance to real situations faced by

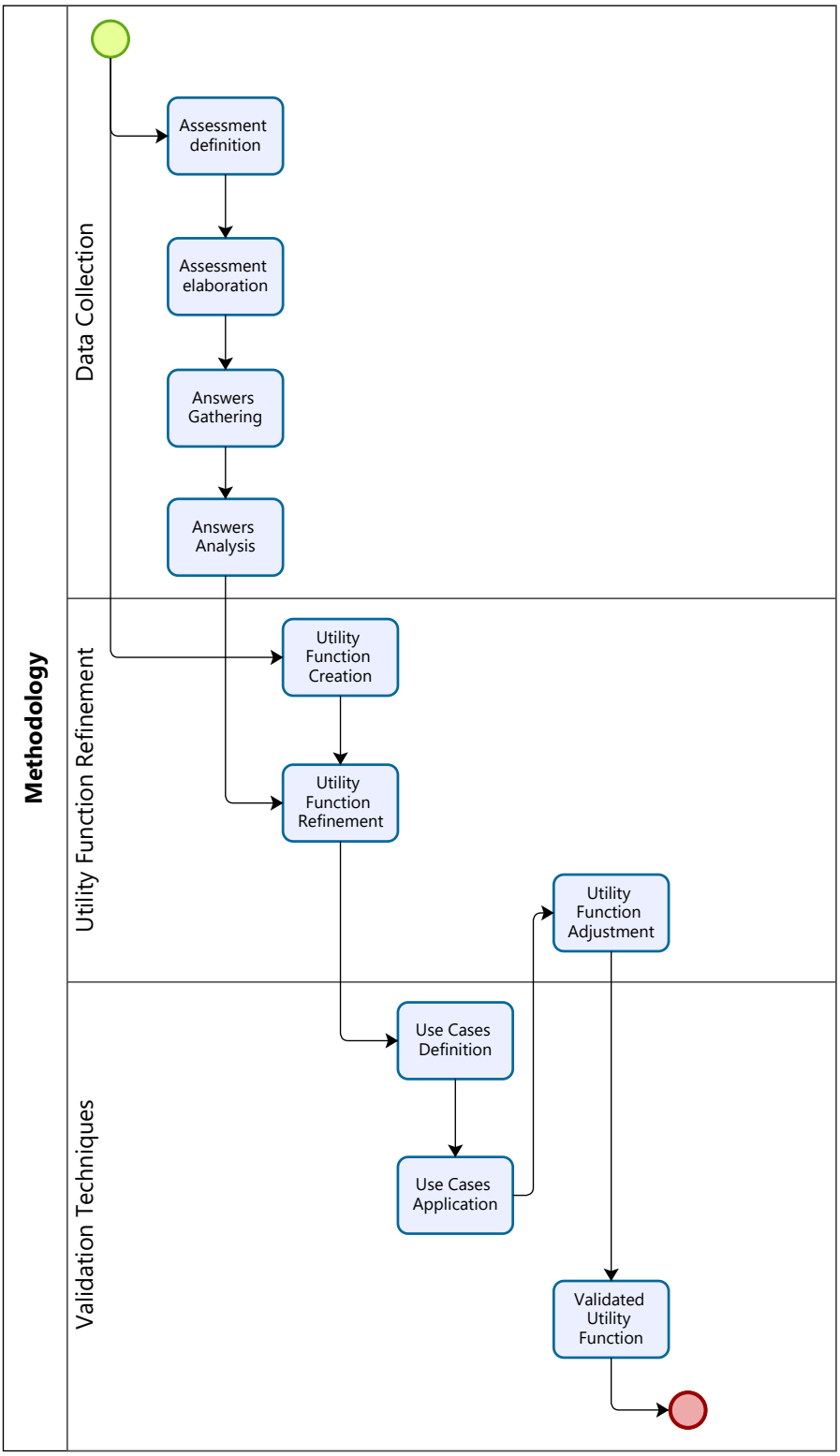

Figure 3.1: Methodology Used

organizations. The refinement involved simplifying the model and focusing on the most impactful aspects of ransomware recovery times.

The Validation Techniques section outlines the validation techniques used to confirm the value of the refined utility function for estimating ransomware recovery times. This phase involved testing the utility function against use cases simulating various organizational sizes and configurations. The process consisted of applying the utility function to three model organization, small, medium, and large and to observe how it performed across different IT infrastructure scales and complexities.

Details of the tasks involved are depicted in the following sections.

3.1 Data Collection

To obtain ransomware recovery times, the time organizations need to recover their assets after a ransomware attack was collected. This time is key in the estimation of operational downtime, allowing for better preparation of business continuity processes. The purpose of this data collection was to gather data on current recovery capabilities and to analyze the effectiveness of these capabilities in diverse IT environments and scenarios.

The data collection assumed the form of an online questionnaire that consisted of nineteen questions. It was designed to extract information regarding the presence and efficacy of DR policies, the extent of redundancy systems, and the needed recovery time for various IT components. It was divided into two sections. The first section was about the existence of DR and the geographical distribution of the resources. The second was aimed at the restoration capabilities of IT assets. The questions were structured to elicit both qualitative and quantitative data, with some emphasis on the difference in recovery times when backups are available, compared to scenarios with no backups. The questions were selected to cover a broad range of IT assets, from workstations and servers to user applications, and network peripherals. This approach allowed the data collection to be evaluated through the recovery operations across different technologies and infrastructure components. Distinguishing between recovery times with and without backups, the data collection provides insight into the real-world impact of backup strategies on DR processes.

The questionnaire comprised the following questions:

- (Q01) Does your organization have a DR policy?
- (Q02) Does your organization have multiple locations?

- (Q03) Does your organization have a redundancy system (or fail-over) for essential services?
- (Q04) If you answered Yes to the previous question, how much time (in hours) is needed to get your redundancy or fail-over operational?
- (Q05) Can you restore a group of workstations automatically and simultaneously?
- (Q06) If you answered Yes to the previous question, how many can you restore simultaneously?
- How much time do you need to restore:
  - (Q07) a workstation.
  - (Q08) user applications used by the institution.
  - (Q09) a server.
  - (Q10) an enterprise application.
  - (Q11) a database management system.
  - (Q12) an email system.
  - (Q13) a backup system.
  - (Q14) a cloud service or a virtual machine.
  - (Q15) a storage, NAS, or equivalent.
  - (Q16) a security system (for example, a firewall).
  - (Q17) network equipment (routers, switches, wireless access points, etc.).
  - (Q18) a mobile device or tablet.
  - (Q19) a printer or another peripheral used in your institution.

Questions Q07 to Q19 were asked in two different scenarios: one in which the company has usable backups and one in which there are no usable backups.

3.1.1 Overview

The questionnaire was available from January 25 until February 25. A total of 34 submissions were obtained.

