The impact of cyberattacks on the brand image of higher education institutions: the case study of the Polytechnic of Leiria

Master's degree in Cybersecurity and Digital Forensics

Maria Cipriano Espírito Santo

Leiria, April of 2026

The impact of cyberattacks on the brand image of higher education institutions: the case study of the Polytechnic of Leiria

Master's degree in Cybersecurity and Digital Forensics

Maria Cipriano Espírito Santo

Dissertation under the supervision of Professor Mário João Gonçalves Antunes and Professor Ana Catarina Cadima Lisboa

Leiria, April of 2026

Originality and Copyright

This dissertation is original, made only for this purpose, and all authors whose studies and publications were used to complete it are duly acknowledged.

Dedication

To my partner, André Fernandes, whose support and belief in me made this journey possible.

Acknowledgments

I would like to express my sincere gratitude to my supervisors, Mário Antunes and Ana Lisboa, for their guidance, support, and valuable insights throughout the development of this dissertation. Their expertise and constructive feedback were essential in shaping the direction and quality of this work.

I am also deeply grateful to Luís Cachulo and João Fraga, who kindly participated in this study. Their openness, technical expertise, and willingness to share detailed insights into the incident response process were fundamental to understanding the operational and cybersecurity dimensions of this research.

Furthermore, I would like to thank Alexandre Soares for his valuable contribution. His perspective on crisis communication, stakeholder engagement, and reputational management provided critical depth to the analysis and greatly enriched the interdisciplinary nature of this study.

Finally, I extend my appreciation to all those who, directly or indirectly, supported the completion of this dissertation.

Abstract

Cyberattacks have become a growing concern for higher education institutions, generating consequences that extend well beyond operational disruption into institutional reputation, stakeholder trust, and brand credibility. Despite this, the cybersecurity and brand management literatures have largely evolved in isolation from one another, leaving institutions without integrated frameworks for understanding and responding to ransomware incidents as both technical and reputational crises. This dissertation addresses that gap by exploring the impact of a ransomware attack on the brand image of a public higher education institution in Portugal, the Polytechnic Institute of Leiria.

Using a qualitative case study approach, the research combines semi-structured interviews with institutional stakeholders, document analysis, and media monitoring to assess both technical and reputational consequences of the May 2023 Akira ransomware incident.

The findings indicate that, although the attack exposed vulnerabilities in infrastructure and incident response planning, the institution's transparent communication strategy and timely coordination with national authorities contributed to mitigating reputational damage. The study further highlights the importance of integrating cybersecurity and crisis communication within institutional reputation management, particularly in academic environments where trust and public perception are critical.

In addition, the dissertation proposes practical recommendations to strengthen institutional resilience, including diversified backup strategies, enhanced stakeholder engagement, and cybersecurity awareness initiatives.

This research contributes to the emerging intersection of cybersecurity governance and institutional reputation management in higher education, offering insights for both academic literature and institutional practice.

Keywords: higher education, ransomware, cybersecurity, crisis communication, resilience, brand management

Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

BCP	Business Continuity Plan
CISO	Chief Information Security Officer
CNCS	National Cybersecurity Centre (in Portuguese, “Centro Nacional de Cibersegurança”)
CNPD	National Data Protection Commission (in Portuguese, “Comissão Nacional de Proteção de Dados”)
CSIRT	Computer Security Incident Response Team
DSI	Directorate of Information Systems
DPO	Data Protection Officer
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
HEI	Higher Education Institution
IPLeiria	Polytechnic Institute of Leiria (in Portuguese, “Instituto Politécnico de Leiria”
ISO	International Organization for Standardization
MFA	Multi-Factor Authentication
NIS2	Network and Information Security Directive 2
NIST	National Institute of Standards and Technology
PJ	Judicial Police (in Portuguese, “Polícia Judiciária”)
RaaS	Ransomware-as-a-Service
RDP	Remote Desktop Protocol
SCCT	Situational Crisis Communication Theory
SIEM	Security Information and Event Management
SOC	Security Operations Centre
VPN	Virtual Private Network
XDR	Extended Detection and Response

1. Introduction

The digital transformation of higher education has been swift and, in many respects, remarkable. Over the past two decades, higher education institutions (HEIs) have moved core functions such as teaching, administration, research collaboration, and student services onto interconnected digital platforms, gaining in efficiency what they sometimes lost in simplicity [1], [2]. For institutions whose mission depends on access, openness, and the free circulation of knowledge, this shift has been largely welcome.

The same openness that defines academic culture also creates vulnerability. HEIs manage vast quantities of sensitive data, including student records, financial information, research outputs and staff credentials, within environments that are structurally difficult to secure due to being decentralized, heterogeneous, and populated by large, transient user communities with widely varying levels of digital literacy [1], [3]. These conditions have made HEIs increasingly attractive targets for cybercriminals. Ransomware attacks, in particular, have emerged as a serious and growing threat as they encrypt institutional systems, threaten data exposure, and demand payment under conditions of acute operational pressure [3], [4].

The academic response to these challenges has been substantial but fragmented along disciplinary lines. On one side, a rich body of literature in information technology and cybersecurity has documented the technical dimensions of ransomware: attack vectors, encryption mechanisms, incident response frameworks, and the structural vulnerabilities specific to academic environments [1], [5], [6]. On the other side, the marketing and institutional management literature has developed detailed accounts of how organizations build and protect brand reputation, manage stakeholder perceptions during crises, and recover institutional legitimacy after disruptive events [7], [8], [9], [10]. These two bodies of work have largely evolved in parallel, with little conversation between them.

This separation is increasingly difficult to justify. In higher education, institutional reputation is inseparable from the trust stakeholders place in the institution's capacity to protect sensitive data and ensure service continuity [9], [11]. A cyberattack does not merely disrupt systems; it disrupts the intangible social contract between an HEI and its students, staff, partners, and public. Cybersecurity incidents are thus simultaneously IT failures and brand crises and understanding them fully requires integrating perspectives from both

domains. Yet few studies have done so systematically, and even fewer in the context of higher education [12], [13], [14].

This dissertation addresses that gap. Its central aim is to evaluate how a ransomware attack affected the brand image and institutional reputation of a public higher education institution in Europe, while accounting for both the technical and operational dimensions of the incident. The study pursues three specific objectives: to identify the operational and reputational consequences of the attack; to analyze the institution's technical response, crisis communication practices, and image recovery strategies; and to propose evidence-based recommendations for strengthening cyber resilience and reputational preparedness in HEIs. By bridging cybersecurity and brand management literature, the research contributes to an interdisciplinary understanding of how ransomware incidents unfold as institutional crises and how institutions can respond to both dimensions in an integrated way.

The empirical setting is the Akira ransomware attack that struck the Polytechnic Institute of Leiria (IPLeiria) in May 2023, causing widespread disruption to academic platforms, institutional email, and network connectivity, and requiring phased recovery over several weeks [15], [16]. The study adopts a qualitative case study design [17], drawing on semi-structured interviews with representatives from the Directorate of Information Systems and the Communication Department, supplemented by documentary and media analysis. This combination makes it possible to examine the incident from both the technical and reputational sides and, crucially, to explore how these two dimensions interacted during and after the attack.

Following this introductory chapter, the dissertation is structured as follows. Chapter 2 presents a comprehensive literature review addressing ransomware threats, cybersecurity resilience in higher education, and crisis communication and reputation management frameworks. Chapter 3 outlines the research methodology, detailing the case study design, data collection procedures, and ethical considerations. Chapter 4 presents the empirical case study of the IPLeiria ransomware attack, describing the incident, institutional response, and observed impacts. Chapter 5 discusses the findings in relation to the theoretical framework, focusing on both technical and reputational dimensions. Finally, Chapter 6 concludes the dissertation by synthesizing the main contributions, acknowledging limitations, and proposing directions for future research.

2. Literature Review

2.1. Cybersecurity in the Higher Education Sector

Cybersecurity has emerged as one of the defining governance challenges of the digital age. As organizations across all sectors have become increasingly dependent on interconnected digital systems, the threat landscape has expanded in both scale and sophistication, from opportunistic malware to coordinated, multi-stage attacks targeting critical infrastructure, financial systems, healthcare, and public institutions [3], [18], [19]. Cybersecurity can be broadly defined as the set of practices, technologies, and organizational processes designed to protect systems, networks, and digital assets from malicious attacks, unauthorized access, disruption, or misuse [19]. ISO/IEC 27032 extends this definition further, emphasizing that cybersecurity encompasses network resilience, operational continuity, and risk-based decision-making across complex and interconnected environments [20]. What these definitions share is a recognition that cybersecurity is no longer a purely technical domain – it is a strategic and governance concern for any organization that depends on digital infrastructure to function [12], [21].

Higher education institutions occupy a particularly exposed position within this landscape. Unlike most organizations, HEIs combine the data sensitivity of healthcare or financial services, managing student records, research data, intellectual property, and financial information, with the openness and decentralization characteristic of academic culture [22], [5]. Their digital environments typically feature open network architectures, heterogeneous device ecosystems, large and transient user populations with varying levels of security awareness, and limited centralized control over how systems are accessed and used [1], [2], [6]. These structural characteristics create an attack surface that is both unusually wide and unusually difficult to defend. As digital transformation accelerates across academic, administrative, and research activities, cybersecurity has become an essential dimension of institutional governance, risk management, and stakeholder trust, not an IT problem to be delegated but a strategic priority to be owned at leadership level [3], [12].

2.1.1. Vulnerability of Higher Education Institutions

HEIs are widely recognized as frequent targets of cyberattacks due to a combination of structural and operational vulnerabilities [2], [22]. Unlike corporate organizations, HEIs are

designed to promote accessibility, collaboration, and academic freedom, often resulting in networks that prioritize openness over strict control [1]. Students, staff, visiting researchers, and external partners routinely access institutional platforms through personal devices and unsecured networks, significantly expanding the attack surface [1], [2].

In addition, HEIs typically operate decentralized IT structures, where different departments may manage their own systems with varying security standards [1]. This fragmentation can hinder the consistent implementation of cybersecurity policies and increase exposure to vulnerabilities [2], [23]. Limited financial resources, particularly in public institutions, further constrain the ability to invest in advanced security technologies, dedicated cybersecurity staff, and continuous monitoring mechanisms [2], [22].

2.1.2. Sensitive Data and Strategic Value

HEIs also store substantial amounts of sensitive and valuable data, making them attractive targets for cybercriminals [1], [22]. This includes personal information about students and employees, financial records, intellectual property, and high-value research outputs [22]. According to [2], the education sector has experienced a sustained rise in attacks targeting credentials, research data, and institutional identity systems. Research HEIs may face threats from both financially motivated cybercrime groups and actors involved in espionage and geopolitical competition [22].

The compromise of such information can lead not only to operational disruption but also to legal consequences under frameworks such as the General Data Protection Regulation (GDPR), which imposes strict obligations regarding personal data breaches and notification requirements [24]. The reputational risks associated with failing to protect sensitive information are therefore substantial, especially in institutions whose legitimacy depends heavily on trust and credibility [25].

2.1.3. Common Threats in Academic Environments

Several forms of cyber threats are particularly prevalent within HEIs [1], [22]. Phishing remains one of the most common initial attack vectors, exploiting human behavior rather than technical weaknesses [22]. Academic communities are especially vulnerable due to frequent email communication, high turnover of users, and limited cybersecurity awareness among non-technical populations [2], [26].

Ransomware has emerged as one of the most disruptive threats facing HEIs worldwide [22]. Ransomware attacks encrypt critical institutional data and demand payment for decryption, often accompanied by threats of public data exposure [4], [27]. Such incidents can paralyze teaching platforms, administrative systems, and communication channels, creating immediate disruption and long-term reputational damage [28].

Data exfiltration is also increasingly observed in attacks against educational organizations, where stolen information may be sold, leaked, or used for further extortion. This trend [22] reflects the shift towards "double extortion" strategies in which attackers seek both financial gain and reputational leverage [4].

2.1.4. Notable Incidents in the Higher Education Sector

Recent high-profile cases demonstrate the severity of ransomware attacks in academic settings [22]. For example, Maastricht University suffered a ransomware attack in 2019 that severely disrupted operations and ultimately resulted in a ransom payment of approximately €200,000 [29]. Similarly, the University of California, San Francisco paid over $1 million following an attack that compromised critical medical research systems during the COVID-19 pandemic [30].

These cases highlight that cyberattacks against HEIs have consequences that extend beyond financial losses [1], [22]. Operational shutdowns, loss of institutional credibility, stakeholder anxiety, and media scrutiny can undermine the trust upon which higher education depends [8], [25]. As ransomware actors increasingly target HEIs, cybersecurity becomes inseparable from institutional resilience and reputation management [22], [31].

2.1.5. Regulatory Pressure and the Future of HEI Cybersecurity

The growing frequency of cyberattacks has led to increased regulatory attention [3], [18]. In Europe, the NIS2 Directive strengthens cybersecurity obligations for essential and important entities, potentially including higher education institutions depending on national transposition [32]. For European HEIs, this evolving regulatory landscape reinforces the urgency of developing robust incident response frameworks, business continuity planning, and integrated crisis communication strategies [3], [19].

In this context, cybersecurity must be understood not only as a technical defense function but also as a strategic institutional priority linked to governance, risk, reputation, and long-term resilience [12], [31].

2.2. Anatomy and Evolution of Ransomware Attacks

Ransomware has become one of the most significant and operationally disruptive forms of cybercrime affecting organizations globally [3], [18]. While early ransomware variants were relatively simplistic, contemporary ransomware operations have evolved into highly sophisticated campaigns combining advanced malware engineering, network intrusion techniques, and psychological extortion mechanisms [3], [4]. In higher education institutions, ransomware represents a particularly severe threat due to the sector's extensive attack surface, decentralized infrastructures, and dependence on continuous digital service availability [1], [2].

Ransomware is generally defined as a form of malicious software designed to deny access to data or systems, typically through encryption, while demanding a ransom payment in exchange for restoration [27]. Unlike other categories of malware that may prioritize stealth or long-term persistence, ransomware attacks are often designed to maximize immediate disruption and financial leverage [3], [33].

2.2.1. Evolution of Ransomware Threats

The development of ransomware has followed a clear trajectory of increasing complexity [3], [27]. Early ransomware attacks in the 1990s and early 2000s relied on basic lock-screen mechanisms and weak encryption [27], limiting their effectiveness. However, the emergence of strong asymmetric cryptography, anonymous payment systems such as Bitcoin, and increasingly professionalized cybercriminal ecosystems transformed ransomware into a profitable and scalable threat model [34].

Modern ransomware operations frequently function under a "Ransomware-as-a-Service" (RaaS) model, in which developers maintain ransomware toolkits and lease them to affiliates who conduct attacks in exchange for a share of profits [22], [35]. This division of labor mirrors legitimate software business models and has significantly expanded the number of actors capable of deploying sophisticated ransomware campaigns.

As ransomware has matured, attackers have also shifted from indiscriminate mass infections to highly targeted intrusions against organizations with greater financial capacity and higher reputational exposure, including HEIs, hospitals, and public institutions [4], [18]. Higher education institutions are particularly vulnerable due to their complex digital environments and the high availability requirements of academic operations [1], [2].