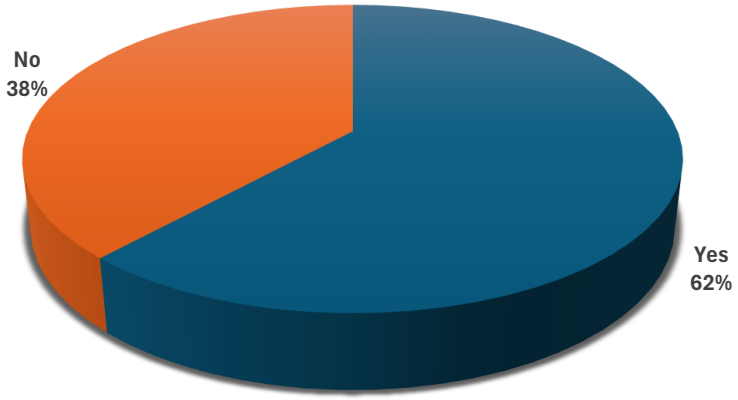

Figure 3.2: Answers to Q1 - Does your organization have a DR policy?

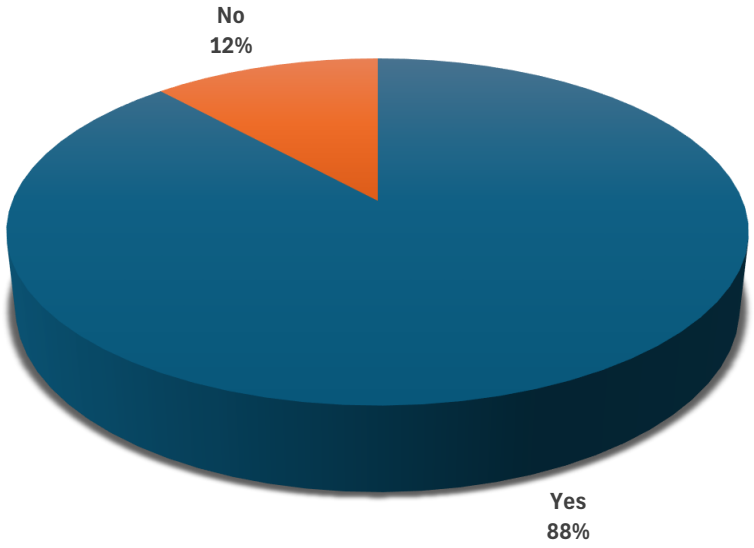

Figure 3.3: Answers to Q2 - Does your organization have multiple locations?

In Fig. 3.2 it can be seen the percentage of organizations that have or don't have a DR policy. Analyzing these results, it can be concluded that 61.8% (21 of 34) have a DR mechanism in place, indicating a good level of preparedness. In Fig. 3.3 there is represented the percentage of organizations that have multiple locations. This Figure highlights that the majority of the inquired, 88.2% (30 in 34), have multiple locations, indicating that the DR solutions are distributed. Both results can be verified in Fig. 3.2 and in Fig. 3.3.

Fig. 3.4 illustrates the number of organizations with redundancy systems and Fig. 3.5 the time it takes for organizations to activate these systems. According to the data 64.7% (22 of 34) of participants reported using redundancy systems as part of their DR approach.

There is a clear trend towards activating the redundancy systems in less than an hour. However, some questions were raised about the efficacy of these systems because there is also a significant variance in the time necessary to activate the fail-over or redundancy thus leaving some room for future studies, as presented in Fig. 3.4 and Fig. 3.5.

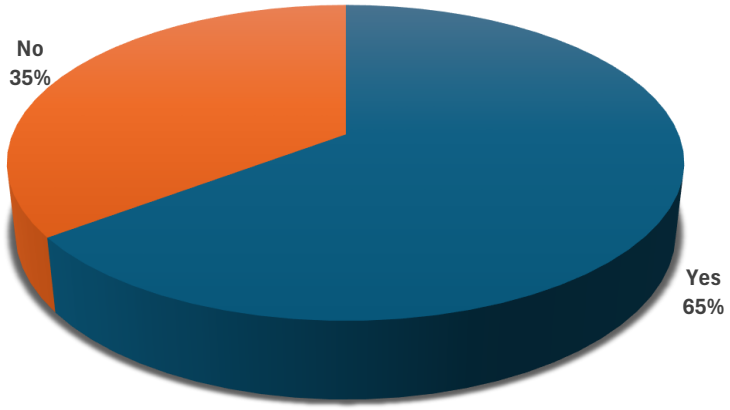

Figure 3.4: Answers to Q3 - Does your organization have a redundancy system (or failover) for essential services to its operation?

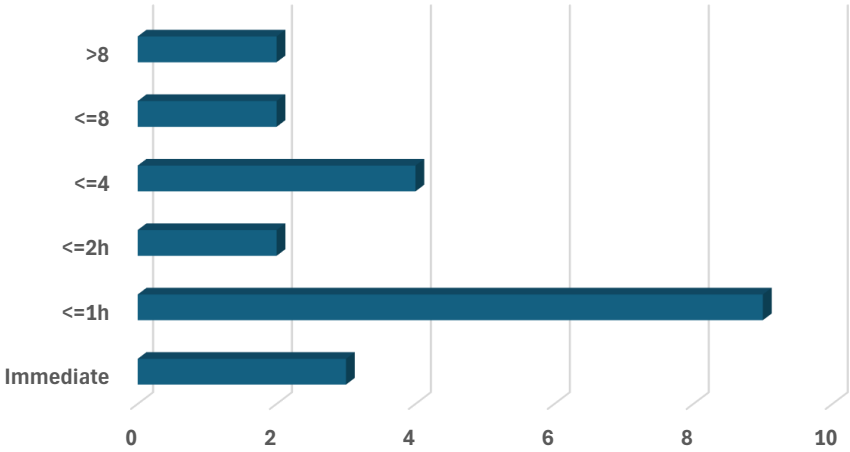

Figure 3.5: Answers to Q4 - If you answered Yes to the previous question, how much time (in hours) is needed to get your redundancy or failover operational?

A relevant feature in ransomware recovery is the ability to simultaneously restore workstations (see Fig. 3.6, and only 32.4% (11 of 34) affirmed to have this capability, as presented in Fig. 3.6. Of the ones that answered yes to this question, 54.5% (6 of 11) affirmed that they could recover 30 or more pieces of equipment simultaneously as presented in Fig. 3.7.

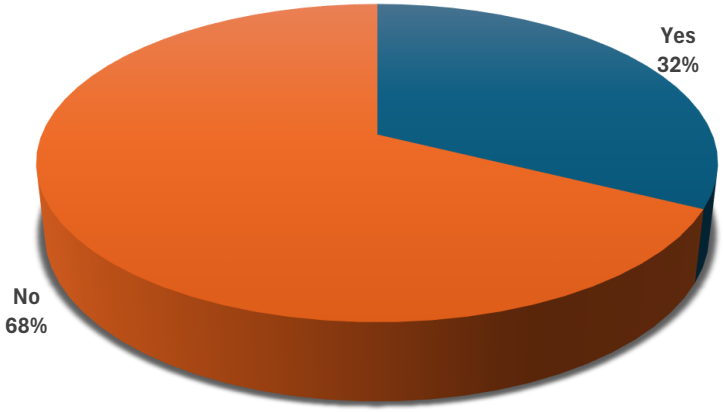

Figure 3.6: Answers to Q5 - Can you restore a group of workstations automatically and simultaneously?

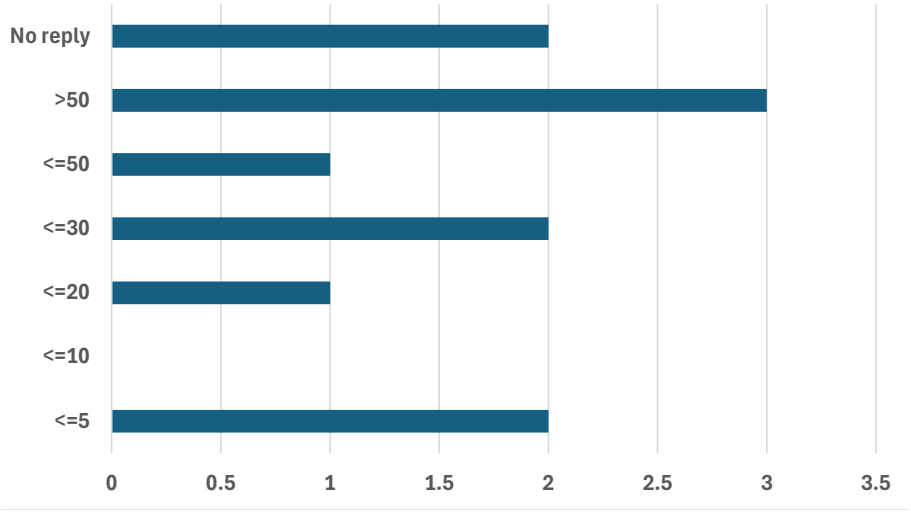

Figure 3.7: Answers to Q6 - If you answered Yes to the previous question, how many can you restore simultaneously?

The recovery time reported varies for critical infrastructure such as servers, databases, and email systems, with a fraction of organizations capable of achieving restoration within a single day. However, detailed recovery times displayed a broad spectrum, highlighting the diverse IT environments and the complexity of recovery processes. One of the factors distinguishing the recovery process is the presence of usable backups. The survey results exhibited this dependency, with responses showing a marked decrease in recovery times across all queried IT assets when backups were available. The contrast was particularly notable in database and email system recoveries. This is visible in server and workstation recovery for example, as presented in Fig. 3.8 and Fig. 3.9, which presents the recovery

times per asset when there are no backups and when backups are available.

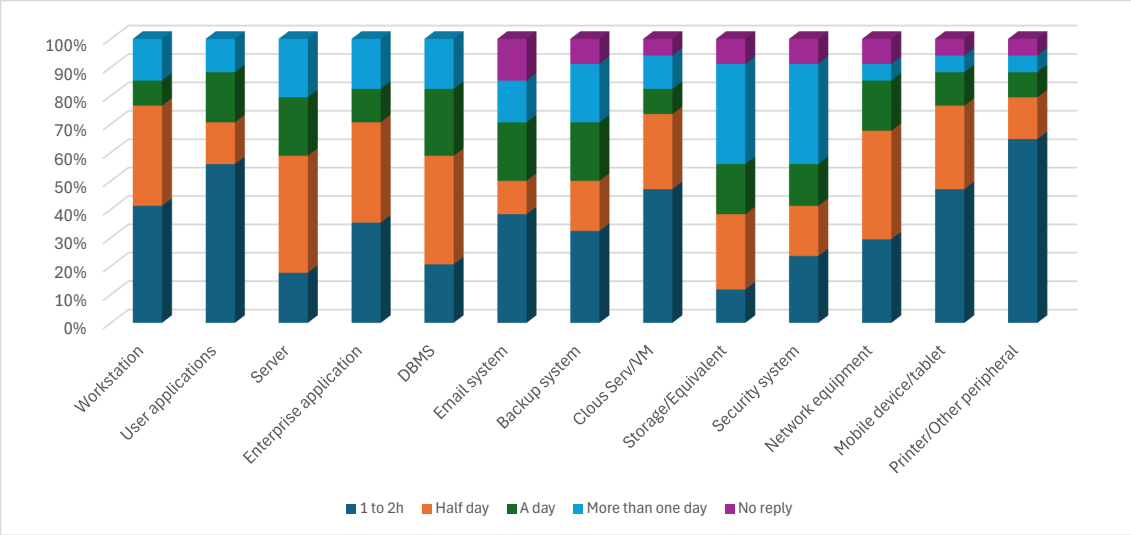

Figure 3.8: IT assets recovery time without backup.

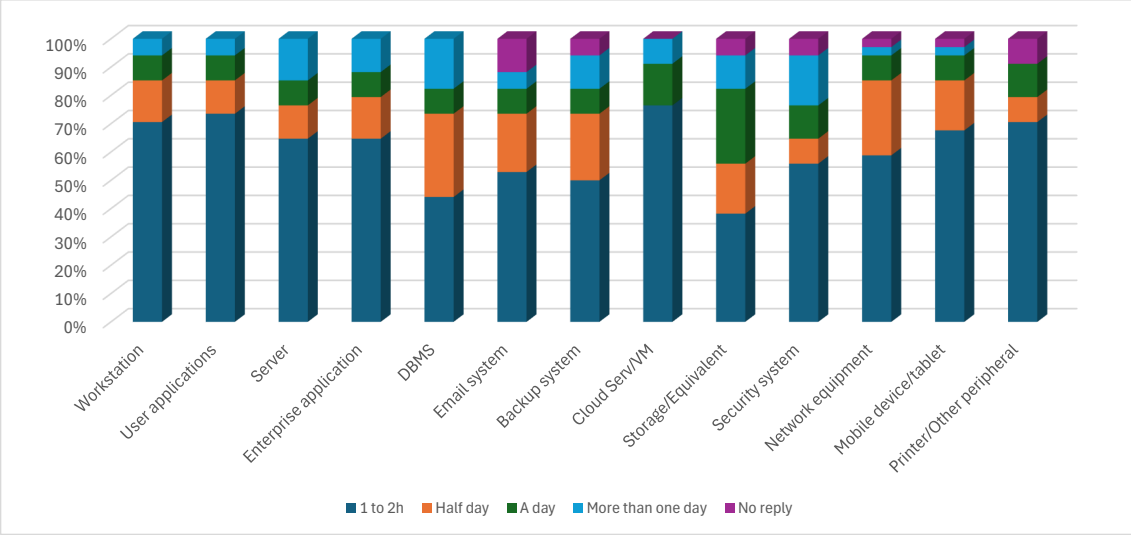

Figure 3.9: IT assets recovery time with backup.

This data collection provided insight into the current practices of recovering from ransomware attacks. The adoption of DR policies and redundancy confirmed their relevancy for faster recovery. There is a great variability in recovery times, especially when there are no backups. This shows a margin for improvement and that future studies can be done.

3.1.2 Results

Considering the questionnaire, the mean recovery time for the different types of equipment, with and without the use of backups, was estimated. The estimated values are presented in Table 3.1).

Table 3.1: Mean recovery times (hours:minutes) with and without backups

Equipment type	**With backups**	**Without backups**
Workstation + Apps	5:25	7:43
Server + Software (Enterprise App / DBMS / Email / Backup)	7:09	9:59
Cloud services / Virtual Computers	3:05	3:39
Storage	4:21	6:52
Security Appliance	4:10	6:34
Network Equipment	2:38	3:40
Mobile Device	2:30	3:11
Printer	2:13	2:48

The results show that backups effectively reduce recovery times across all equipment types. For instance, when considering the recovery of a workstation and its applications when using backups, would require 5 hours and 25 minutes, compared to 7 hours and 43 minutes, when no backups are available. This is particularly evident when considering servers, storage, and security appliances, where the differences can be more than 2 hours and 30 minutes, per equipment. Minimal differences were estimated for the recovery of devices, such as mobile devices and printers, suggesting that these are easier to recover.