2.2.2. Technical Anatomy of a Ransomware Attack

Ransomware attacks typically unfold through multiple stages, resembling the structured phases of an advanced persistent threat (APT). These stages can be mapped to frameworks such as the Cyber Kill Chain or MITRE ATT&CK, highlighting that ransomware is rarely a single-event infection but rather a multi-step intrusion process [3], [36].

2.2.2.1. Initial Access Vectors

Attackers commonly gain entry into institutional environments through several technical pathways:

- **Phishing and Social Engineering:** Malicious emails remain one of the most frequent initial vectors, exploiting human vulnerabilities to deliver malware or harvest credentials [26].
- **Credential Theft and Reuse:** Compromised passwords, often obtained through data breaches or credential stuffing [18], provide access to privileged accounts and remote services.
- **Exploitation of Remote Services:** Misconfigured or exposed Remote Desktop Protocol (RDP), VPN gateways, and web-facing applications are regularly exploited as entry points [3], [28].
- **Supply Chain Compromise:** Attackers may infiltrate trusted third-party software providers, enabling lateral compromise across institutional networks [3].

In the context of higher education, remote access services are especially critical due to distributed campuses, hybrid work patterns, and international collaboration, increasing the opportunity for attackers to exploit weak authentication or exposed endpoints [1], [2].

2.2.2.2. Privilege Escalation and Lateral Movement

After gaining access, ransomware actors typically attempt to escalate privileges and move laterally within the network [35], [36]. This often involves:

- Harvesting administrator credentials from memory (e.g., LSASS dumping)
- Exploiting Active Directory weaknesses
- Using tools such as PsExec or remote management frameworks
- Identifying high-value systems such as file servers and backup repositories

This phase is essential because ransomware's impact depends heavily on the ability to encrypt shared resources and disrupt critical institutional infrastructure [27].

2.2.2.3. Encryption and System Impact

Once sufficient access is achieved, the ransomware payload is deployed to encrypt files across local and networked systems. Contemporary ransomware employs strong cryptographic algorithms [22], [27], typically combining:

- **Symmetric encryption** (e.g., AES) for rapid file encryption;
- **Asymmetric encryption** (e.g., RSA or ECC) to encrypt the symmetric key.

This hybrid approach ensures that victims cannot decrypt files without access to the attacker's private key, making recovery without backups extremely difficult [22].

Attackers frequently disable or delete recovery mechanisms [3], including:

- Volume shadow copies;
- System restoring points;
- Backup catalogues.

This demonstrates that ransomware is not merely a destructive malware but an operationally strategic tool designed to eliminate alternatives to ransom payment.

2.2.2.4. Double Extortion and Data Exfiltration

A major evolution in ransomware strategy has been the rise of "double extortion." In this model, attackers do not rely solely on encryption but also exfiltrate sensitive data before deployment, threatening to leak it publicly if payment is refused [3], [4].

This tactic significantly increases reputational damage, particularly for institutions responsible for safeguarding personal student data, confidential research, and financial information. In HEIs, the threat of exposure may extend beyond regulatory penalties to international reputational consequences, affecting partnerships and stakeholder confidence.

Some campaigns have escalated further into "triple extortion" [3], incorporating additional pressure mechanisms such as:

- Direct harassment of stakeholders;
- Secondary denial-of-service attacks;

- Media exposure campaigns.

Such developments illustrate that ransomware has increasingly become both a technical and psychological warfare instrument.

2.2.2.5. Akira Ransomware and Emerging Variants

The Akira ransomware strain, first widely observed in 2023, represents a contemporary example of advanced ransomware targeting medium-to-large organizations, including the education sector [34]. Akira campaigns are characterized by:

- Rapid lateral movement;
- Targeting of VPN credentials as an entry vector;
- Use of double extortion leak sites;
- High operational coordination.

Threat intelligence reports suggest that Akira operators frequently exploit compromised administrative accounts to accelerate encryption across multiple systems, maximizing institutional disruption and reputational pressure [34], [35].

The relevance of Akira to this dissertation lies not only in its technical impact but also in its reputational dimension. By leveraging threats of data exposure, Akira transforms ransomware from an availability attack into a broader crisis affecting public trust and organizational legitimacy.

2.2.2.6. Consequences of Ransomware for Institutional Resilience

The consequences of ransomware attacks extend beyond immediate system outages. Direct technical effects include:

- Service disruption and downtime;
- Loss of access to institutional platforms;
- Infrastructure rebuilding costs;
- Incident response resource exhaustion [3].

Indirect consequences include:

- Regulatory liabilities under GDPR;
- Erosion of stakeholder trust;

- Long-term reputational harm; and
- Strategic governance pressures [8], [12].

For HEIs, ransomware incidents may disrupt teaching schedules, impair research continuity, delay administrative services, and create uncertainty among domestic and international students. These effects demonstrate that ransomware is not solely a technical phenomenon but an institutional crisis event requiring integrated operational, communicational, and reputational response mechanisms.

In conclusion, understanding the anatomy and evolution of ransomware attacks is essential for analyzing how institutions such as IPLeiria experience not only technical disruption but also broader brand and trust-related challenges. The next section explores how these cyber incidents translate into organizational reputation crises and influence institutional brand image over time.

2.3. The Impact of Cyberattacks on Brand and Reputation

Cyberattacks are increasingly recognized not only as technical security incidents but as organizational crises capable of producing consequences that extend well beyond system disruption. In the broader organizational literature, data breaches and ransomware incidents have been shown to erode stakeholder trust, damage brand credibility, and generate lasting reputational harm, effects that persist long after technical recovery is complete [8], [13], [21]. Research confirms that the way an organization responds to a cyber incident matters as much as the incident itself: transparency, speed, and evidence of control are consistently associated with better reputational outcomes, while silence or perceived incompetence amplifies damage [8], [37]. Cybersecurity incidents must therefore be understood as multidimensional events, combining operational disruption with symbolic consequences for institutional credibility that unfold in the eyes of customers, partners, regulators, and the public simultaneously [3], [38].

For higher education institutions, these dynamics are particularly acute. HEIs derive their institutional legitimacy from trust and the confidence of students, staff, research partners, and funding bodies that the institution is competent, responsible, and reliable [9], [25]. A cyberattack that disrupts core services or compromises sensitive data challenges that trust directly and publicly, often attracting media attention and stakeholder scrutiny at a moment when the institution is least equipped to respond [1], [5]. Unlike commercial organizations,

where reputational damage may primarily manifest in customer behavior or share price, in HEIs it can affect student enrolment, research partnerships, regulatory relationships, and the institution's broader standing within the academic community. The reputational dimension is therefore not a secondary layer added to a technical event, it is an integral part of how the crisis unfolds and how fully the institution recovers [8], [12].

2.3.1. Brand Image and Reputation in Higher Education

An institution's brand represents the values, identity, and promises associated with its name, shaped over time through consistent performance, stakeholder experiences, and public perception [7], [39]. In higher education, brand image carries strategic weight: it influences student recruitment, research partnerships, funding prospects, and an institution's capacity to compete in an increasingly global academic marketplace [9], [40], [41]. Unlike commercial brands, which are primarily defined through transactions and marketing communications, HEI brands are socially constructed, built on perceptions of academic quality, ethical conduct, service reliability, and the lived experience of students and staff [11], [42]. Students do not merely consume a service; they relate to their institution, and that identification shapes how they perceive and respond to events that affect it [42], [43].

Reputation, as distinct from brand image, reflects the accumulated external judgement of an institution over time – the aggregate of what stakeholders believe about its competence, integrity, and reliability based on its past behavior [7], [10]. Research on HEI reputation consistently identifies stakeholder engagement, media coverage, public perception, and demonstrated service continuity as the primary drivers of reputational standing [10], [44]. These factors are not merely symbolic as reputational strength translates directly into enrolment levels, international attractiveness, and crisis resilience and the capacity to absorb disruptive events without lasting damage to institutional standing [25], [45].

This is precisely where cybersecurity becomes a brand and reputation issue, not just a technical one. HEIs are expected to provide safe learning environments, protect sensitive personal and research data, and ensure continuity of essential services [2], [22]. When a cyberattack disrupts those expectations visibly, publicly, and often with media amplification, it does not simply create an operational problem, it creates a reputational signal that the institution may not be as competent, prepared, or trustworthy as stakeholders assumed [8], [14]. Even when the institution is unambiguously a victim of external criminal activity,

perceptions of inadequate preparedness or opaque communication can shift stakeholder assessments of institutional responsibility [8], [13].

2.3.2. Cyberattacks as Reputational Crises

Cybersecurity incidents can generate reputational crises through several interrelated mechanisms [3], [8]. First, service disruption may create immediate operational frustration among students and staff, affecting perceptions of institutional competence [8]. Second, data breaches raise concerns about privacy and regulatory compliance, particularly under legal frameworks such as GDPR [21], [24]. Third, media coverage and online discourse can amplify negative narratives, turning a technical failure into a public crisis [8], [38].

Reputational harm is often among the most severe long-term consequences of cyber incidents, frequently surpassing direct financial loss [3], [13]. This is especially relevant in HEIs, where trust plays a central role in institutional identity and stakeholder commitment.

Furthermore, HEIs may experience heightened reputational vulnerability because they are often perceived as guardians of sensitive research, innovation, and student welfare [1], [22]. A ransomware attack that disrupts learning platforms, compromises email systems, or threatens exposure of confidential research may create perceptions of institutional weakness that persist beyond technical recovery [8].

[1] also highlight that HEIs may underreport incidents due to fear of reputational consequences, which can reduce transparency and limit sector-wide learning. This creates a paradox in which institutions attempt to protect their reputation through silence, yet risk greater damage if stakeholders perceive concealment or delayed communication [8]. Recent analysis of cyber incidents in UK higher education institutions reinforces this pattern, identifying limited disclosure of attack details as a major structural concern that hinders institutions' ability to assess vulnerabilities and respond effectively [5]. The tension between reputational protection and institutional transparency represents a challenge particularly acute in the higher education sector.

2.3.3. Stakeholder Trust and Perceived Institutional Responsibility

Trust is one of the most important mediating variables between cyber incidents and reputational impact [7]. Stakeholders evaluate institutions not only based on whether an attack occurred, but also on how the institution responds [8]. Research in organizational

crisis management suggests that effective response strategies depend on transparency, accountability, empathy, and evidence of control [8].

In HEIs, key stakeholder groups include:

- students (particularly international students dependent on digital communication);
- academic staff and researchers;
- administrative employees;
- government regulators and funding bodies;
- partner institutions and industry collaborators.

A cyberattack may generate distinct concerns across these groups: students may fear disruption and data exposure, researchers may worry about intellectual property theft, and regulators may focus on compliance failures [3], [25]. As a result, reputational impact is not uniform but socially distributed across multiple audiences [25].

2.3.4. Measuring Reputational Damage After Cyberattacks

Reputation is inherently difficult to quantify, but both qualitative and quantitative indicators can be used to assess reputational impact and recovery progress [7], [25]. Existing literature proposes several metrics commonly applied in crisis contexts, including public sentiment analysis, stakeholder surveys, enrolment trends, and media framing [8], [25].

In the context of higher education institutions, reputational damage may manifest across several observable dimensions affecting stakeholders, institutional performance, and public perception. Table 1 [8], [13], [25] summarizes key indicators relevant to evaluating reputational consequences of cyberattacks in HEIs.

Table 1 – Indicators of Reputational Impact of Cyberattacks in Higher Education Institutions

Indicator Category	Example Measures	Relevance to HEIs
Media Coverage	Volume and tone of news reporting; crisis framing	Influences public perception and institutional legitimacy
Social Media Sentiment	Positive/negative stakeholder reactions; misinformation spread	Particularly relevant for student communication and rapid narrative shifts
Stakeholder Trust	Surveys of student and staff confidence; partner reassurance	Reflects perceived reliability and institutional credibility

Operational Continuity	Duration of service disruption; impact on teaching and administration	Strongly affects student experience and satisfaction
Regulatory Response	GDPR breach notifications; investigations by authorities	Signals accountability and governance maturity
Long-Term Institutional Attractiveness	Changes in applications, enrolments, partnerships	Indicates whether reputational damage persists beyond recovery

These indicators provide a structured basis for examining not only immediate reputational disruption but also long-term institutional consequences, particularly in cases where trust recovery requires sustained engagement [8], [25].

2.3.5. Reputation Repair and Image Recovery Strategies

Post-incident reputation recovery depends on both technical remediation and symbolic reassurance [8], [25]. Institutions must demonstrate that vulnerabilities have been addressed while simultaneously communicating stability and responsibility [46]. Strategies commonly associated with image repair include [3], [46]:

- proactive disclosure and transparency;
- collaboration with law enforcement and cybersecurity authorities;
- visible investments in improved security controls (e.g., MFA, CSIRT);
- stakeholder engagement through regular updates and support;
- longer-term cybersecurity awareness initiatives.

Empirical research demonstrates that the timing and type of response strategy significantly affect stakeholder outcomes after a data breach, with prompt and transparent communication associated with better trust recovery [8], [37]. In HEIs, where institutional reputation is deeply tied to public mission and student welfare, communication must be carefully adapted to diverse audiences and expectations [9], [11].

Ultimately, cyberattacks highlight that cybersecurity is no longer purely an IT function but a central component of brand integrity and reputational resilience [3], [12]. The reputational stakes associated with ransomware, particularly under double extortion models, reinforce the need for integrated institutional strategies combining technical preparedness with crisis communication governance [3], [4].

The next section explores crisis management models and cyber resilience frameworks, providing the theoretical foundation for assessing organizational response effectiveness in cyber crisis situations.

2.4. Crisis Management Models and Cyber Resilience

Cyberattacks, particularly ransomware incidents, represent not only technical security failures but also organizational crises that require structured management across multiple dimensions [3], [8]. In the context of HEIs, such crises affect not only infrastructure availability but also institutional legitimacy, stakeholder trust, and brand reputation [25]. Effective response therefore depends on the integration of both cyber incident response frameworks and crisis communication strategies [19], [46].

Crisis management literature emphasizes that crises are characterized by high uncertainty, time pressure, and the potential for reputational harm [8], [38]. In cyber contexts, the disruptive nature of ransomware, combined with the threat of data exposure, means that institutions must respond simultaneously at technical, organizational, and communicational levels [3], [8].

2.4.1. Crisis Communication Theory and Organizational Reputation

One of the most influential frameworks in crisis communication research is the Situational Crisis Communication Theory (SCCT) developed by [8]. SCCT argues that an organization's reputational risk depends largely on stakeholder perceptions of responsibility. Stakeholders assess whether the organization is a victim of external circumstances, partially responsible due to negligence, or fully responsible due to preventable failures [8].

SCCT classifies crisis types into three broad categories:

- **Victim crises**, where the organization is primarily viewed as a target (e.g., terrorism or external cybercrime);
- **Accidental crises**, where harm results from unintentional operational failures;
- **Preventable crises**, where organizational negligence or misconduct is perceived [8].