3.2 Utility Function

The definition of a utility function for ransomware recovery time estimation involved a series of steps, going from a conceptual model to a tool. This process integrated a combination of empirical data and theoretical modeling to ensure the utility function's applicability and accuracy in estimating the impact of ransomware attacks.

The development of the utility function commenced with an initial conceptual framework aimed at quantifying the costs associated with ransomware attacks. The framework was designed to integrate both direct and indirect time variables that encapsulate the impacts of such cybersecurity incidents.

The preliminary version of the utility function was developed using a deductive approach, where variables were selected based on literature review findings and inputs from cybersecurity experts (see Eq. 3.1). This version was structured to allow preliminary testing through hypothetical scenario analyses, providing a basis for initial validation and refinement.

$$RT = a \times t_{\mathrm{NA}} + b \times DC + c \times IR \tag{3.1}$$

In this initial version, each of the variables has the following meaning:

- Number of Assets (NA) accounts for the number of assets
- Direct Costs (DC) that stands for the direct costs (in time)associated with initial recovery efforts
- Initial Response (IR) denotes the time required to detect and begin responding to the attack
- a,b, and c are coefficients representing the weight of each factor on the overall recovery cost
- t represents the time

This preliminary function was over-simplistic and some adjustments were made to ensure that a more refined version was available that could be more precise and capable of being of use. As a result, a more extensive function was defined (see Eq. 3.2).

$$\begin{aligned} RT_U = & \overbrace{t_{\mathrm{AD}} + t_{\mathrm{RM}} + t_{\mathrm{PA}}}^{t_{\mathrm{DI}}} + \overbrace{(t_{\mathrm{CP}} + t_{\mathrm{CI}} + t_{\mathrm{DA}} + t_{\mathrm{EP}} + t_{\mathrm{EE}})}^{t_{\mathrm{CE}}} + \\ & \overbrace{\frac{t_{\mathrm{WA}} \times n_{\mathrm{WA}}}{s_{\mathrm{WA}}} + \frac{t_{\mathrm{SA}} \times n_{\mathrm{SA}}}{s_{\mathrm{SA}}} + \frac{t_{\mathrm{CV}} \times n_{\mathrm{CV}}}{s_{\mathrm{CV}}} + \frac{t_{\mathrm{ST}} \times n_{\mathrm{ST}}}{s_{\mathrm{ST}}}}^{t_{\mathrm{RT}}} + \\ & \overbrace{\frac{t_{\mathrm{SE}} \times n_{\mathrm{SE}}}{s_{\mathrm{SE}}} + \frac{t_{\mathrm{NE}} \times n_{\mathrm{NE}}}{s_{\mathrm{NE}}} + \frac{t_{\mathrm{MD}} \times n_{\mathrm{MD}}}{s_{\mathrm{MD}}} + \frac{t_{\mathrm{PR}} \times n_{\mathrm{PR}}}{s_{\mathrm{PR}}}}^{t_{\mathrm{RT}}} + \\ & \overbrace{(t_{\mathrm{SI}} \times n_S) + (t_{\mathrm{WI}} \times (n_S + n_W)) + (t_{\mathrm{DV}} \times (n_S + n_W)) + (t_{\mathrm{AF}} \times (n_S + n_W)}^{t_{\mathrm{TV}}} + \\ & \overbrace{t_{\mathrm{RC}} + t_{\mathrm{IP}} + t_{\mathrm{II}} + t_{\mathrm{TR}}}^{t_{\mathrm{MS}}} + \overbrace{(t_{\mathrm{CM}} + t_{\mathrm{IC}} + t_{\mathrm{EC}} + t_{\mathrm{CM}} + t_{\mathrm{MA}})}^{t_{\mathrm{CC}}} + t_{\mathrm{AV}} \end{aligned} \tag{3.2}$$

In this intermediate function, the following items were identified (each of the components of the formula takes into account the time (t) needed for the referred operation):

- Detection and Initial Analysis (DI), composed of:
  - Attack Detection (AD): Identify the abnormal activity as an attack
  - Response Team Mobilization (RM): Inform the response team and start working
  - Preliminary Analysis (PA): Evaluate and analyze the information received
- Contention and Eradication (CE), composed of:
  - Contention Points Identification (CP): Verify if a contention is eventually possible and where to do it
  - Contention Implementation (CI): Contention plan implementation
  - Damage Assessment (DA): Verify the extent of the damage
  - Eradication Planning (EP): Plan the eradication
  - Eradication Execution (EE): Implement the eradication plan
- Recovery Time (RT), composed of:
  - Workstation and Apps Recovery (WA)
  - Server and Enterprise Apps or Server and DBMS or Server and Email or Server and Backup Recovery (SA)
  - Cloud Service / Virtual Computer Recovery (CV)
  - Storage Appliance Recovery (ST)
  - Security Appliance Recovery (SE)
  - Network Equipment Recovery (NE)
  - Mobile Device Recovery (MD)
  - Printer Recovery (PR)
- Test and Validation Time (TV), composed of:
  - Server Integrity Tests (SI)

  - Computer Security Verification (WI)
  - Data Validation (DV)
  - Application Functional Tests (AF)
  - Number of Servers (NS)
  - Number of Workstations (NW)

- Mitigation and Security Improvements (MS), composed of:
  - Root Cause Analysis (RC)
  - Security Improvements Planning (IP)
  - Improvements Implementation (II)
  - Training (TR)

- Crisis Management and Comunication Measures Time (CC), composed of:
  - Communication Plan Preparation (CM)
  - Internal Communication (IC)
  - External Communication (EC)
  - Crisis Management Coordination (MC)
  - Communication Adjustments and Monitorization (MA)

- Aditional Variables (AV)

Following the initial development, the utility function underwent an evaluation to assess its complexity and utility. This evaluation revealed some redundancies and overlapping variables that did not enhance the model's capability. A decision was made to remove these elements, simplifying the model and focusing on variables with impact.

The revised utility function was subjected to validation using some use cases encompassing diverse ransomware scenarios across various industries. The validation process involved applying the utility function to simulated real-world data and comparing the model's predictions with actual data when possible.

This stage was crucial for assessing the accuracy of the variable values within the utility function. Discrepancies between predicted and actual results prompted further

adjustments to the model's parameters. The validation process tried to ensure that the function reflected the realities of ransomware recovery thus enhancing its reliability.

The final refinement involved adjusting the time assigned to each variable within the utility function. The time attribution process was important as it determined the impact of each component on the overall estimated recovery time. Time assignments were based on both quantitative analyses, such as the questionnaire results, and qualitative inputs through expert opinion.

These adjustments ensured that the time defined accurately reflected the value of each variable in the context of ransomware recovery, thereby enhancing the utility function's accuracy and practical utility.