Cyberattacks such as ransomware often fall within the "victim crisis" category, yet perceptions may shift if stakeholders believe that the institution lacked adequate security controls or preparedness. Therefore, even when an institution is attacked externally,

reputational damage can be intensified if stakeholders perceive poor governance or insufficient response planning [3], [8].

SCCT also emphasizes that crisis response should prioritize three key communication objectives:

- **Providing instructing information** (what stakeholders should do immediately);
- **Providing adjusting information** (psychological reassurance and empathy);
- **Protecting organizational reputation** through corrective action and transparency [8], [46].

In HEIs, this may involve informing students about service disruptions, reassuring staff regarding data protection measures, and communicating the steps taken to restore systems and prevent recurrence [1], [2].

2.4.2. Cyber Incident Response Frameworks and Organizational Preparedness

While crisis communication focuses on perception and reputation, cybersecurity literature highlights the importance of structured technical response [3], [19]. Cyber resilience depends on institutions having formalized incident response processes aligned with recognized frameworks and standards [3], [12].

NIST guidance on incident response defines it as a continuous lifecycle encompassing preparation, detection and analysis, containment, eradication, recovery, and post-incident improvement. This framework reflects the technical reality of ransomware incidents, which require rapid containment, system isolation, evidence preservation, and recovery planning [19].

Similarly, ISO/IEC 27035 provides an international standard for information security incident management, emphasizing governance, coordination, documentation, and continuous improvement [3], [47]. These frameworks demonstrate that incident response is not solely an operational IT task but an institutional governance function requiring leadership oversight and interdepartmental collaboration.

In higher education, incident response is often complicated by decentralized infrastructures, limited cybersecurity budgets, and open network cultures, reinforcing the importance of formal crisis management procedures [1], [2].

2.4.3. Business Continuity and Cyber Resilience

Cyber resilience refers to an organization's ability not only to prevent cyber incidents but also to sustain operations and recover effectively when attacks occur [12], [22]. Resilience therefore extends beyond immediate response to include organizational learning, redundancy planning, and long-term adaptive improvement [3], [19].

A critical component of resilience is the existence of a Business Continuity Plan (BCP) and disaster recovery capabilities. BCP frameworks ensure that institutions can maintain essential functions during disruptions, for example through offline alternatives, backup systems, and redundant infrastructure [19], [48].

Ransomware attacks frequently target backup repositories, making resilience dependent on diversified backup strategies such as the "3-2-1 rule" (three copies of data, stored across two media types, with one offline copy). These practices reduce institutional dependence on ransom negotiation and support rapid restoration of critical services [3], [4].

For HEIs, resilience is particularly important because digital infrastructure supports core academic functions, including learning management systems, student services, research platforms, and international communications [1], [2].

2.4.4. Integrating Crisis Communication and Cyber Incident Response

The interdisciplinary nature of ransomware crises requires institutions to align technical response actions with reputational and stakeholder-facing communication [3], [8]. A purely technical recovery may fail to restore trust if stakeholders perceive confusion, silence, or lack of transparency [8]. Conversely, strong communication without operational control may undermine credibility if services remain unavailable [46].

Effective crisis management therefore involves coordination between IT leadership, institutional governance, legal authorities, and communication departments [3], [19]. Cyber crises highlight the need for integrated socio-technical response structures, such as Computer Security Incident Response Teams (CSIRTs) that work alongside crisis communication stakeholders [12], [22].

Table 2 [8], [19] summarizes how technical incident response phases align with crisis communication objectives derived from incident response frameworks and crisis communication theory [8], [19].

Table 2 – Alignment of Cyber Incident Response Phases with Crisis Communication Priorities

Incident Response Phase	Technical Objective	Communication Priority (SCCT)	Example in HEIs
Preparation	Policies, training, backups, IR plans	Reputation building through readiness	Awareness campaigns, MFA implementation
Detection and Analysis	Identify attack vector and scope	Early transparency and situational updates	Inform community of disruption without panic
Containment	Isolate systems, prevent spread	Instructing information (what users must do)	Password resets, shutdown announcements
Eradication and Recovery	Restore systems securely	Corrective action and reassurance	Phased service return with stakeholder updates
Post-Incident Learning	Strengthen controls, document lessons	Reputation repair and renewal strategies	Public commitment to improved cyber resilience

This alignment demonstrates that ransomware crises require institutions to manage both "system recovery" and "trust recovery" simultaneously [3], [8].

2.4.5. Crisis Management in Higher Education Contexts

HEIs face unique challenges in crisis management [1], [2]. Academic institutions depend heavily on decentralized access, collaborative environments, and large transient user populations, making strict security enforcement difficult [1]. Additionally, HEIs operate under public accountability expectations, meaning that cyber incidents can attract significant media and governmental scrutiny [1], [3].

Crisis communication in HEIs must also address diverse stakeholder groups, including students, parents, researchers, staff, authorities, and international partners [9], [25]. The reputational implications of cyberattacks therefore extend beyond operational downtime, influencing institutional attractiveness and long-term credibility [8].

Ultimately, ransomware incidents illustrate that cybersecurity preparedness cannot be separated from crisis governance and institutional reputation [3], [12]. Crisis communication frameworks such as SCCT provide tools for managing stakeholder expectations [8], while technical models such as NIST and ISO/IEC 27035 provide structured response mechanisms [19], [47]. Together, these perspectives enable a holistic understanding of cyber resilience in higher education.

The following section explores resilience not only as recovery, but also as organizational learning and cultural transformation following cyber crises [22].

2.5. Cyber Resilience and Institutional Learning in Higher Education

The increasing frequency and sophistication of cyberattacks has shifted organizational priorities from a narrow focus on prevention towards a broader emphasis on cyber resilience [3], [12]. In ransomware incidents, where breaches may occur despite security controls, institutional success is often determined not only by defensive strength but by the capacity to respond, recover, and adapt [19], [22]. For HEIs, resilience is particularly critical because digital infrastructure supports essential educational and administrative functions, while stakeholder trust forms a central pillar of institutional legitimacy [1], [2].

Cyber resilience can be defined as an organization's ability to maintain or rapidly restore critical operations during and after cyber disruptions while continuing to evolve and improve its defensive posture [22]. Unlike traditional cybersecurity approaches, which prioritize risk avoidance and perimeter defense, resilience frameworks acknowledge that cyber incidents are increasingly inevitable and require systemic preparedness [3].

2.5.1. Resilience Beyond Technical Recovery

A key distinction in contemporary literature is that resilience extends beyond technical restoration [12], [22]. While recovery involves returning systems to operational status, resilience includes organizational capacity for continuity, governance coordination, and long-term improvement [3], [12]. In ransomware contexts, resilience is often tested by the simultaneous loss of availability, disruption of communication channels, and the reputational exposure created by extortion threats [3], [4].

HEIs face challenges in achieving resilience due to structural and cultural characteristics [1]. HEIs typically operate decentralized IT environments, open-access networks, and heterogeneous user populations, which complicate uniform security enforcement and increase susceptibility to phishing, credential compromise, and lateral movement [1], [3]. As a result, resilience strategies in academia must account not only for infrastructure complexity but also for behavioral risk and institutional governance maturity [12].

2.5.2. Business Continuity and Adaptive Preparedness

Cyber resilience is closely linked to business continuity planning and disaster recovery readiness [22], [48]. Business continuity refers to an institution's capacity to sustain essential operations during disruptive events, including cyber crises [19], [48]. In HEIs, this may include maintaining access to learning platforms, student support systems, financial services, and internal communications [1], [2].

Literature emphasizes that institutions with tested contingency plans, redundant infrastructure, and diversified backup architectures tend to recover more effectively from ransomware incidents [3], [4]. Conversely, organizations without formal continuity planning may be forced into improvised recovery efforts, increasing downtime and reputational vulnerability [3].

Resilience is therefore increasingly viewed as an institutional governance responsibility rather than solely a technical IT function [12]. Cybersecurity investment, policy formalization, executive awareness, and crisis preparedness all contribute to organizational stability under attack conditions [22].

2.5.3. Organizational Learning After Cyber Crises

A central dimension of resilience is the capacity for organizational learning following cyber incidents [12], [22]. Cyberattacks frequently expose gaps not only in technical controls but also in communication workflows, policy governance, and institutional risk perception [3]. Post-incident reflection can therefore act as a catalyst for transformation and institutional improvement [22].

Organizational learning in cybersecurity contexts often includes several institutional improvements [19], [22], such as:

- the formalization of security policies and response procedures;
- implementation of new technical safeguards (e.g., MFA, network segmentation);
- revision of backup strategies;
- strengthening coordination with external authorities and partners;
- expanded cybersecurity awareness training.

Such improvements represent what crisis scholars describe as "renewal," where crises generate opportunities for institutional development rather than solely loss [8], [46]. In HEIs,

where digital transformation continues to accelerate, crisis-driven learning can contribute significantly to long-term resilience and reputational credibility [3], [25].

2.5.4. Cybersecurity Culture and Human Factors

Resilience also depends heavily on institutional culture [12]. Many ransomware incidents begin not through advanced technical exploitation but through human factors such as phishing susceptibility, weak password practices, or misconfigured access privileges [3], [26]. HEIs, with large and diverse user groups, are especially exposed to these risks [1].

A growing body of literature highlights the importance of fostering a cybersecurity-aware culture through continuous training, simulated phishing campaigns, and staff/student engagement initiatives [2], [22]. Awareness programs are most effective when cybersecurity is framed as a shared institutional responsibility rather than a specialized technical concern [12].

In this sense, cyber resilience becomes inseparable from stakeholder communication and trust-building [8], [25]. Institutions that demonstrate proactive improvement and transparent learning after cyber incidents may reinforce their reputational standing as responsible and adaptive organizations [25], [46].

2.5.5. Resilience as a Component of Institutional Reputation

In higher education, resilience has reputational implications [3], [25]. Stakeholders do not expect institutions to be immune to cybercrime, but they increasingly evaluate how institutions respond, communicate, and improve after crises [8]. Institutions that demonstrate preparedness, transparency, and learning-oriented governance may preserve trust more effectively than those perceived as disorganized or silent [8], [37].

Cyber resilience therefore functions as both an operational requirement and a reputational asset [12], [22]. Ransomware incidents reveal that cybersecurity maturity influences institutional credibility, especially in environments where trust is central to educational mission and public responsibility [9], [11].

Ultimately, the concept of cyber resilience provides a critical bridge between technical cybersecurity frameworks and institutional brand management [12]. HEIs must increasingly adopt integrated strategies that combine infrastructure preparedness, crisis communication capacity, and long-term cultural change [22], [46].

The following section consolidates the theoretical insights presented in this chapter and identifies the research gap addressed by the present dissertation, leading to the conceptual framework guiding the IPLeiria case study.

2.6. Research Gap and Conceptual Framework

The previous sections have demonstrated that ransomware attacks have become a critical threat to HEIs, producing severe operational disruption and increasingly significant reputational exposure [3]. Literature has advanced substantially in explaining the technical evolution of ransomware, the institutional vulnerabilities of academic environments, and the growing importance of cyber resilience frameworks [1], [22]. At the same time, crisis communication theory provides well-established models for understanding how organizations manage stakeholder perceptions and reputational risk during disruptive events [8].

However, despite these contributions, important gaps remain in the academic understanding of ransomware incidents within HEIs, particularly when viewed through an interdisciplinary lens combining cybersecurity and institutional brand management.

2.6.1. Research Gap

A first gap concerns the limited number of empirical studies examining cyberattacks in the higher education sector from a reputational and communication perspective. While cybersecurity research has extensively documented the technical impact of ransomware, such as encryption mechanisms, access vectors, and recovery challenges [1], [5], [6], fewer studies explore how these incidents influence trust, legitimacy, and organizational image in academic settings. Where reputational consequences are addressed, they tend to be treated as secondary outcomes of technical failure rather than as analytically distinct dimensions requiring dedicated investigation [1], [13]. This asymmetry between the technical and reputational strands of the literature represents a significant gap, particularly given that trust and credibility are among the most strategically important assets an HEI holds.

A second gap lies in the insufficient integration of cybersecurity incident response literature with frameworks of brand and reputation management. Reputation in higher education is an intangible yet strategically vital asset, influencing student recruitment, stakeholder loyalty, research partnerships, and international credibility [7]. Ransomware attacks increasingly exploit this reputational dimension through double extortion tactics [3], [4], meaning that

cyber incidents must be analyzed not only as technical disruptions but also as crises of institutional identity and trust. Nevertheless, academic research often treats cybersecurity and brand management as separate domains, limiting holistic understanding.

A third gap is the scarcity of qualitative, context-specific case studies focusing on ransomware crises within Southern European higher education institutions. Much of the available literature and incident analysis originates from North American or Northern European contexts, where governance structures, regulatory maturity, and institutional resources may differ significantly. As Portugal prepares for the full implementation of the NIS2 Directive, which strengthens cybersecurity obligations across sectors, understanding how national HEIs experience and respond to cyber crises becomes especially timely [32].

2.6.2. Contribution of This Study

In response to these gaps, this dissertation contributes to the emerging interdisciplinary field at the intersection of cybersecurity governance and institutional reputation management. By integrating technical incident response analysis with crisis communication theory and brand management frameworks, the study advances understanding of how ransomware attacks function simultaneously as operational crises and reputational crises in academic environments and how institutions can respond to both dimensions in an integrated way. A real-world ransomware incident affecting a European public higher education institution serves as the empirical setting through which these dynamics are examined.

The dissertation therefore provides:

- a theoretically grounded and empirically informed analysis of the multidimensional consequences of ransomware attacks in higher education, spanning technical, operational, and reputational dimensions;
- an interdisciplinary contribution bridging cybersecurity incident response literature with crisis communication and institutional brand management theory;
- practical recommendations for strengthening cyber resilience and reputational preparedness in HEIs, with broader transferability to similar institutional contexts across Europe.

2.6.3. Conceptual Framework Guiding the Case Study

To structure the empirical analysis, this study adopts a conceptual framework that integrates three interconnected dimensions highlighted throughout the literature review:

A. **Cybersecurity Incident and Operational Disruption** – This dimension draws on cybersecurity incident response frameworks, particularly the NIST lifecycle model [19] and ISO/IEC 27035 [47], as well as sector-specific vulnerability research in higher education [1], [5]. It encompasses the technical and operational consequences of a ransomware attack, including service downtime, infrastructure compromise, data exposure, and recovery complexity.
B. **Institutional Crisis Response and Communication Strategy** – This dimension is grounded in Situational Crisis Communication Theory [8] and crisis management literature [38]. It examines how organizations respond to disruptive events through both technical containment and stakeholder-facing communication, and how the quality of that response shapes subsequent perceptions of institutional competence and transparency.
C. **Reputational Impact and Brand Trust Outcomes** – This dimension draws on reputation theory [7], [25] and HEI brand management research [9], [10]. It addresses how the interaction between operational disruption and institutional response influences stakeholder trust, institutional legitimacy, and longer-term brand standing.

These three dimensions are not sequential but interdependent; technical response shapes communication possibilities, communication shapes stakeholder perception, and stakeholder perception determines whether reputational recovery is achievable. The framework reflects the central argument of this dissertation: that cyber resilience in higher education depends not only on restoring systems but on restoring confidence, and provides the analytical structure through which the empirical case study is examined in Chapters 4 and 5.