3.3 Model Organizations

To validate the proposed ransomware recovery time estimation utility function, three sample organizations, of different dimensions, were considered. The three model organizations, detailed in Table 3.2, were defined based on real-world organizations that were adapted to be used in this study. For instance, a small organization would need 10 workstations (i.e. 10 users), a medium organization would need 280 workstations, and a large organization would need 5.800 workstations.

Table 3.2: Use cases definition (number of equipment)

	Small	**Medium**	**Large**
Total Workstations	10	280	5800
Total Servers	1	240	450
Total Cloud Services/VM	0	0	40
Total Storages	1	2	10
Total Security Appliances	0	4	600
Total Network Equipments	1	40	700
Total Mobile Devices	0	300	0
Total Printers	1	15	1000

These three sample organizations were used in all the calculations made using the formula to make sure that the calculations were stable.

The validation method used later revealed results within acceptable values, considering the input variables and the calculations performed. The calculated results demonstrated

consistency and logic.

Chapter 4

The Utility Function Proposal

The complexity and variability of ransomware attacks make accurate cost estimation challenging. Traditional approaches to estimating cybersecurity threats often fail to capture the multifaceted and dynamic nature of ransomware. This gap in knowledge and capability underscores the need for a specialized tool that can provide organizations with a reliable estimate of potential recovery costs.

The development of a recovery utility is essential for quantifying the time needed to recover from a ransomware attack. It estimates the time needed to restore services in case of an attack and enhances organizational response strategies against cyber attacks.

Some of the objectives of developing such a utility function involve the quantification of the time needed to recover from a ransomware attack thus allowing for the calculation of the direct costs, facilitating decision-making through simulations that can predict each input scenario, and allowing the calculation of multiple scenarios through the use of a formula.

As stated in Section 3.1, after the questionnaire was done and the answers were collected, grouped, and analyzed. The responses were quantitatively analyzed to derive some statistical measures for the recovery times of different IT assets. This analysis helped identify trends and outliers in the data, providing a baseline for understanding the average recovery scenario.

Using the insights obtained from the data analysis, it was possible to develop a utility function to calculate the cost of recovering from ransomware attacks using the time obtained from the answers of the questionnaire. The function incorporates variables de-

rived from the data, such as the average time to recover various types of equipment and the effectiveness of existing DR policies. After that, the utility function was adapted to use the default values obtained from the data analysis. This adaptation ensured that the function reflected realistic recovery scenarios and could provide accurate cost estimates. Sensitivity tests were also conducted on the utility function to determinate how changes in input variables affect the time outcomes. This analysis was important for understanding the validity of the model and for identifying key drivers. The function was also applied to three use cases representing small, medium, and large organizations. Each use case was constructed based on actual organizations, including specific IT infrastructures and DR policies. The function was used to estimate the recovery times for each organization, simulating a ransomware attack scenario based on their specific data.

Then, a utility function was developed to estimate ransomware recovery costs by calculating the time needed for the recovery. The proposal divided into three distinct parts: Initial Recovery, Recovery, and Validation. Each segment plays a role in ensuring that the function is not only comprehensive but also precise and adaptable to various real-world scenarios. This division allows each phase to focus on different aspects of ransomware recovery time and cost estimation, thereby enhancing the utility and applicability of the function.

The Initial Recovery part of the utility function is designed to capture the immediate costs and actions required following a ransomware attack. This includes the time spent directly associated with the initial response to the attack and short-term recovery efforts. Such times often involve immediate technical assessments, deployment of emergency cybersecurity measures, and initial communications to stakeholders. The reason for isolating these immediate costs in the utility function is to provide organizations with a clear understanding of the upfront expenditures they might face. The importance of the Initial Recovery phase cannot be overstated. By quantifying these early-stage times, the function allows for the evaluation of the immediate response activities.

The Recovery part of the utility function addresses the time spent in activities associated with the recovery process. This phase is crucial as it involves the restoration of full operational capabilities and the strengthening of cybersecurity postures to prevent future attacks. Times accounted for in this part include data recovery, system repairs, and

Table 4.1: Weight of formula parts per organization size (in percentage)

	Small				Medium				Large			
	No Bkp		Bkp		No Bkp		Bkp		No Bkp		Bkp	
	Time	%	Time	%	Time	%	Time	%	Time	%	Time	%
RT1	24:00	18%	24:00	23%	24:00	0%	24:00	1%	24:00	0%	24:00	0%
RT2	100:29	75%	70:31	68%	5.740:20	90%	4.146:37	86%	58.770:30	92%	41.361:00	89%
RT3	09:15	7%	09:15	9%	630:00	10%	630:00	13%	5.137:30	8%	5.137:30	11%
Total	133:44	100%	103:46	100 %	6.394:20	100%	4.800:37	100%	63.932:00	100%	46.522:30	100 %

upgrades to cybersecurity infrastructure. The segmentation of the utility function to include Recovery is important because it recognizes that the impact of a ransomware attack extends far beyond the initial breach. The processes and time involved in fully restoring operational capabilities are often complex and prolonged. By separately analyzing these costs, the utility function provides a more detailed and accurate estimation of the total financial impact.

The Validation part of the utility function addresses the time spent to ensure the integrity and reliability of the recovered systems. The inclusion of a dedicated validation phase in the utility function is indicative of a commitment to reliability and integrity of the recovered systems. Validation is indispensable as it provides a security mechanism for the Recovery part of the utility function, allowing for validation of the systems. Through validation, the recovered systems are refined to fulfill the security rules, and tested in accordance.

$$RT = RT_1 + RT_2 + RT_3 \tag{4.1}$$

The proposed formula (see Eq. 4.1) consists in adding the computed duration of each of the three steps. RT_1 referring to the Initial Recovery step duration, RT_2 referring to the Recovery step duration, RT_3 referring to the Validation step duration. Finally, it is important to note that in the creation of the utility function IT automation tools or the level of expertise of the staff that will be used during the recovery, were not taken into account.

Using the division of the utility function into Initial Recovery, Recovery, and Validation and taking into account each of the use cases, it is possible to evaluate the weight of each of the parts depending on company size and the existence or not of backups as shown in Table 4.1.

4.1 Initial Recovery

This step includes the activities of the recovery process that are generally invariant across different incidents. It includes the initial detection of the ransomware attack and the immediate response actions. The duration of the Initial Recovery was predefined based on historical data providing a baseline duration for these early stages. This simplification assumes standard conditions and operational responses, offering a time estimate that precedes more variable recovery activities.

The following activities were identified:

- DI, composed of:
  - AD: Identify the abnormal activity as an attack
  - RM: Inform the response team and start working
  - PA: Evaluate and analyze the information received
- CE, composed of:
  - CP: Verify if a contention is eventually possible and where to do it
  - CI: Contention plan implementation
  - DA: Verify the extent of the damage
  - EP: Plan the eradication
  - EE: Implement the eradication plan

Eq. 4.2 denotes the components used to estimate the total duration of the first step. One first consideration that can be made is that this formula does not consider the number of equipment (servers, workstations, etc.) of the entity, meaning that, later on, it may be simplified to a constant value. Each of the components of the formula take into account the time (t) needed for the referred operation.

$$RT_1 = \overbrace{t_{\mathrm{AD}} + t_{\mathrm{RM}} + t_{\mathrm{PA}}}^{t_{\mathrm{DI}}} + \overbrace{(t_{\mathrm{CP}} + t_{\mathrm{CI}} + t_{\mathrm{DA}} + t_{\mathrm{EP}} + t_{\mathrm{EE}})}^{t_{\mathrm{CE}}} \tag{4.2}$$

4.2 Recovery

The Recovery step is one of the key terms when estimating the duration of a ransomware recovery; therefore, it is essential to allow it to be adaptable to any organizational context and recovery capabilities. In essence, it evaluates the time required to recover various types of IT assets, such as workstations, servers, and network equipment. It considers the number of affected assets and the organization's capability to restore multiple assets simultaneously.

The following items are listed to be recovered:

- WA: Workstation and Apps Recovery
- SA: Server and Enterprise Apps or Server and DBMS or Server and Email or Server and Backup Recovery
- CV: Cloud Service / Virtual Computer Recovery
- ST: Storage Appliance Recovery
- SE: Security Appliance Recovery
- NE: Network Equipment Recovery
- MD: Mobile Device Recovery
- PR: Printer Recovery

One first consideration that can be made is that the considered component values vary according to the existence, or not, of backups. For instance, as a result of the questionnaire presented in Section 3.1.2, WA assumes an average value of 325 minutes with backups, and 463 minutes without, per workstation. Each of the components of the formula takes into account the time (t) needed for recovery and is then multiplied by the number of equipment of each type (n) and divided by the number of equipment that can be restored simultaneously (s).

Eq. 4.3 denotes the components used to estimate the total duration of the second step.

$$RT_2 = \frac{t_{\mathrm{WA}} \times n_{\mathrm{WA}}}{s_{\mathrm{WA}}} + \frac{t_{\mathrm{SA}} \times n_{\mathrm{SA}}}{s_{\mathrm{SA}}} + \frac{t_{\mathrm{CV}} \times n_{\mathrm{CV}}}{s_{\mathrm{CV}}} + \frac{t_{\mathrm{ST}} \times n_{\mathrm{ST}}}{s_{\mathrm{ST}}} + \frac{t_{\mathrm{SE}} \times n_{\mathrm{SE}}}{s_{\mathrm{SE}}} + \frac{t_{\mathrm{NE}} \times n_{\mathrm{NE}}}{s_{\mathrm{NE}}} + \frac{t_{\mathrm{MD}} \times n_{\mathrm{MD}}}{s_{\mathrm{MD}}} + \frac{t_{\mathrm{PR}} \times n_{\mathrm{PR}}}{s_{\mathrm{PR}}} \tag{4.3}$$

4.3 Validation

In the context of ransomware recovery, the validation of restored systems is a critical phase that ensures the integrity and operational functionality of IT systems post-recovery. This process involves testing and verification procedures to confirm that all systems and data are fully restored to their pre-attack state and are free from any remnants of the ransomware. After the technical recovery tasks are completed, it is essential to ensure that the restored systems are secure, functional, and compliant with organizational standards. The third step, Validation, addresses this need by incorporating times for verification and validation activities. This includes integrity checks, security verifications, data validations, and functional tests for applications and systems. This part of the formula pretends to ensure that all restored assets are operational and secure before they are reintegrated into the live environment, marking the final step in the recovery process. The main goal of validating the recovered systems is to ensure that the recovery process is complete, secure, and effective. This involves confirming that no vulnerabilities are left unaddressed, which could potentially lead to re-infection or additional security breaches. Additionally, this phase assures stakeholders that the systems are reliable and the data integrity is intact, thereby reinstating operational confidence.

The validation of restored systems is structured to address multiple layers of the IT infrastructure, including hardware, software, and data. The hardware verification can involve physical and functional checks to ensure that all hardware components are running correctly and have not been compromised. Techniques include hardware diagnostics, performance testing, and security scans to detect any anomalies that could indicate tampering or residual damage. The software verification verifies that all systems are updated to the latest secure versions and that all security patches are applied. This includes operating systems, applications, and utilities. The data validation ensures that all data restored from backups is complete and untampered. This involves for instance, checksum verifications,

hash comparisons, and, in some cases, manual review of critical data sets. Data validation ensures that no corrupt files have been reintroduced into the environment, which could potentially harbor elements of the ransomware.

In short, the following tests and verifications were identified:

- SI: Test the server and verify if it is capable of assuming its functions and is secure
- WI: Test the computer and verify if it is capable of assuming its functions and is secure
- DV: Verify if all needed data is in its place and available as needed
- AF: Verify if the application is working as it should

Eq. 4.4 denotes the components used to estimate the total duration of the third step. Besides the time needed (t) to do each test and verification, the formula has also into account the total number of Servers (n_S) and the total number of Workstations (n_W).

$$RT_3 = (t_{\mathrm{SI}} \times n_S) + ((t_{\mathrm{WI}} + t_{\mathrm{DV}} + t_{\mathrm{AF}}) \times (n_S + n_W)) \tag{4.4}$$

Chapter 5

Results and Discussion

This chapter presents some results obtained by estimating ransomware recovery times while using the proposed utility function. Next, some discussion is made regarding the proposed utility function and the obtained results.

5.1 Results

In this section, the function's effectiveness is evaluated in accurately estimating recovery costs across various organizational contexts. The results are discussed in detail, highlighting the findings and any unexpected outcomes that could influence future use or modifications of the utility function.

As stated earlier, three sample organizations, of different dimensions, were considered: A small organization with 10 workstations, a medium organization with 280 workstations, and a large organization with 5.800 workstations. For the sake of simplification, and considering that the Initial Recovery time (RT_1) is not dependent on the number of equipment, a duration of 24 hours (3 working days) was assumed. It was also assumed that none of the organizations had disaster recovery or used failover systems because it was intended to test the worst-case recovery scenario.

Table 5.1 shows not only the results obtained for the case where there are no backups but also the results obtained for the case where there are backups. The results show that, for a big organization without backups (worst case), the total recovery can take up to 63.932 hours. Such value implies a significant disruption in the operation of such an

Table 5.1: Total recovery time, per organization size, with and without backup (in hours)

	Small Org.			**Medium Org.**			**Large Org.**		
	No Bkp	**Bkp**	**Dif. %**	**No Bkp**	**Bkp**	**Dif. %**	**No Bkp**	**Bkp**	**Dif. %**
RT1 (DI+CE)	24:00	24:00	0	24:00	24:00	0	24:00	24:00	0
WA	77:10	54:10	30	2.160:40	1.516:40	30	44.756:40	31.416:40	30
SA	09:59	07:09	28	2.396:00	1.716:00	28	4.492:30	3.217:30	28
CV	00:00	00:00	0	00:00	00:00	0	146:00	123:20	16
ST	06:52	04:21	37	13:44	08:42	37	68:40	43:30	37
SE	00:00	00:00	0	26:16	16:40	37	3.940:00	2.500:00	37
NE	03:40	02:38	28	146:40	105:20	28	2.566:40	1.843:00	28
MD	00:00	00:00	0	955:00	750:00	21	00:00	00:00	0
PR	02:48	02:13	21	42:00	33:15	21	2.800:00	2.216:40	21
RT2	100:29	70:31	30	5.740:20	4.146:37	28	58.770:30	41.361:00	30
SI	01:00	01:00	0	240:00	240:00	0	450:00	450:00	0
WI	02:45	02:45	0	130:00	130:00	0	1.562:30	1.562:30	0
DV	02:45	02:45	0	130:00	130:00	0	1.562:30	1.562:30	0
AF	02:45	02:45	0	130:00	130:00	0	1.562:30	1.562:30	0
RT3	09:15	09:15	0	630:00	630:00	0	5.137:30	5.137:30	0
RT	133:44	103:46	22	6.394:20	4.800:37	25	63.932:00	46.522:30	27

organization. The results also show that having a good backup system also significantly reduces the total recovery time. For instance, when comparing medium-sized organizations, the total recovery time drops from 6.394 hours and 20 minutes to 4.800 hours and 37 minutes, a reduction of 1.593 hours and 43 minutes (24.92%).