2.7. Chapter Summary

In summary, Chapter 2 has established the theoretical foundation for understanding ransomware as both a cybersecurity threat and a reputational crisis in higher education. The literature indicates that HEIs face distinct vulnerabilities due to open infrastructures and stakeholder diversity, while crisis communication and resilience frameworks are essential for preserving institutional trust.

The identified research gap highlights the need for more integrated and context-specific analysis of ransomware incidents in academia. The conceptual framework presented above provides the analytical structure for examining the empirical case study, which is introduced in the following chapter through the methodological approach and data collection strategy.

3. Methodology

3.1. Research Design and Approach

This dissertation adopts a qualitative, exploratory research design to examine how a ransomware incident can affect the brand image and reputation of a higher education institution. The study is positioned at the intersection of cybersecurity incident response and organizational reputation management, an area where perceptions, meanings, and stakeholder interpretations are central to understanding the impact. A qualitative approach is therefore appropriate, as it allows the researcher to capture contextual detail and nuanced viewpoints that may not be visible through purely quantitative measures [49].

The research is structured as a single-case study of a ransomware incident affecting a public higher education institution in Europe. Case study research is particularly suitable when investigating contemporary events within real-life contexts, especially where the boundaries between the phenomenon and its context are not clearly defined [17]. In this instance, the operational disruption caused by the attack, the institutional response, and the communication dynamics that followed are deeply interdependent, all conditions that reinforce the relevance of an in-depth case study design over survey-based or experimental approaches. Primary data were collected through semi-structured interviews with institutional stakeholders directly involved in both the technical response and the communication management of the incident, supplemented by documentary and media sources to enable triangulation.

The dissertation is exploratory in nature, not seeking statistical generalization but rather aiming for analytical generalization, whereby the findings are interpreted in relation to relevant theories and prior research on crisis communication, reputation, and cyber resilience [17]. The intention is to generate insights and recommendations that may be transferable to similar HEIs facing comparable threats, while acknowledging contextual differences across institutions and countries.

3.2. Case Study Selection and Context

The empirical setting for this dissertation is the Polytechnic Institute of Leiria, a public higher education institution in Portugal and one of the largest polytechnic institutions in the

Iberian Peninsula, serving approximately 14,000 students across five campuses. In May 2023, IPLeiria was the target of an Akira ransomware attack that caused widespread disruption to its digital infrastructure, affecting institutional email, academic platforms, student portals, and network connectivity. The incident required phased service recovery over several weeks and attracted significant national media coverage that documented the operational disruption and the institution's response [15], [16]; a selection of representative press coverage is provided in Appendix B, illustrating the breadth and tone of public reporting during the incident period. IPLeiria issued public communications acknowledging the attack, coordinating with national cybersecurity authorities, including the National Cybersecurity Center (CNCS), and providing stakeholder updates throughout the recovery period.

IPLeiria was selected as the research setting for this study for four interconnected reasons that are briefly described below:

- First, it represents a European public HEI operating under governance and regulatory conditions, including GDPR and NIS directives, that are directly relevant to the broader research questions addressed in this dissertation.
- Second, the scale and nature of the May 2023 incident provide a substantive empirical basis for examining both the technical and reputational dimensions of a ransomware crisis, including detection challenges, infrastructure damage, backup compromise, and communication under uncertainty.
- Third, the public visibility of the incident through media coverage, institutional communications, and online stakeholder discourse enables triangulation across multiple secondary sources, strengthening the credibility of the analysis.
- Fourth, the researcher's proximity to the institutional context facilitated access to key stakeholders and internal documentation, supporting the depth and feasibility of the study while also requiring reflexive awareness of potential bias, which is addressed in section 3.6.

Taken together, these characteristics make IPLeiria a particularly suitable critical case exploring how a European public HEI experiences and manages a major ransomware incident.

3.3.Data Collection Methods

To address the research objectives, the study draws on multiple sources of evidence, combining primary and secondary data. This multi-source strategy supports triangulation, strengthening the credibility of findings by comparing and cross-validating evidence from different perspectives and formats [17].

3.3.1. Primary Data: Semi-Structured Interviews

Primary data were collected through two semi-structured interviews conducted in Portuguese via Microsoft Teams with institutional stakeholders directly involved in the incident response.

The selection of interviewees was deliberate and directly aligned with the interdisciplinary design of this study. Since the dissertation seeks to integrate two analytically distinct but complementary perspectives, cybersecurity incident response and institutional crisis communication, it was essential to collect data from representatives of both domains. The Directorate of Information Systems (DSI) holds primary responsibility for the technical management of the institution's digital infrastructure and led the operational response to the attack. The Communication Department, by contrast, was responsible for managing institutional messaging, stakeholder engagement, and reputational risk throughout the crisis. Together, these two profiles provide the dual-perspective evidence base required to examine how technical and communicative dimensions of a ransomware crisis unfold, interact, and jointly shape institutional outcomes. No other institutional roles were better positioned to speak to both sides of this intersection.

The interviews were therefore structured as follows:

- A joint interview with two members of the Directorate of Information Systems (DSI), focused on technical response, operational recovery, infrastructure damage, governance decisions, and lessons learned; and
- An interview with the Director of the Communication Department, focused on crisis communication strategy, reputational risk management, stakeholder engagement, and institutional messaging.

Conducting the interviews online allowed flexibility, ensured institutional accessibility, and enabled the researcher to engage directly with key stakeholders despite scheduling and operational constraints.

The interview scripts used for each stakeholder group were developed in advance based on the research objectives and the theoretical framework presented in Chapter 2. These scripts ensured consistency while allowing flexibility for follow-up questions and deeper exploration of emerging themes. The full interview guides are provided in Appendix A, allowing transparency and replicability of the research design.

Interviews are widely recognized as a particularly appropriate data collection method for exploratory qualitative research, where the goal is to develop an in-depth understanding of complex phenomena that are not yet well-documented in the literature [50], [51]. Unlike surveys or structured instruments, interviews allow researchers to access the perspectives, interpretations, and decision-making rationales of participants who have direct experience of the phenomenon under investigation [52], [53]. Given that the intersection of cybersecurity incident response and institutional reputation management in higher education remains empirically underexplored, an interview-based approach is well-suited to generating the contextual, nuanced evidence needed to advance understanding in this area.

Semi-structured interviews were selected because they provide a balance between consistency – ensuring alignment with the research objectives across both interviewees – and flexibility – allowing participants to expand on relevant events, decisions, and perceptions that may not have been anticipated in advance [54], [55]. This is particularly important in cyber crisis contexts, where institutional decisions involve trade-offs and evolving priorities that are best captured through narrative explanation rather than fixed-response instruments. Each interview lasted approximately one hour. Interviews were conducted with the aim of capturing both factual descriptions (e.g., actions taken, sequence of events, communication channels used) and interpretative insights (e.g., perceived reputational impact, perceived effectiveness of messaging, internal challenges).

Notes were taken during the interviews, and these notes served as the primary record for analysis. Although note-based recording may limit verbatim detail compared to full transcripts, the approach was considered acceptable given the exploratory nature of the study and the practical constraints typical in organizational research. To mitigate limitations associated with note-based capture, the researcher focused on documenting: (i) key

statements; (ii) concrete examples provided by interviewees; and (iii) reported rationales for decisions and actions.

3.3.1.1. Interview Topics and Alignment with Objectives

The interview scripts were designed around the research objectives and the conceptual framework presented in Chapter 2, ensuring that the empirical data collected would directly address each analytical dimension of the study. The two interview guides were deliberately differentiated to reflect the distinct professional perspectives of each interviewee group, while remaining complementary and together covering both the technical and reputational dimensions that the dissertation seeks to integrate.

The DSI interview topics were structured to address the first and second research objectives: identifying the operational consequences of the attack and analyzing the institution's technical response. Topics were organized to follow the logical sequence of a ransomware incident, from initial detection through containment, recovery, and post-incident learning, drawing on the NIST incident response lifecycle [19] and ISO/IEC 27035 [47] as the underlying conceptual structure. This allowed the researcher to capture both the factual timeline of events and the governance and decision-making dimensions that shaped the technical response.

The Communication Department interview topics were structured to address the second and third research objectives: analyzing crisis communication practices and image recovery strategies and generating recommendations for reputational preparedness. Topics were organized around the stages of crisis communication identified in Situational Crisis Communication Theory [8], enabling systematic examination of how the institution managed stakeholder perceptions before, during, and after the incident.

The two sets of questions were designed to be analyzed both independently and in conjunction, reflecting the dissertation's central argument that technical response and crisis communication are interdependent rather than sequential. The full interview scripts are provided in Appendix A and Appendix B.

The technical interview with the DSI covered the following themes:

- Detection and confirmation of the incident;
- Containment decisions and service shutdown rationale;

- Impact on infrastructure and backup systems;
- Recovery strategy and restoration timeline;
- Engagement with authorities and external providers;
- Governance/documentation gaps identified (e.g., ISP/BCP);
- Post-incident changes (e.g., MFA, segmentation, backup strategy);
- Lessons learned and organizational constraints (resources, public administration context).

The communication interview with the Director of the Communication Department addressed the following themes:

- Crisis communication responsibilities and approval workflow;
- Choice of channels and prioritization of audiences;
- Stakeholder management (students, staff, international community);
- Media engagement and external consultancy role;
- Transparency strategy and reputational risk assessment;
- Social media monitoring and public sentiment;
- Post-incident initiatives (awareness campaigns, stakeholder meetings);
- Lessons learned and readiness improvements.

3.3.2. Secondary Data: Documentary and Media Sources

Secondary data were collected to complement and validate the interview evidence. These sources included:

- Official institutional communications and public statements related to the incident;
- Media coverage from Portuguese news outlets reporting on the cyberattack;
- Publicly available commentary and discussion in digital spaces (e.g., social media and forum posts) where relevant to stakeholder sentiment and perceived impact.

These materials were used to reconstruct elements of the public narrative and to support comparison between internal institutional accounts and external perceptions. The intent was not to treat media reports as definitive factual evidence of technical details, but rather as indicators of how the incident was framed publicly and how reputational exposure may have evolved during the response period.

3.4. Data Analysis Strategy

Given the qualitative nature of the study and the manual, note-based interview record, analysis followed a manual interpretive approach informed by principles of thematic analysis [56], [57]. Rather than applying software-supported coding, the researcher conducted structured reading and categorization of the interview notes and secondary materials.

The analysis proceeded in four stages:

1. **Familiarization:** review of interview notes and collected documents to identify recurring ideas, notable statements, and references to key events.
2. **Initial categorization:** grouping content into preliminary categories aligned with the research objectives (e.g., "containment actions", "communication channels", "stakeholder concerns", "reputational mitigation", "lessons learned").
3. **Theme consolidation:** consolidating categories into higher-level themes that capture patterns across data sources. Themes were organized to reflect both dimensions of the case:
    a. Technical/operational dimension (preparedness, detection, response, recovery, governance improvements);
    b. Reputational/communication dimension (transparency, message control, stakeholder engagement, media handling, trust preservation).
4. **Interpretation and linkage to theory:** interpreting themes using the theoretical lens outlined in the literature review, particularly crisis communication principles and reputation/trust frameworks. This stage informs the Discussion chapter by explicitly connecting empirical findings to academic models and previously documented cases.

To increase internal consistency, key claims drawn from interviews were checked against secondary sources where possible (e.g., reported timelines, described disruptions, and the existence of stakeholder dissatisfaction) [17].

3.5. Methodological Framework

To ensure coherence between research objectives, data collection, and analysis, the study followed a structured methodological framework integrating qualitative inquiry, case study logic, and triangulation. This framework is summarized in Figure 1 and reflects four interconnected phases.

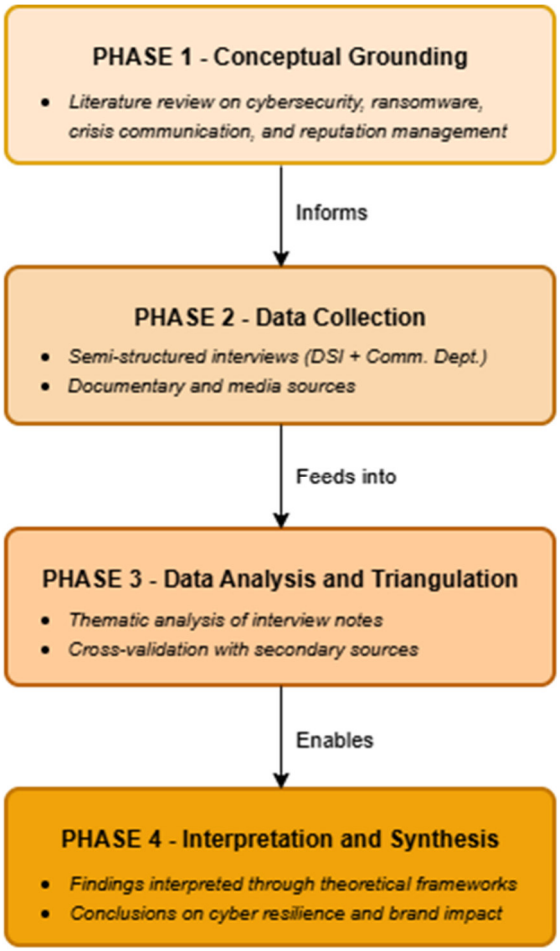

Figure 1 – Methodological Framework: Four-Phase Research Design

Phase 1 – Conceptual Grounding: The study began with a review of literature on cybersecurity in higher education, ransomware, crisis communication, and reputation management. This phase informed the identification of the research problem, the formulation of objectives, and the development of interview scripts.

Phase 2 – Data Collection: Primary data were gathered through semi-structured interviews with technical and communication stakeholders, while secondary data were collected from institutional documents, media reports, and online discourse related to the IPLeiria cyberattack.

Phase 3 – Data Analysis and Triangulation: Interview notes and documentary sources were analyzed using a thematic approach. Evidence was compared across sources to identify convergences and discrepancies between internal institutional narratives and external public perceptions.

Phase 4 – Interpretation and Synthesis: Findings were interpreted using theoretical models of crisis communication and reputation management, allowing the study to draw conclusions about institutional resilience and brand impact.

3.6. Trustworthiness and Research Quality

Qualitative research is evaluated through criteria such as credibility, dependability, and confirmability rather than statistical validity [58]. Several measures were used to strengthen trustworthiness:

- **Triangulation:** combining interviews with documentary and media sources to reduce reliance on a single narrative and to strengthen interpretative confidence [17].
- **Role diversity of interviewees:** collecting data from both the technical response side (DSI) and the communication/reputation side (Communication Department) to capture complementary perspectives.
- **Transparency of method:** documenting how data were collected (notes), how themes were derived (manual categorization), and how interpretations were linked to the research objectives.
- **Reflexivity:** acknowledging that the author's proximity to the institutional context may create both advantages (access and contextual understanding) and risks (interpretative bias) [59]. The use of secondary data and structured thematic organization served as partial mitigation.

While the absence of full interview recordings and transcripts restricts the use of verbatim quotes and may reduce granularity, the study compensates by focusing on consistent cross-source patterns and by maintaining a clear chain of reasoning from evidence to conclusions.