As stated before, the enhancements allowed for the removal of RT1 and RT3 from the formula whenever the requirements of the number of workstations were met. This could allow for the simplification of the formula making it easier to calculate and to read.

Taking into account each of the use cases, the weight of each of the parts can be evaluated depending on company size as it can be seen in Table 4.1. This simplification allows for the removal of the parts of the formula that organizations find not relevant according to the weight of each of the parts.

5.2 Discussion

In this section, the implications of the utility function for organizations' planning and decision-making processes are examined. Also, it discusses how the function can be integrated into existing frameworks to enhance organizational resilience against ransomware attacks.

This utility function represents a new approach to the assessment of ransomware recovery costs. The function's design and refinement process was made by an analysis of existing challenges that organizations face during ransomware incidents. The integration of this utility function into current cybersecurity practices offers organizations a tool to prepare and respond to ransomware attacks by providing a clearer picture of potential financial impacts.

The research findings underscore the function's applicability across different organizational sizes and industries, demonstrating its versatility. For instance, the function's ability to adjust estimations based on various operational and environmental variables allows organizations to simulate different scenarios and plan their cybersecurity investments more effectively. This adaptability makes it a usable tool for risk management strategies, complementing existing cybersecurity frameworks which often lack a focused perspective on ransomware preparedness and recovery.

One of the key contributions of this utility function is its potential to influence decision-making within organizations. By providing a more accurate estimation of recovery times, the function helps decision-makers weigh the benefits and drawbacks of different cybersecurity investments and strategies. For example, the utility function can be used to justify the allocation of budget towards more robust backup solutions or advanced intrusion detection systems, which may otherwise seem unjustifiably expensive.

Moreover, the function's detailed breakdown of times can aid organizations in identifying which areas of their cybersecurity practices need strengthening. It also offers insights into the potential returns on investment for different recovery strategies, thereby supporting a more informed approach to managing ransomware risks.

The results of the utility function for ransomware recovery cost estimation, as detailed in earlier chapters, provide insights into the cost dynamics of ransomware impacts on organizations. This section interprets these results, exploring their significance in the context of cybersecurity risk management and organizational preparedness.

The utility function developed in this thesis has demonstrated its capacity to provide nuanced economic assessments, which is crucial for organizations facing the threat of ransomware. The function not only estimates the immediate time and costs associated with ransom payments and technical mitigation efforts but also allows for the quantification of

factors such as operational downtime, reputational damage, and potential legal liabilities. The interpretation of these results highlights the often-underestimated ransomware's economic impact. For instance, the function's ability to factor in reputational damage and its subsequent financial implications is particularly noteworthy. Reputation can significantly influence customer trust and investor confidence, which are critical to long-term organizational sustainability. By quantifying these aspects, the utility function allows organizations to see the potential long-term financial repercussions of ransomware attacks, extending beyond the immediate aftermath.

The results also underscore the strategic value of investing in proactive cybersecurity measures. Organizations that understand the potential cost implications of various ransomware scenarios can make more informed decisions about where to allocate resources to mitigate these risks. For example, the utility function's results can help justify the investment in advanced threat detection systems that may reduce the likelihood or impact of a ransomware attack. Moreover, these results serve as a crucial tool for cybersecurity training programs. By demonstrating the potential downtime of inaction, the utility function can be used to underscore the importance of employee training and compliance with security protocols, which are often the first line of defense against cyber threats.

The interpretation of these results can also have implications for policy-making. With a clearer understanding of the costs associated with ransomware attacks, policymakers can better advocate for stringent cybersecurity regulations and standards. For instance, the cost assessments provided by the utility function could inform the development of policies that mandate regular security audits and incident response drills for critical infrastructure sectors. Additionally, these results could influence the design of cyber insurance policies. Insurance providers could use the detailed breakdown of potential downtime to create more accurate risk assessment models, which in turn could lead to more tailored insurance products that better meet the needs of different types of organizations.

Finally, the results from the utility function align with the objectives of cybersecurity frameworks which aim to reduce the incidence and impact of attacks. Integrating the utility function into established frameworks like NIST can enhance these frameworks' effectiveness by providing a more concrete, quantitative tool for risk assessment and economic analysis. By interpreting these results within the context of cybersecurity management

practices, it becomes clear that the utility function is not only a tool for financial estimation but also an asset that can enhance overall organizational resilience.

The implications of this research extend beyond individual organizations to inform broader policy and regulatory considerations. Given the increasing prevalence of ransomware attacks, there is a growing need for policies that encourage the development and adoption of risk management tools such as the utility function proposed in this thesis.

Policymakers could use insights from this research to advocate for standards that require organizations to maintain a minimum level of preparedness for cyber incidents. Additionally, the cost assessments provided by the utility function could inform the creation of more effective cyber insurance products, which currently suffer from a lack of standardization and a clear understanding of risk profiles related to ransomware.

Chapter 6

Conclusion

This thesis presented a study on ransomware recovery practices across several organizations, with a focus on the variability of recovery times across different types of IT assets. Additionally, it proposes areas for future research that could further extend the utility of the ransomware recovery utility function or address new challenges presented in cybersecurity.

The work herein revealed that many of the inquired organizations have disaster recovery policies and redundant systems. However, in terms of deployment in case of a ransomware attack, there is a significant variability. Some organizations are capable of immediate fail-over or recovery but others need several hours to restore services. This assessment provided insight that was used for the development of a recovery utility function that estimates the time needed to recover from a ransomware attack. The variability of the obtained recovery times reinforces the need for an approach to estimating recovery times and costs.

The proposed utility function makes it clear that specific measures have a significant impact on the overall recovery time. Examples are the use of backups, or the ability to simultaneously reinstall multiple equipment. Such leads to the conclusion that by having such a utility function, organizations can better prepare themselves for a ransomware attack.

The work carried out demonstrates the complexity and difficulty of evaluating ransomware recovery times but also shows that the development of a recovery utility function can represent an innovative approach that enables organizations with a new mechanism

to test, forecast, and plan for the implications of a ransomware attack.

While the development of this utility function has demonstrated benefits, this research also opens several avenues for future work. Further refinement of the function could include the integration of machine learning techniques to dynamically update time estimations based on emerging trends in ransomware tactics and organizational vulnerabilities. Additionally, future research could explore the application of the utility function across multinational corporations to understand how cross-border regulatory environments impact ransomware recovery costs.

Exploring the psychological and cultural impacts of ransomware attacks on organizational behavior could also enhance the utility function's comprehensiveness. Such studies would provide a deeper understanding of the less tangible costs of ransomware incidents, potentially leading to more holistic cybersecurity strategies.