3.7. Ethical Considerations

This research adhered to standard ethical principles for academic research involving human participants. Interviewees were informed of the purpose of the study and the intended use of collected information. Participation was voluntary, and interviewees retained the right to decline to answer specific questions or to withdraw from participation.

Given the sensitive nature of cybersecurity incidents, care was taken to avoid disclosing operational details that could unnecessarily increase institutional risk. However, as the institution did not impose specific constraints on reporting and the study focuses on strategic

response rather than exploitable technical configurations, the analysis prioritizes organizational learning and reputational implications.

When presenting interview evidence, the dissertation uses anonymized attribution to support clarity while maintaining professional discretion.

3.8. Limitations

This study has some limitations that should be acknowledged. First, the research is based on a single case study, which limits broad generalization. The findings aim for analytical rather than statistical generalization and should be interpreted as context-dependent.

Second, the interview dataset comprises two interviews and therefore reflects a focused set of institutional perspectives. Although interviewees were directly involved and highly relevant to the research objectives, additional stakeholder voices (e.g., students, teaching staff, external partners) could provide further insight into perceived reputational impact.

Third, interviews were recorded through notes only, which may reduce interpretative richness and prevent precise quotation. This limitation is partly mitigated through triangulation with secondary sources.

Finally, the study relies on publicly available secondary sources for external narrative and stakeholder sentiment. Such sources may be incomplete or influenced by journalistic framing and online discourse dynamics. For this reason, they are used as contextual indicators rather than definitive factual records of the incident.

Despite these limitations, the methodological design is appropriate for the study's exploratory purpose and provides a credible basis for understanding how a ransomware incident can interact with institutional trust, communication strategy, and brand image in the higher education context.

4. Case Study of IPLeiria's Cyber Attack

4.1. Institutional Profile

The Polytechnic Institute of Leiria is one of Portugal's leading public higher education institutions, recognized for its strong regional engagement, applied research, and diverse academic offerings across multiple campuses. Positioned within the national network of polytechnic education, IPLeiria serves thousands of students annually in fields ranging from technology and health to arts and management [60].

As a modern HEI, IPLeiria relies heavily on digital infrastructure to support academic delivery, administrative services, internal communications, and research activities. This dependence on interconnected systems, combined with the openness typical of academic environments, increases institutional vulnerability to large-scale cyber disruptions, particularly ransomware attacks.

4.2. Incident Overview

In the early hours of 2 May 2023, IPLeiria was targeted by a major ransomware attack carried out using the Akira variant [15]. The breach was first identified around 4:00 a.m., when the institution's external Security Operations Centre (SOC) lost access to its data collection systems, signaling abnormal activity. Upon inspection, it became evident that multiple systems were being encrypted simultaneously; the presence of a dropped ransom note file (*akira_readme.txt*), illustrated in Figures 3 and 4, confirmed the nature of the attack as an Akira ransomware intrusion.

From the onset, it was necessary to disconnect servers to contain the spread and assess potential exfiltration of sensitive data. Immediate institutional priorities included diagnosing the incident, coordinating with relevant authorities, and ensuring a structured organizational response. Although no formal crisis communication manual existed at the time, the Directorate of Information Services (DSI) relied on an existing technical contingency plan, which proved instrumental during the early response phase.

Despite having preventive measures in place, including periodic audits, vulnerability scanning, an active SOC, and outsourced Chief Information Security Officer (CISO) and Data Protection Officer (DPO) functions, a critical monitoring gap was identified. Detection

did not occur through automated internal alerting but rather when systems became unreachable.

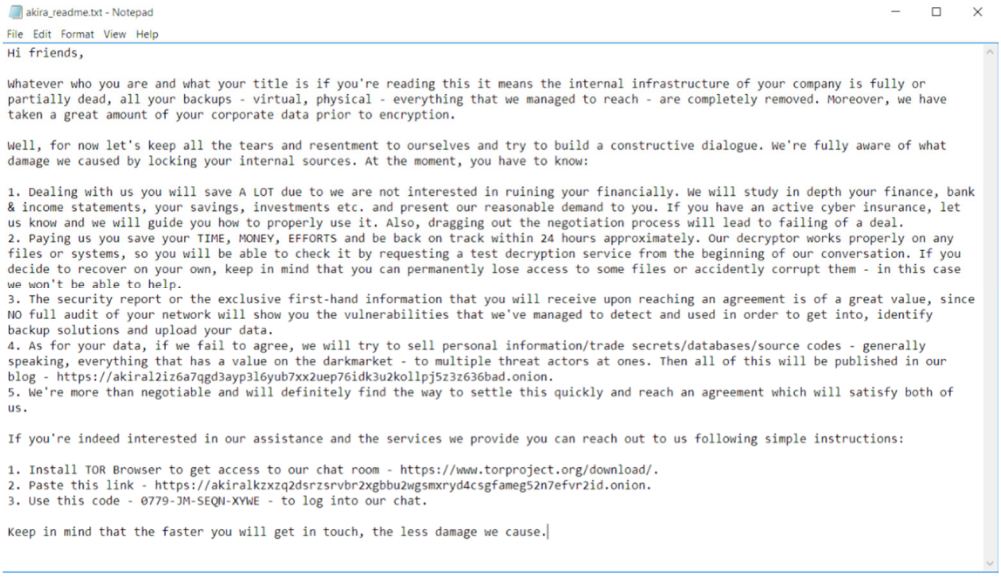

Figure 2 – Akira ransomware note (akira_readme.txt) recovered from compromised IPLeiria systems

Figure 3 – Akira ransomware dark web interface

Because of the attack, IPLeiria's internal network, internet connectivity, institutional email system, and academic platforms such as Moodle were disabled, leading to near-total disruption of digital operations [61].

In the weeks preceding the attack, a documented escalation of phishing activity had been observed, with increasing reports from users and identifiable patterns in the email service. Microsoft blocked the institution's entire email tenant on 28 April due to suspicious outbound activity. While these signals were monitored, they were not identified at the time as indicators of an imminent coordinated intrusion. There is no conclusive evidence confirming phishing as the initial attack vector, though investigators suspected the compromise of privileged credentials through phishing-related credential theft [62].

Data exfiltration was later confirmed on two machines, although the full extent of exposure remained unclear. A ransom payment of approximately €200,000 was demanded; however, no direct negotiation or communication with the attackers was reported, and IPLeiria refused to pay.

The chronological sequence of events, from the pre-attack period through to recovery, is summarized in Table 3.

Table 3 - Timeline of the Pre-Attack Period and Institutional Response

Date / Period	Key Event	Institutional Actions
~20 April 2023	Significant increase in phishing attempt reports observed	N/A
~25 April 2023	Users identified as falling for phishing attempts; patterns detected in email service	N/A
28 April 2023	Microsoft blocked outgoing email for entire institutional tenant	Email communications disrupted
2 May 2023 (04:00)	Attack detected through external SOC alert	Immediate system shutdown and containment
2-3 May 2023	Encryption activity confirmed across infrastructure	Servers disconnected, evidence preserved
Early May 2023	Full outage of critical services (email, Moodle, student portal, network)	Alternative communication channels activated
Same day reporting	Authorities notified (PJ, CNCS, CNPD, Prosecutor’s Office)	Investigation initiated with national bodies
11 May 2023	Critical services restored	Core infrastructure operational again
11-end May 2023	Gradual service recovery (e.g., Wi-Fi restored by 20 May)	Phased return of full institutional functionality
Following months	Backup systems unusable for ~3 months	Long-term rebuilding and upgrades

4.3. Technical Response and Infrastructure Recovery

The DSI's immediate technical response prioritized containment, forensic preservation, and infrastructure rebuilding. External consultants and cybersecurity providers were engaged to support vulnerability analysis, firewall maintenance, and network monitoring, including EDR/XDR tooling (provider name withheld).

Encryption attempts were detected across approximately 300 servers, with four to five confirmed as compromised, alongside several workstations. The attack propagated primarily through the SYSVOL folder of the institution's domain controllers, all of which were compromised. This vector enabled rapid lateral spread across the network, as SYSVOL is replicated between domain controllers and accessible to authenticated users, illustrating how attackers leveraged trusted internal mechanisms to maximize reach. Notably, antivirus solutions intercepted and terminated many of the encryption processes before completion – a significant mitigating factor that limited the scale of data loss despite the broad scope of the intrusion. This partial effectiveness of existing controls is analytically important as it demonstrates that preventive measures were not entirely absent, but were insufficient to prevent the attack from causing extensive operational disruption. The distinction between systems where encryption was completed and those where it was interrupted shaped both the recovery strategy and the forensic preservation requirements that followed.

Recovery required building functional infrastructure without reactivating compromised systems prematurely. New servers were acquired, and offline restoration through external drives enabled secure rebuilding. The restoration of the most critical services took approximately two weeks, with gradual recovery beginning on May 11th.

The online backup system was specifically targeted, highlighting the risk of relying exclusively on connected backups. Since the incident, IPLeiria has adopted a five-layer backup strategy, incorporating online, offline, external-drive, cloud-based, and isolated environments.

Post-incident technical improvements included:

- multi-factor authentication (MFA);
- stronger segmentation and access controls;
- VPN-based restrictions;
- formalization of documentation aligned with ISO 20000 and CIS Controls;

- ongoing implementation of a Computer Security Incident Response Team (CSIRT).

4.4. Legal and Institutional Coordination

The attack was reported immediately to several authorities, including:

- Judicial Police (PJ);
- National Cybersecurity Centre (CNCS);
- National Data Protection Commission (CNPD);
- Public Prosecutor's Office.

The PJ collected evidence onsite on the same day, though the investigation was later archived. The CNCS monitored the process but did not provide direct technical remediation solutions beyond institutional support [63].

Beyond formal regulatory coordination, the institution received significant support from a broader network of external partners during the recovery period. Several higher education institutions offered practical assistance and solidarity, which reflects sector-wide recognition of shared vulnerability to ransomware threats. Additional support was provided by municipal bodies and intermunicipal communities in the Leiria region, as well as by private technology partners who contributed resources, expertise, and infrastructure on both contractual and voluntary bases. This network of institutional solidarity played a meaningful role in enabling recovery under conditions of severe resource constraint, and illustrates a dimension of cyber crisis response that is rarely documented in the academic literature: the informal and inter-institutional support mechanisms that supplement formal governance structures during acute operational disruption.

4.5.Impact Assessment

4.5.1. Operational Disruption

The attack severely disrupted institutional operations. Academic platforms, administrative systems, and communication services were offline. Classes were affected, forcing staff to distribute materials through external services, while administrative tasks reverted temporarily to manual procedures.

4.5.2. Financial Burden

While no official figures were disclosed, the institution incurred substantial recovery costs, including procurement of new servers, consultancy support, staff overtime, and infrastructure rebuilding. Long-term costs also include security investments necessary for regulatory compliance and resilience.

4.5.3. Reputational Exposure

Reputational risks were mitigated through cautious and transparent communication. Although discomfort emerged, particularly among international students, there were no major hostile reactions on social media. Continuous monitoring and responsive clarification helped preserve stakeholder trust.

An official institutional statement released between May 11–12 indicated no evidence of data theft at that stage. However, as shown in Figure 4 [64], [65], Falcon Feeds reported claims by attackers suggesting possession of sensitive data, though no leaks have surfaced, indicating psychological extortion leverage rather than confirmed publication.

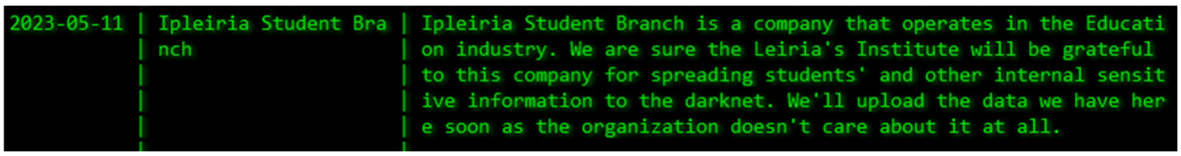

Figure 4 – Falcon Feeds threat intelligence post reporting IPLeiria as an Akira ransomware victim

4.6. Communication Strategy and Stakeholder Engagement

Internal and external communication was managed carefully. Social media became a critical channel due to disruption of email services, especially for maintaining contact with international students.

All public messages were coordinated between the Presidency and DSI, and reviewed to ensure clarity and alignment with institutional values. Media engagement was supported by an external communications consultancy.

Although no crisis communication manual existed, the institution demonstrated effective coordination, transparency, and control, contributing to reputational stability.

Post-incident, IPLeiria strengthened stakeholder engagement through training initiatives, phishing simulation campaigns, and cybersecurity literacy seminars.

4.7. Lessons Learned and Institutional Resilience

As part of the post-incident phase of the response cycle, the DSI conducted an internal review to identify structural vulnerabilities and inform future preparedness. The lessons identified through this process reflect both the technical gaps exposed by the attack and the organizational constraints that shaped the response.

From a technical standpoint, the incident underscored the necessity of diversified and offline backup strategies, given that online backup infrastructure had been specifically targeted and rendered unusable. The absence of a formal Business Continuity Plan (BCP) and Information Security Policy (ISP) prior to the attack was identified as a significant gap, limiting the institution's capacity to respond through established and widely known procedures. The need for sustained investment in cybersecurity infrastructure and tooling was also highlighted, alongside the importance of executive awareness and institutional commitment to security governance.

From an organizational standpoint, the stakeholders noted constraints typical of public administration contexts, including limited dedicated resources, the absence of formal recognition mechanisms for overtime contributions during the crisis, and the procurement complexities involved in emergency server acquisition. At the same time, informal resilience practices, such as locally maintained redundant backups by a DSI member, proved critical in enabling partial recovery where centralized systems had failed.

These lessons directly informed the post-incident improvements implemented by the institution, including the adoption of multi-factor authentication, enhanced network segmentation, diversified backup strategies, and the initiation of a formal CSIRT establishment process. Institutional leadership support was identified as a key enabling factor throughout, facilitating rapid cross-departmental coordination under significant operational pressure.

4.8. Chapter Summary

The May 2023 Akira ransomware attack caused extensive disruption across IPLeiria's infrastructure, disabling essential services and exposing vulnerabilities in monitoring and continuity planning. The institutional response combined rapid containment, cooperation with authorities, phased recovery beginning on May 11th, and significant post-incident security improvements.

Communication strategies were cautious yet transparent, helping mitigate reputational damage and preserve stakeholder trust. Overall, IPLeiria's response demonstrated adaptability, institutional resilience, and commitment to both technical recovery and reputational responsibility.

Chapter 5 will now discuss these findings in relation to crisis communication theory, cyber resilience frameworks, and comparable higher education ransomware incidents.

5. Discussion of the Results

5.1. Discussion Overview

Chapter 4 presented the empirical case study of the May 2023 Akira ransomware attack that affected IPLeiria, highlighting the operational disruption, institutional response measures, and reputational considerations associated with the incident. Building upon those findings, the present chapter provides a critical discussion of the results in relation to the theoretical frameworks introduced in Chapter 2, including ransomware threat evolution, crisis communication theory, and cyber resilience models.

In particular, this discussion is organized around two complementary analytical dimensions that emerged directly from the primary interview data. The first dimension concerns the technical and infrastructural impact of the cyberattack, focusing on operational disruption, incident detection challenges, recovery complexity, and post-incident cybersecurity improvements, as emphasized by the Directorate of Information Systems (DSI). The second dimension relates to the management of institutional brand image and stakeholder trust, focusing on crisis communication strategies, reputational mitigation, and engagement with internal and external audiences, as highlighted by the Communication Department.

This dual approach reflects the interdisciplinary nature of ransomware incidents in higher education institutions, where cyberattacks constitute not only technical disruptions but also organizational crises capable of undermining legitimacy and public confidence. By interpreting the IPLeiria case through both perspectives, the chapter aims to demonstrate how effective response requires integration between cybersecurity governance and communication strategies, ultimately contributing to institutional resilience.

5.2. Technical and Operational Impact of the Ransomware Attack

The first major set of findings derived from the interviews concerns the infrastructural and operational consequences of the ransomware attack. The DSI interviewees provided detailed insight into the timeline of the incident, the technical response measures adopted, and the vulnerabilities that were exposed. These findings reinforce existing literature highlighting that ransomware attacks in HEIs represent complex socio-technical crises, where operational disruption is compounded by governance and resource challenges [1].

5.2.1. Detection and Containment Challenges

One of the most significant technical findings relates to the initial detection of the attack. According to the DSI interviewees, the ransomware infection was identified at approximately 4:00 a.m. on 2 May 2023, following an alert from the institution's external Security Operations Centre (SOC), which lost access to a monitoring node. As the DSI interviewees described, the first indication of compromise was not an automated alert but the observation that "a set of machines had stopped responding and were being encrypted" (author's translation), indicating that detection occurred through system failure rather than an automated internal alert mechanism.

This finding is consistent with broader research suggesting that many organizations, particularly in the public and academic sectors, face persistent limitations in real-time monitoring and early-stage intrusion detection [3]. Although IPLeiria maintained preventive measures such as vulnerability scanning, periodic audits, and outsourced CISO/DPO functions, the attack revealed a critical monitoring gap. The need for stronger alert correlation and anomaly detection reflects the broader challenge HEIs face in maintaining robust situational awareness across decentralized infrastructures [23].

It is worth noting that the attack did not emerge without precursors. In the weeks prior to May 2nd, the institution experienced a documented escalation of phishing activity, with increasing reports from users and identifiable patterns of credential compromise in the email service; Microsoft ultimately blocked the institution's entire email tenant on 28 April due to suspicious activity. While these signals were monitored, they were not recognized at the time as indicators of an imminent coordinated intrusion. This retrospective observation reinforces the broader literature on detection gaps: pre-attack indicators are frequently present but not identified as such until after the incident occurs [3], [18].

Once encryption activity was confirmed, the institution's immediate response was rapid containment. Systems were shut down, servers disconnected, and network segments isolated to prevent lateral spread. The severity of the containment measures was directly related to the propagation mechanism identified – the attack had spread through the SYSVOL folder of the domain controllers, all of which were compromised. Because SYSVOL replication operates across the entire domain infrastructure, the decision to shut down systems broadly rather than selectively was a necessary consequence of the architectural scope of the intrusion. The DSI interviewees were direct about the immediate rationale: "the machines

were shut down with the purpose of isolating and containing the incident" (author's translation), a decision taken within the first hours of confirmed encryption activity and consistent with established containment principles. This aligns with incident response best practices, where early containment is essential to limit ransomware propagation and preserve evidence for forensic investigation [19]. The decision to disable core services, although operationally disruptive, was therefore a necessary measure to regain institutional control over the attack.

5.2.2. Infrastructure Damage and Service Disruption

The operational impact of the ransomware incident was extensive. The attack compromised critical institutional services, including network connectivity, institutional email, Moodle learning systems, and student portals. Encryption attempts were detected across approximately 300 servers, with several confirmed as compromised, alongside multiple workstations.

These disruptions illustrate the particularly severe consequences ransomware poses for HEIs, whose daily functioning depends on continuous access to digital infrastructure. As noted in the literature review, higher education institutions maintain broad attack surfaces due to open-access cultures, heterogeneous devices, and high user turnover, which collectively increase systemic vulnerability [1].

The disruption extended beyond IT systems into core academic operations. Teaching staff were forced to redistribute course materials through external platforms, while administrative processes temporarily reverted to manual execution. This reinforces the argument that ransomware attacks in education environments constitute institutional crises affecting service continuity, stakeholder experience, and organizational legitimacy.

In this sense, the IPLeiria case reflects global patterns observed in other HEI ransomware incidents, where operational paralysis often generates cascading consequences for pedagogy, governance, and institutional credibility [29].

5.2.3. Backup Compromise and Recovery Complexity

A further critical finding concerns the compromise of the institution’s backup infrastructure. The DSI interviewees confirmed that the attack specifically targeted connected online backup systems, rendering them unusable for approximately three months. This significantly

increased recovery complexity and highlighted the dangers of relying exclusively on online backup environments.

This finding strongly supports existing research emphasizing that ransomware groups increasingly target backups as a strategic priority, aiming to eliminate recovery alternatives and increase ransom pressure [3], [4]. The attack therefore demonstrates the operational importance of diversified backup models, such as multi-layer or offline redundancy architectures.

In IPLeiria's case, restoration relied partially on informal redundant backups maintained by technical staff, alongside the acquisition of new servers and the use of offline external drives. This reflects a broader institutional lesson: resilience depends not only on formal infrastructure but also on technical culture and precautionary practices. As the DSI interviewees reflected, it was ultimately informal staff practices that proved decisive: "the typically cautious instinct of individual system administrators contributed enormously to the recovery" (author's translation).

Critical services were restored by May 11th, yet full recovery required a phased approach, with services such as Wi-Fi only restored by 20 May. This illustrates that ransomware recovery is not immediate but often involves prolonged rebuilding, testing, and risk containment, particularly when evidence preservation is required.

5.2.4. Post-Incident Improvements and Resilience Maturity

The attack acted as a catalyst for significant institutional cybersecurity improvements. The DSI interviewees highlighted multiple post-incident measures, including:

- implementation of multi-factor authentication (MFA);
- stronger network segmentation and access restriction by user profile;
- expansion to a five-layer backup policy incorporating offline and cloud components;
- increased reliance on VPN-based service protection;
- ongoing implementation of a Computer Security Incident Response Team (CSIRT);
- formalization of documentation aligned with ISO and CIS control frameworks.

These improvements reflect a shift from reactive recovery towards a more mature cyber resilience posture. As ENISA (2023) notes, resilience is increasingly defined by

organizational capacity to adapt and improve following cyber disruption, rather than by prevention alone.

However, the interviews also revealed constraints typical of public-sector administration, including limited staffing resources and difficulties in recognizing overtime contributions. The DSI interviewees were candid about the structural reality facing public institutions: "it is impossible, with the level of resources and quality of training available, to comply with all applicable regulation" (author's translation), a constraint that reflects not individual failure but systemic underfunding of cybersecurity governance in the public sector. Such structural limitations are frequently identified in academic cybersecurity governance, where institutional complexity and budgetary restrictions may hinder long-term security investment [2].

Overall, the technical findings from the IPLeiria case demonstrate that ransomware attacks expose not only infrastructural weaknesses but also governance challenges, reinforcing the importance of preparedness, diversified recovery planning, and institutional commitment to resilience.

5.3. Communication Strategy and Institutional Reputation Management

The second major analytical perspective emerging from the primary interview data concerns the management of institutional communication, brand image, and stakeholder trust during the cyber crisis. The Communication interviewee emphasized that ransomware incidents in higher education institutions extend beyond technical disruption, representing situations with the potential to threaten institutional credibility, public confidence, and reputational legitimacy.

As discussed in Chapter 2, HEIs depend heavily on trust as an intangible asset, since their public mission is closely tied to perceptions of reliability, ethical responsibility, and service continuity [7]. Consequently, cyberattacks that disrupt essential academic services or raise concerns regarding sensitive data protection may be interpreted as institutional failures, even when the organization is primarily a victim of external cybercrime [8]. The Communication interviewee confirmed that reputational risk was therefore treated as a central dimension of the response strategy.

5.3.1. Cyberattacks as Reputational Crises in Higher Education

From a reputational standpoint, ransomware attacks increasingly function as crises of organizational trust. Modern campaigns frequently employ double extortion tactics, where data exposure threats amplify pressure beyond mere encryption [4]. In academic contexts, this reputational leverage is especially significant, since HEIs manage personal student data, research outputs, and international partnerships.

The Communication interviewee noted that the May 2023 incident immediately raised concerns not only about operational continuity but also about the institution's public image and stakeholder reassurance. This is directly correlated to the statement that reputational harm is often among the most severe long-term consequences of cyber incidents, frequently affecting stakeholder trust and organizational credibility [3], [8], [13].

Within crisis communication theory, [8] highlights that stakeholder perceptions of responsibility are crucial in shaping reputational outcomes. Although ransomware attacks are typically classified as "victim crises," perceptions may shift if stakeholders believe the institution lacked preparedness or transparency. The Communication interviewee therefore emphasized the importance of demonstrating institutional control, responsibility, and commitment to resolution from the earliest stages of public communication.

5.3.2. Crisis Communication Practices During the IPLeiria Incident

A key finding from the communication-focused interview concerns the absence of a formally established crisis communication manual at the time of the attack. Nevertheless, the institution relied on coordinated internal governance, supported by existing contingency practices and external communication expertise.

The Communication interviewee explained that all institutional messaging was managed carefully through collaboration between the Presidency and the Directorate of Information Systems (DSI). This interdepartmental alignment was essential to ensure consistency between technical recovery realities and stakeholder-facing communication. External media engagement was further supported by a professional communications consultant, reflecting an institutional priority to manage public narrative responsibly.

Communication channels were selected strategically due to operational constraints. With institutional email services disrupted, social media platforms became a particularly important means of maintaining contact with stakeholders. As the Communication

interviewee described: “social media was essential at this stage for providing responses, there was a very important effort in that regard” (author's translation), particularly in reaching international students whose primary institutional communication channel was unavailable. This response is consistent with Coombs' [8] principle that crisis communication must provide timely instructing information, enabling stakeholders to understand immediate implications and required actions. At the same time, the institution attempted to avoid alarmism, balancing transparency with reassurance, demonstrating the dual crisis objective of maintaining stakeholder confidence while managing uncertainty.

5.3.3. Stakeholder Trust and Perception Management

The Communication interviewee reported that stakeholder reactions were monitored closely throughout the incident. Despite operational disruption, the overall public response was largely understanding, with no significant hostile mobilization observed on social media. Continuous monitoring enabled the institution to collect feedback, correct misinformation, and clarify institutional actions where necessary.

Nevertheless, the interviewee acknowledged that discomfort and dissatisfaction were present, particularly among groups most affected by service unavailability. Communication efforts therefore prioritized clarity, empathy, and responsiveness, reinforcing the institutional values of transparency and accountability.

This aligns with SCCT’s emphasis on “adjusting information”, which addresses stakeholder psychological needs through reassurance, empathy, and explanation of recovery efforts [8]. By engaging proactively with affected communities, IPLeiria reduced reputational escalation and preserved trust despite operational difficulties.

Moreover, the institution emphasized that authorities had been notified promptly and that preventive measures were already underway. This public positioning contributed to reputational mitigation by demonstrating responsibility and alignment with regulatory expectations.

5.3.4. Post-Incident Awareness Initiatives and Brand Reinforcement

Beyond immediate crisis communication, the Communication interviewee emphasized that the incident produced a positive secondary effect: heightened cybersecurity awareness within the academic community. Following the attack, IPLeiria strengthened stakeholder

engagement through initiatives such as phishing simulation campaigns, seminars, and training sessions aimed at improving digital literacy.

Such measures represent not only technical improvement but also reputational reinforcement. Institutions that demonstrate learning and proactive reform after crises tend to recover trust more effectively than those that treat incidents as isolated disruptions [37], [46]. In this sense, IPLeiria's post-incident communication strategy contributed to long-term image recovery by signaling institutional adaptation and resilience.

The Communication interviewee further noted that the institution maintained its relationship with the external communications consultancy, moving toward a more proactive partnership model. Stakeholder meetings, particularly with students, were also integrated into communication strategy, reinforcing institutional transparency and trust-building.

Reflecting on what ultimately preserved institutional trust, the Communication interviewee identified: "above all, the transparency and clarity of the message, as well as the consistent follow-through of the process and the support of the authorities" (author's translation), positioning these as the primary factors behind the institution's ability to maintain stakeholder confidence despite prolonged disruption.

Although the ransomware attack did not fundamentally alter IPLeiria's brand strategy, the response actions aligned strongly with its established identity principles: responsiveness, institutional integrity, and cooperation with authorities. The clarity and speed of messaging, combined with phased restoration of services and a demonstrated sense of control, were essential to preserving institutional legitimacy.

Overall, findings from the Communication interviewee suggest that reputational resilience in HEIs depends not only on technical containment but also on structured communication practices, stakeholder empathy, and visible organisational learning. These elements reinforce the argument that cybersecurity crises must be managed as both operational disruptions and brand reputation challenges within higher education environments.

5.4. Integrated Interpretation: Linking Cyber Resilience and Brand Image Recovery

The findings from the IPLeiria case study demonstrate that ransomware attacks in HEIs must be understood as multidimensional crises, where technical disruption and reputational

exposure evolve simultaneously. The dual perspectives provided by the Directorate of Information Systems (DSI) and the Communication interviewee reinforce the argument developed throughout Chapter 2: effective crisis management requires integration between cybersecurity resilience and institutional brand protection.

From a technical standpoint, the DSI interview emphasized the infrastructural severity of the Akira ransomware attack, including widespread encryption attempts, outage of critical services, and compromise of backup systems. From a reputational standpoint, the Communication interviewee highlighted the risk of stakeholder distrust, the importance of transparency, and the need to maintain institutional credibility during operational uncertainty. Taken together, these perspectives illustrate that ransomware incidents represent both a crisis of systems and a crisis of confidence.

This integrated interpretation aligns directly with the conceptual framework proposed in Section 2.6, where cyberattacks trigger operational disruption, institutional response mechanisms, and reputational outcomes through stakeholder perception dynamics.

5.4.1. Cyber Resilience as a Reputational Asset

The IPLeiria case confirms that cyber resilience extends beyond the restoration of digital infrastructure. While critical services were recovered beginning on May 11th, the institution's longer-term resilience depended equally on the demonstration of governance, control, and learning. As ENISA (2021) emphasizes, resilience is increasingly defined by an organization's capacity to adapt and improve after disruption, rather than by prevention alone.

In academic environments, this resilience carries reputational significance. Stakeholders such as students, staff, research partners, and authorities do not evaluate institutions solely based on whether an attack occurred, but rather on how competently and responsibly the institution responded. In this sense, technical recovery functions as a prerequisite for trust recovery: service restoration and infrastructure improvements become symbolic indicators of institutional reliability [25].