The ransomware continues to evolve, and the proposed utility function will need ongoing updates and refinements. Future research should focus on expanding the utility function's capabilities to include new cyber threats and recovery technologies. Moreover, further studies could explore the integration of this utility function into broader cybersecurity management frameworks, enhancing its practical utility and impact on organizational resilience.

References

[1] M. Alhanahnah et al. “Optimizing Ransomware Mitigation in Healthcare Sectors: A Cross-Layer Security Framework”. In: *Journal of Computer Security* 28.5 (2020), pp. 1–26. DOI: 10.3233/JCS-200056. URL: https://content.iospress.com/articles/journal-of-computer-security/jcs200056.

[2] Amjad Alraizza and Abdulmohsen Algarni. “Ransomware Detection Using Machine Learning: A Survey”. In: *Big Data and Cognitive Computing* 7.3 (2023). ISSN: 2504-2289. DOI: 10.3390/bdcc7030143. URL: https://www.mdpi.com/2504-2289/7/3/143.

[3] At-Bay. *Cyber Risk Calculators*. 2024. URL: https://www.at-bay.com/cyber-risk-calculators/ (visited on 10/30/2023).

[4] Ross Brewer. “Ransomware attacks: detection, prevention and cure”. In: *Netw. Secur.* 2016 (2016), pp. 5–9. DOI: 10.1016/S1353-4858(16)30086-1.

[5] BullWall. *Cost of Downtime Calculator*. 2024. URL: https://bullwall.com/cost-of-downtime/calculator-eur/ (visited on 10/30/2023).

[6] L. Cristea. “Current security threats in the national and international context”. In: *Journal of Accounting and Management Information Systems* (2020). DOI: 10.24818/jamis.2020.02007.

[7] Scarlett Cybersecurity. *How Much Ransomware Recovery Really Cost?* [Online; accessed 9-April-2024]. 2024. URL: https://www.scarlettcybersecurity.com/how-much-ransomware-recovery-really-cost.

[8] M. Al-Dwairi et al. “Ransomware-resilient self-healing xml documents”. In: *Future Internet* 14 (4 2022), p. 115. DOI: 10.3390/fi14040115.

[9] T. M. Fernandez-Carames and P. Fraga-Lamas. "A Review on the Use of Blockchain for the Internet of Things". In: *IEEE Access* 7 (2019), pp. 117059–117078. DOI: 10.1109/ACCESS.2019.2935192. URL: https://ieeexplore.ieee.org/document/8373692.

[10] Fortinet. *The 2023 Global Ransomware Report*. [Online; accessed 9-April-2024]. 2023. URL: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf.

[11] Julija Gavėnaitė-Sirvydienė and Algita Miečinskienė. "Forecasting costs of cyber attacks using the Global Cost of Cyber Risk Calculator V 1.2". In: *Contemporary Issues in Business, Management and Economics Engineering* 2021 (2021). DOI: 10.3846/cibmee.2021.618.

[12] J. Guo, H. Liang, and J. Long. "Leveraging file system characteristics for ransomware mitigation in linux operating system environments". In: (2024). DOI: 10.21203/rs.3.rs-4308346/v1.

[13] IBM. *Cost of a Data Breach Report 2024*. [Online; accessed 12-October-2024]. 2024. URL: https://www.ibm.com/reports/data-breach.

[14] Equipe Kaspersky. *How effective are security solutions against ransomware?* Oct. 2021. URL: https://www.kaspersky.com/blog/ransomware-protection-test-2021/42324/ (visited on 11/28/2024).

[15] Jabed Kumar. "Enhancing Public Awareness and Education of Ransomware Attacks". In: (Dec. 2023). DOI: 10.36227/techrxiv.24634806.v1. URL: http://dx.doi.org/10.36227/techrxiv.24634806.v1.

[16] McAfee Labs. *McAfee Labs Threats Report*. Tech. rep. Disponível em: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2019.pdf. McAfee, 2019. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2019.pdf.

[17] Nandita Pattnaik et al. "It's more than just money: The real-world harms from ransomware attacks". In: *ArXiv* abs/2307.02855 (2023). DOI: 10.48550/arXiv.2307.02855.

[18] Salwa Razaulla et al. “The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions”. In: *IEEE Access* 11 (2023), pp. 40698–40723. DOI: 10.1109/ACCESS.2023.3268535.

[19] B. Reidys, P. Liu, and J. Huang. “Rssd: defend against ransomware with hardware-isolated network-storage codesign and post-attack analysis”. In: *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems* (2022). DOI: 10.1145/3503222.3507773.

[20] Matthew Ryan. “Introduction”. In: *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*. Cham: Springer International Publishing, 2021, pp. 1–15. ISBN: 978-3-030-66583-8. DOI: 10.1007/978-3-030-66583-8_1. URL: https://doi.org/10.1007/978-3-030-66583-8_1.

[21] IT Security. *Ataques de ransomware a organizações governamentais diminui, mas custo de recuperação aumenta*. [Online; accessed 19-October-2024]. 2024. URL: https://www.itsecurity.pt/news/analysis/ataques-de-ransomware-a-organizacoes-governamentais-diminui-mas-custo-de-recuperacao-aumenta.

[22] Satyendra K. Sharma and Triveni Singh. “Ransomware : A Severe Cyber Security Threat in The Digital Era”. In: *International Journal of Scientific Research in Science and Technology* 6 (2019), pp. 211–218. DOI: 10.32628/IJSRST196120.

[23] Sophos. *Ransomware recovery costs vs. the ransom demands*. [Online; accessed 9-April-2024]. 2024. URL: https://www.ft.com/partnercontent/sophos/ransomware-recovery-costs-vs-the-ransom-demands.html.

[24] Fabian M. Teichmann and Sonia R. Boticiu. “The most impactful ransomware attacks in 2023 and their business implications”. In: *International Cybersecurity Law Review* 5.2 (June 2024), pp. 301–311. ISSN: 2662-9739. DOI: 10.1365/s43439-024-00115-3. URL: https://doi.org/10.1365/s43439-024-00115-3.

[25] Paulo Jorge da Silva Teixeira. “Evolutive Software Asset Management”. In: 2021. URL: http://hdl.handle.net/10400.22/19862.

[26] CFC Underwriting. *Ransomware Cost Calculator*. 2024. URL: https://www.cfc.com/en-gb/ransomware-calculator/ (visited on 10/30/2023).

[27] Sérgio Valente. “A ciberseguranca no contexto das pequenas e medias empresas portuguesas: um estudo sobre a consciencializacao e investimento na mitigacao do cibercrime”. In: 2022. URL: https://dspace.uevora.pt/rdpc/bitstream/10174/33107/1/Mestrado-Engenharia_Informatica-Sergio_Valente.pdf.

[28] Lena Yuryna Connolly et al. “An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability”. In: *Journal of Cybersecurity* 6.1 (Dec. 2020), tyaa023. ISSN: 2057-2085. DOI: 10.1093/cybsec/tyaa023. eprint: https://academic.oup.com/cybersecurity/article-pdf/6/1/tyaa023/35198032/tyaa023.pdf. URL: https://doi.org/10.1093/cybsec/tyaa023.