IPLeiria's refusal to pay ransom and its emphasis on phased, controlled recovery reflect a commitment to institutional integrity and operational accountability. These actions contributed not only to system recovery but also to the preservation of legitimacy.

5.4.2. Communication as an Extension of Incident Response

The findings further demonstrate that crisis communication cannot be treated as an external or secondary layer applied after technical containment. Instead, communication is embedded within incident response itself, shaping stakeholder understanding and influencing reputational trajectories.

The Communication interviewee confirmed that IPLeiria's messaging strategy prioritized clarity, caution, and alignment between the Presidency and DSI. This coordination illustrates the necessity of integrating technical and communicational governance during cyber crises. A disconnect between these domains may generate contradictory messages, uncertainty, or perceived incompetence.

Situational Crisis Communication Theory (SCCT) provides a useful lens for interpreting this dynamic. [8] argues that crisis response must include instructing information, adjusting information, and corrective action. In the IPLeiria case, technical containment measures were accompanied by public communication stressing institutional control, reporting to authorities, and phased restoration. These actions contributed to reputational mitigation by reducing speculation and reinforcing stakeholder reassurance.

5.4.3. Institutional Trust and Stakeholder-Centered Resilience

A key insight emerging from the integration of both interviews is that ransomware crises challenge HEIs not only operationally but socially. Trust is central to higher education legitimacy, and cyber incidents test stakeholder confidence in institutional responsibility and competence [7].

Although the Communication interviewee noted limited hostile reactions online, dissatisfaction among staff and operational strain were evident, reflecting that reputational impact is unevenly distributed across stakeholder groups [25]. This reinforces the importance of stakeholder-centered crisis strategies, where institutions must address both external audiences (media, partners, prospective students) and internal communities (faculty, administrative staff, researchers).

The reliance on social media during the email outage also illustrates how stakeholder communication channels become essential resilience mechanisms when core infrastructure is compromised. Maintaining contact with international students, for example, was not merely a communication task but a continuity requirement linked to institutional trust.

5.4.4. Learning, Adaptation, and Long-Term Brand Recovery

The IPLeiria case also illustrates how post-incident learning contributes to both technical maturity and reputational reinforcement. The implementation of MFA, network segmentation, five-layer backup policies, and CSIRT planning reflects infrastructural strengthening. Simultaneously, phishing simulations, thematic seminars, and awareness initiatives reflect cultural adaptation and stakeholder engagement.

Literature suggests that organizations which treat crises as catalysts for improvement often recover trust more effectively than those that pursue minimal restoration without visible reform [3]. In this sense, IPLeiria's response aligned with a resilience-building model in which recovery is not merely a return to normality but an opportunity to enhance institutional governance and reaffirm public mission.

5.4.5. Synthesis of Technical and Reputational Dimensions

Ultimately, the IPLeiria ransomware incident demonstrates that cybersecurity in HEIs cannot be conceptualized solely as an IT or operational function. Instead, it forms part of institutional identity, governance, and reputation. Ransomware groups increasingly exploit reputational leverage through extortion threats [3], [4], meaning that technical preparedness must be complemented by crisis communication readiness.

The case therefore supports the broader conclusion that ransomware attacks generate an interdependent cycle:

- operational disruption creates stakeholder uncertainty;
- institutional response shapes perceptions of control and responsibility;
- perceptions influence reputational outcomes and long-term trust.

IPLeiria's experience shows that transparency, collaboration with authorities, phased restoration, and organizational learning are essential components not only of cyber resilience but also of brand image recovery.

The following section situates these findings within a comparative international context, contrasting IPLeiria's response with other ransomware incidents affecting higher education institutions.

5.5. Comparative Context: Lessons from Other Higher Education Ransomware Cases

To further contextualize the findings from the IPLeiria ransomware incident, it is valuable to compare this case with other high-profile ransomware attacks affecting higher education institutions internationally. Comparative reflection allows the identification of common sector vulnerabilities, contrasting response strategies, and broader lessons regarding both cyber resilience and reputational recovery.

Ransomware has increasingly targeted higher education institutions worldwide due to their complex infrastructures, decentralized governance structures, and the high value of the data they store [1]. Several documented cases demonstrate that HEIs face similar operational challenges, yet adopt differing approaches depending on institutional resources, governance maturity, and reputational priorities.

5.5.1. Maastricht University (2019)

One of the most frequently cited ransomware incidents in the European higher education context is the 2019 attack on Maastricht University in the Netherlands. The attack caused significant operational disruption, impacting teaching platforms and institutional services for an extended period. Ultimately, Maastricht University chose to pay a ransom of approximately €200,000 to regain access to encrypted systems and accelerate recovery [29].

This decision highlights a key strategic dilemma in ransomware response: whether ransom payment is justified as a means of reducing downtime and operational loss. Maastricht's payment was influenced by the perceived urgency of restoring academic functionality and concerns regarding the feasibility of recovery through backups alone.

In contrast, IPLeiria refused to engage in ransom negotiation, opting instead for infrastructure rebuilding and cooperation with Portuguese authorities. This illustrates an alternative institutional posture grounded in long-term integrity and governance control. While refusal may prolong recovery efforts, it can also reinforce institutional values and reduce the risk of future targeting, as payment may incentivize attackers or establish precedent.

5.5.2. University of California, San Francisco (2020)

A further relevant comparison is the ransomware attack against the University of California, San Francisco (UCSF) in 2020. UCSF reportedly paid over $1 million following an attack that targeted critical medical and research infrastructure during the COVID-19 pandemic [30]. The disruption threatened not only administrative continuity but also urgent biomedical research, increasing pressure for rapid resolution.

This case demonstrates that ransomware impact in HEIs is not limited to teaching disruption but may extend into strategic research domains with global implications. In institutions where research outputs constitute major reputational and economic assets, ransomware may generate extreme pressure to restore operations quickly.

The IPLeiria case, although not situated within a major biomedical crisis context, similarly illustrates how ransomware disrupts institutional mission: teaching delivery, student services, and organizational credibility. However, IPLeiria's recovery strategy relied on phased service restoration and infrastructure reconstruction rather than ransom-driven decryption.

5.5.3. Communication and Reputation Management Across Cases

Comparisons also reveal differences in crisis communication strategies. In ransomware incidents, institutions must manage both operational uncertainty and public perception. [8] argues that transparency and timely communication reduce reputational escalation by demonstrating responsibility and control.

In Maastricht and UCSF, public narratives focused heavily on service disruption and the controversial nature of ransom payment. Such cases illustrate that reputational risk is shaped not only by the attack itself but also by institutional decisions regarding negotiation, disclosure, and accountability.

In IPLeiria's case, reputational mitigation was supported through coordinated communication between the Presidency and DSI, reliance on social media due to email disruption, and emphasis on cooperation with national authorities. The Communication interviewee noted that stakeholder hostility remained limited, suggesting that transparency and consistent messaging contributed to trust preservation.

Additionally, the threat of double extortion, reported through platforms such as Falcon Feeds [65], reflects the modern reputational pressure ransomware groups exert. While no leaked data emerged publicly, the presence of exfiltration threats demonstrates how cyber crises increasingly operate at both technical and symbolic levels [4].

5.5.4. Sector-Wide Patterns and Lessons for Higher Education

Across cases, several shared vulnerabilities emerge:

- reliance on interconnected digital infrastructure;
- exposure through phishing and credential compromise;
- challenges in backup resilience and redundancy;
- difficulties balancing openness with security controls;
- reputational sensitivity due to public mission and stakeholder trust.

At the same time, response strategies differ significantly based on institutional preparedness, crisis governance, and resource constraints. IPLeiria's experience highlights the importance of rapid containment, refusal to pay ransom, phased recovery, and post-incident learning. Maastricht and UCSF illustrate that operational urgency may sometimes lead institutions to pursue ransom payment, raising ethical and strategic debates.

Overall, comparative evidence supports the conclusion that ransomware incidents in HEIs require integrated planning combining technical preparedness, business continuity governance, and reputational communication strategy [1], [3]. The IPLeiria case contributes to this international landscape by demonstrating how a Portuguese public HEI managed both infrastructural recovery and institutional image preservation without capitulating to extortion demands.

The next section builds upon these findings by outlining strategic recommendations and opportunities for improvement for higher education institutions facing similar ransomware threats.

5.6. Strategic Recommendations and Opportunities for Improvement

The IPLeiria ransomware incident provides valuable lessons for HEIs seeking to strengthen both cyber resilience and reputational preparedness. The combined insights from the Directorate of Information Systems (DSI) and the Communication interviewee demonstrate

that ransomware crises are not exclusively technical events, but organizational disruptions requiring integrated governance across infrastructure, leadership, and stakeholder engagement.

This section outlines key opportunities for improvement derived from the case study, offering strategic recommendations applicable to HEIs facing similar threat environments.

5.6.1. Strengthening Detection and Monitoring Capabilities

One of the main technical vulnerabilities exposed during the IPLeiria incident was the limitation in automated detection. The attack was identified indirectly through the loss of access to an SOC monitoring node, rather than through internal alert correlation. This highlights the importance of investing in advanced monitoring systems capable of detecting anomalous activity before widespread encryption occurs.

HEIs should strengthen:

- Security Information and Event Management (SIEM) integration;
- real-time alerting mechanisms;
- continuous endpoint detection and response (EDR/XDR);
- regular threat-hunting exercises.

Improved detection reduces response latency and limits the scale of disruption, supporting both operational continuity and stakeholder confidence.

5.6.2. Diversifying Backup and Business Continuity Strategies

The attack demonstrated that online backup infrastructures are increasingly targeted by ransomware actors. IPLeiria's inability to use its backup environment for approximately three months significantly complicated recovery. Therefore, HEIs must adopt layered backup architectures aligned with best practices such as offline and immutable storage.

Institutions should prioritize:

- multi-layer backup models (online, offline, cloud, isolated);
- regular backup integrity testing;
- documented disaster recovery procedures;
- formal Business Continuity Plans (BCPs) approved at governance level.

Such measures reduce institutional dependency on ransom negotiation and improve resilience under extortion pressure [4].

5.6.3. Formalizing Crisis Response Governance

Both interviews revealed that response coordination relied heavily on institutional improvisation rather than fully formalized crisis documentation. While the technical contingency plan was essential, the absence of an approved Information Security Policy (ISP) and crisis communication manual highlights the need for structured governance frameworks.

HEIs should develop:

- institution-wide incident response playbooks (ISO 27035 aligned);
- defined escalation chains between IT, leadership, and communications;
- formal CSIRT structures with clear roles;
- regular crisis simulation exercises.

Institutional readiness is strengthened when cybersecurity response is treated as a governance priority rather than a purely operational function [22].

5.6.4. Integrating Crisis Communication into Cyber Incident Management

The Communication interviewee emphasized that reputational mitigation was strongly dependent on transparent and coordinated communication. The reliance on social media due to email disruption illustrates the necessity of communication redundancy and stakeholder-centered messaging.

HEIs should ensure:

- pre-established crisis communication protocols;
- multi-channel communication alternatives (SMS, website banners, social media);
- message validation workflows between technical and leadership units;
- empathy-driven stakeholder engagement during uncertainty.

According to SCCT, instructing and adjusting information are essential in preventing reputational escalation during victim crises [8].

5.6.5. Building a Cybersecurity Culture Through Awareness and Training

The IPLeiria case also highlighted the importance of organizational learning. Post-incident initiatives such as phishing simulations and seminars strengthened cybersecurity awareness across the academic community.

HEIs should institutionalize:

- mandatory cybersecurity training for staff and students;
- recurring phishing simulation campaigns;
- awareness integration into onboarding processes;
- shared responsibility culture rather than IT-only framing.

Human factors remain among the most common ransomware entry vectors, making behavioral resilience central to institutional security [2], [26].

5.6.6. Resource and Structural Considerations in Public Institutions

The DSI interviewees noted constraints typical of public administration, including limited staffing, regulatory pressure, and challenges in recognizing overtime contributions. These structural realities must be considered in resilience planning.

HEIs should advocate for:

- sustained cybersecurity investment at executive and governmental level;
- appropriate resource allocation aligned with regulatory obligations (e.g., NIS2);
- institutional recognition of crisis workload demands.

Resilience maturity depends on strategic support from leadership and long-term investment rather than solely technical effort. Table 4 synthesizes the key challenges identified across all dimensions of the IPLeiria case and the corresponding strategic recommendations for higher education institutions.

Table 4 - Strategic Recommendations for Higher Education Institutions Facing Ransomware

Dimension	Challenge Identified in IPLeiria	Recommended Improvement
Detection and Monitoring	Attack detected indirectly, monitoring gap	Strengthen SIEM, EDR/XDR, automated alerting
Backup Resilience	Online backups targeted; unusable for months	Implement layered offline/immutable backup strategy

Governance and Planning	Lack of formal ISP/BCP at incident time	Approve institutional IR policies and continuity plans
Crisis Communication	No crisis manual; reliance on coordination	Develop formal crisis communication framework and redundancy
Stakeholder Trust	Need for reassurance during service outage	Transparent, empathetic communication aligned with SCCT
Cybersecurity Culture	Awareness raised only after incident	Institutionalize training and phishing simulations
Institutional Resources	Public-sector staffing and investment constraints	Executive advocacy and sustained cybersecurity funding
Long-Term Resilience	Need for structured response maturity	Establish CSIRT and conduct regular crisis simulations

Overall, the IPLeiria ransomware attack illustrates that effective institutional resilience requires simultaneous strengthening of technical infrastructure and reputational governance. Cyber resilience is not achieved solely through system restoration but through proactive preparedness, stakeholder-centered communication, and continuous organizational learning.

The recommendations above reinforce the necessity for HEIs to adopt integrated approaches where cybersecurity strategy is embedded within institutional governance and brand integrity. Such measures are increasingly urgent as ransomware campaigns continue to evolve and regulatory obligations across Europe intensify under frameworks such as NIS2.

5.7. Chapter Summary

This chapter has discussed the findings of the IPLeiria ransomware case study by interpreting empirical evidence through the theoretical frameworks presented in Chapter 2. The discussion was explicitly structured around two complementary perspectives emerging from the primary interview data: the technical and infrastructural impact of the cyberattack, and the institutional management of communication, brand image, and stakeholder trust.

From a technical standpoint, the analysis demonstrated that the Akira ransomware attack caused extensive operational disruption, exposing vulnerabilities in detection, monitoring, and backup resilience. The findings confirm that HEIs face heightened exposure to ransomware due to decentralized infrastructures and dependence on digital services. At the same time, the post-incident improvements implemented by IPLeiria illustrate how cyber

crises can act as catalysts for enhanced resilience maturity, governance formalization, and security investment.

From a reputational and communication perspective, the discussion highlighted that cyberattacks constitute significant trust-based crises in HEIs. The Communication interviewee's insights demonstrated that transparent, coordinated, and empathetic communication played a central role in mitigating reputational damage and preserving stakeholder confidence. The institution's emphasis on authority cooperation, phased recovery, and ongoing engagement contributed to reputational stability despite prolonged operational disruption.

The integrated analysis further revealed that technical recovery and reputational recovery are interdependent processes. Cyber resilience functions not only as an operational capability but also as a reputational asset, influencing perceptions of institutional reliability, responsibility, and legitimacy. IPLeiria's response illustrates the importance of aligning cybersecurity governance with crisis communication strategy to manage ransomware incidents effectively.

Finally, the chapter identified strategic opportunities for improvement relevant to HEIs more broadly, emphasizing the need for enhanced monitoring, diversified backups, formalized crisis governance, and sustained cybersecurity awareness initiatives. These insights provide a foundation for the concluding chapter, which synthesizes the dissertation's contributions, outlines its limitations, and proposes directions for future research.

6. Conclusion

6.1. Overview and Research Purpose Revisited

The increasing frequency and sophistication of ransomware attacks have positioned cybersecurity as a critical challenge for higher education institutions [3], whose missions depend heavily on the availability, integrity, and trustworthiness of digital systems. Beyond operational disruption, such attacks expose institutions to significant reputational risk, particularly in environments characterized by high stakeholder diversity, international visibility, and public accountability.

This dissertation set out to analyze the impact of ransomware attacks on the brand image and institutional reputation of HEIs, using the May 2023 Akira ransomware attack affecting the Polytechnic Institute of Leiria as a case study. The research adopted an interdisciplinary approach, combining cybersecurity incident response perspectives with crisis communication and reputation management theory. By integrating technical analysis with communication strategy evaluation, the study sought to understand how cyber resilience and reputational resilience interact during and after a major cyber incident.

Through qualitative analysis based on semi-structured interviews with institutional stakeholders and supported by secondary media sources, the dissertation explored how IPLeiria responded to the ransomware attack, managed operational disruption, and mitigated potential reputational damage. The concluding chapter synthesizes the main findings, outlines the study's contributions, acknowledges its limitations, and proposes directions for future research.

6.2. Summary of Key Findings

The findings presented in this dissertation address each of the three specific objectives set out in Chapter 1, as described below:

- The first objective, which consisted in identifying the operational and reputational consequences of the ransomware attack, is addressed through the technical and communication findings summarized below (Sections 6.2.1 and 6.2.2), which document the multidimensional impact of the Akira incident across infrastructure, service continuity, stakeholder trust, and institutional credibility.

- The second objective, related to the analyses of the institution's technical response, crisis communication practices, and image recovery strategies, is addressed through the empirical discussion in Chapter 5, which interprets IPLeiria's response against established frameworks including the NIST incident response lifecycle and Situational Crisis Communication Theory.
- The third objective, which aims to propose evidence-based recommendations for strengthening cyber resilience and reputational preparedness in HEIs, is addressed in Section 5.6, where strategic recommendations are derived directly from the case findings and grounded in the theoretical literature

6.2.1. Technical and Operational Findings

From a technical perspective, the findings demonstrate that the Akira ransomware attack caused extensive disruption to IPLeiria's digital infrastructure, affecting core services such as institutional email, academic platforms, student portals, and network connectivity. The attack exposed limitations in monitoring and detection capabilities, as initial identification occurred indirectly through system unavailability rather than automated internal alerting.

The incident further highlighted the vulnerability of online backup infrastructures, which were specifically targeted and rendered unusable for an extended period. As a result, recovery required the acquisition of new servers, reliance on offline restoration mechanisms, and phased service reactivation, with critical services restored by May 11th and full recovery achieved gradually thereafter.

At the same time, the attack acted as a catalyst for institutional improvement. Post-incident measures included the implementation of multi-factor authentication, enhanced network segmentation, diversified backup strategies, and the ongoing establishment of a Computer Security Incident Response Team (CSIRT). These actions indicate a shift towards greater cyber resilience maturity, reinforcing the notion that recovery extends beyond system restoration to encompass organizational learning and governance enhancement.

6.2.2. Communication, Brand Image, and Reputation Findings

From a reputational and communication standpoint, the findings confirm that ransomware attacks constitute significant trust-based crises for HEIs. The Communication interviewee emphasized that the IPLeiria incident posed risks not only to operational continuity but also to institutional credibility and stakeholder confidence.

Despite the absence of a formal crisis communication manual, IPLeiria adopted a cautious and coordinated communication strategy involving close collaboration between the Presidency and the Directorate of Information Systems. Social media channels played a critical role in maintaining contact with stakeholders, particularly international students, during the disruption of institutional email services. Transparency regarding the incident, cooperation with national authorities, and phased recovery updates contributed to limiting reputational escalation.

Overall, stakeholder reactions were largely understanding, with limited hostile responses observed online. The institution's emphasis on responsibility, control, and learning helped preserve trust, demonstrating that effective communication can significantly mitigate reputational damage even in the context of prolonged operational disruption.

6.3. Contribution to Knowledge

This dissertation contributes to existing literature in several important ways. First, it provides an empirical case study of a ransomware attack affecting a Southern European public HEI, addressing a geographic and contextual gap in cybersecurity and crisis communication research, which is often dominated by North American or Northern European cases.

Second, the study offers an interdisciplinary contribution by integrating technical cybersecurity analysis with crisis communication and reputation management frameworks. The findings support the argument that cyber resilience and brand resilience are interdependent, and that cybersecurity governance should be understood as a component of institutional identity and legitimacy.

Third, the conceptual framework developed in this dissertation contributes to theoretical understanding by illustrating how ransomware incidents trigger a dynamic process involving operational disruption, institutional response, stakeholder perception, and reputational outcomes. By applying this framework to a real-world case, the study demonstrates its relevance for analyzing cyber crises in academic environments.

6.4. Practical Implications for Higher Education Institutions

The findings of this study have several practical implications for HEIs facing an increasingly hostile cyber threat landscape [3]. Institutions must recognize that ransomware preparedness

extends beyond technical controls to include crisis communication planning, governance coordination, and stakeholder engagement strategies.

Practically, HEIs should invest in advanced detection and monitoring capabilities, diversify backup and recovery infrastructures, and formalize incident response and business continuity planning. Equally important is the integration of communication functions into cyber incident management, ensuring that messaging is timely, coordinated, and empathetic.

Furthermore, fostering a cybersecurity-aware culture among staff and students through training, simulations, and awareness initiatives can reduce exposure to common attack vectors such as phishing. These measures contribute not only to technical resilience but also to the preservation of institutional trust and reputation.

6.5. Limitations of the Study

As with any qualitative case study, this research is subject to certain limitations. The study focuses on a single institution, which limits the generalizability of the findings to other HEIs with different governance structures, resources, or regulatory contexts. Additionally, the primary data was derived from a limited number of interviews, conducted using note-based recording rather than full transcripts, which may restrict the depth of interpretative analysis.

The sensitive nature of cybersecurity incidents may also have constrained the level of detail shared by interviewees, particularly regarding technical vulnerabilities or internal decision-making processes. Nevertheless, these limitations are consistent with research in security-related contexts and do not diminish the relevance of the insights obtained.

6.6. Directions for Future Research

Future research could build upon this study by adopting comparative approaches across multiple HEIs or national contexts, enabling broader generalization of findings. Quantitative studies examining stakeholder perception and trust recovery following cyber incidents could complement qualitative insights and provide additional empirical depth.

Longitudinal research tracking reputational recovery over time would also contribute to understanding the lasting impact of ransomware attacks on institutional image. Additionally, future studies could further integrate digital forensics perspectives, examining how technical

investigation outcomes influence communication strategies and public narratives during cyber crises.

6.7. Final Remarks

Ransomware attacks represent a growing and complex threat to higher education institutions [3], challenging not only technical infrastructure but also institutional trust and legitimacy. The IPLeiria case demonstrates that effective response requires more than system restoration; it demands integrated governance, transparent communication, and organizational learning.

By highlighting the interdependence between cyber resilience and brand image recovery, this dissertation underscores the need for HEIs to adopt holistic strategies that align cybersecurity preparedness with reputational responsibility. As digital dependence continues to deepen across the academic sector, such integrated approaches will become increasingly essential to safeguarding both institutional operations and public mission.

Bibliographic References

[1] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," Education and Information Technologies, vol. 26, no. 1, pp. 825–848, 2021. doi: 10.3390/fi13020039.

[2] EDUCAUSE, Top IT Issues in Higher Education 2022. Louisville, CO, USA: EDUCAUSE Review, 2022. [Online]. Available: https://er.educause.edu/articles/2021/11/top-10-it-issues-2022-the-higher-education-we-deserve.

[3] European Network and Information Security Agency (ENISA), ENISA Threat Landscape 2023. Athens, Greece: ENISA, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[4] J. Agcaoili, M. Ang, E. Earnshaw, B. Gelera, and N. Tamaña, "Ransomware double extortion and beyond: REvil, Clop, and Conti," Trend Micro Security News, Trend Micro, Jun. 15, 2021. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

[5] H. S. Lallie, A. Thompson, E. Titis, and P. Stephens, "Analysing cyber attacks and cyber security vulnerabilities in the university sector," Computers, vol. 14, no. 2, p. 49, Feb. 2025. doi: 10.3390/computers14020049.

[6] A. Piazza, S. Vasudevan, and M. Carr, "Cybersecurity in UK universities: mapping (or managing) threat intelligence sharing within the higher education sector," *Journal of Cybersecurity*, vol. 9, no. 1, 2023. doi: 10.1093/cybsec/tyad019.

[7] C. J. Fombrun, Reputation: Realizing Value from the Corporate Image. Boston, MA, USA: Harvard Business School Press, 1996.

[8] W. T. Coombs, "Protecting organization reputations during a crisis: The development and application of situational crisis communication theory," Corporate Reputation Review, vol. 10, no. 3, pp. 163–176, 2007. doi: 10.1057/palgrave.crr.1550049.

[9] J. Hemsley-Brown and I. Oplatka, "Universities in a competitive global marketplace: A systematic review of the literature on higher education marketing," International Journal of Public Sector Management, vol. 19, no. 4, pp. 316–338, 2006. doi: 10.1108/09513550610669176.

[10] C. C. Patriche, D. Stoica, G. C. Schin, and V. Sava, "University reputation management: academic knowledge alchemy," Management Decision, ahead-of-print, 2025. doi: 10.1108/MD-04-2024-0889.

[11] C. Chapleo, "Brands in higher education: challenges and potential strategies," International Studies of Management & Organization, vol. 45, no. 2, pp. 150–163, 2015. doi: 10.1080/00208825.2015.1006014.

[12] R. von Solms and J. van Niekerk, "From information security to cyber security," Computers & Security, vol. 38, pp. 97–102, Oct. 2013. doi: 10.1016/j.cose.2013.04.004.

[13] S. Perera, X. Jin, A. Maurushat, and D.-G. J. Opoku, "Factors affecting reputational damage to organisations due to cyberattacks," Informatics, vol. 9, no. 1, p. 28, Mar. 2022. doi: 10.3390/informatics9010028.

[14] K. A. Whitler and P. W. Farris, "The impact of cyber attacks on brand image: Why proactive marketing expertise is needed for managing data breaches," *Journal of Advertising Research*, vol. 57, no. 1, pp. 3–9, Mar. 2017. doi: 10.2501/JAR-2017-005.

[15] Observador, "Suspeita de ataque informático condiciona atividade do Politécnico de Leiria," Observador, May 3, 2023. [Online]. Available: https://observador.pt/2023/05/03/suspeita-de-ataque-informatico-condiciona-atividade-do-politecnico-de-leiria/.

[16] K. Pequenino, "Politécnico de Leiria entre as vítimas da operação de ransomware Akira," Público, May 12, 2023, updated May 13, 2023. [Online]. Available: https://www.publico.pt/2023/05/12/tecnologia/noticia/politecnico-leiria-vitimas-operacao-ransomware-akira-2049524.

[17] R. K. Yin, Case Study Research and Applications: Design and Methods, 6th ed. Thousand Oaks, CA, USA: Sage, 2018.

[18] Verizon, 2024 Data Breach Investigations Report (DBIR), 17th ed. Basking Ridge, NJ, USA: Verizon Business, May 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf.

[19] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST Special Publication 800-61 Rev. 3. Gaithersburg, MD, USA: National Institute of Standards and Technology, Apr. 3, 2025. doi: 10.6028/NIST.SP.800-61r3. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

[20] International Organization for Standardization / International Electrotechnical Commission, Cybersecurity - Guidelines for Internet Security, ISO/IEC 27032:2023, 2nd ed. Geneva, Switzerland: ISO/IEC, Jun. 2023. [Online]. Available: https://www.iso.org/standard/76070.html.

[21] IBM Security and Ponemon Institute, Cost of a Data Breach Report 2020. Armonk, NY, USA: IBM Corp., 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

[22] European Network and Information Security Agency (ENISA), Threat Landscape for Ransomware Attacks. Athens, Greece: ENISA, 2022. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks.

[23] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Hoboken, NJ, USA: Wiley, 2020.

[24] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data (GDPR). Brussels, Belgium: Official Journal of the European Union, 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

[25] C. J. Fombrun, N. A. Gardberg, and J. M. Sever, "The reputation quotient: A multi-stakeholder measure of corporate reputation," Journal of Brand Management, vol. 7, no. 4, pp. 241–255, 2000. doi: 10.1057/bm.2000.10.

[26] J. Abawajy, "User preference of cyber security awareness delivery methods," Behaviour & Information Technology, vol. 33, no. 3, pp. 237–248, 2014. doi: 10.1080/0144929X.2012.708787.

[27] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the Gordian knot: A look under the hood of ransomware attacks," in Proc. 12th Int. Conf. Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), Lecture Notes in Computer Science, vol. 9148, Milan, Italy, Jul. 2015, pp. 3–24. doi: 10.1007/978-3-319-20550-2_1.

[28] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, "CryptoLock (and Drop It): Stopping ransomware attacks on user data," in Proc. 36th IEEE Int. Conf. Distributed Computing Systems (ICDCS), Nara, Japan, Jun. 2016, pp. 303–312. doi: 10.1109/ICDCS.2016.46.

[29] Maastricht University, Response of Maastricht University to FOX-IT Report. Maastricht, Netherlands: Maastricht University, Feb. 5, 2020. [Online]. Available: https://www.maastrichtuniversity.nl/file/reponseofmaastrichtuniversitytofox-itreportpdf.

[30] BBC, "How hackers extorted $1.14m from University of California, San Francisco", Jun. 2020. [Online]. Available: https://www.bbc.com/news/technology-53214783.

[31] P. Gooch, C. Gribben, and R. Davis, "The technology risk landscape - considerations for boards," Deloitte UK, London, UK, Jan. 2026. [Online]. Available: https://www.deloitte.com/uk/en/services/audit-assurance/perspectives/technology-risk-landscape.html.

[32] European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive). Brussels, Belgium: European Commission, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

[33] Sophos, The State of Ransomware 2025. Abingdon, UK: Sophos Ltd., Jun. 2025. [Online]. Available: https://www.sophos.com/en-us/content/state-of-ransomware.

[34] FBI, CISA, Europol EC3, and NCSC-NL, "#StopRansomware: Akira Ransomware," Joint Cybersecurity Advisory AA24-109A, U.S. Cybersecurity and Infrastructure Security Agency, Washington, DC, USA, Apr. 18, 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a.

[35] J. Nutland and M. Szeliga, "Threat spotlight: Akira ransomware continues to evolve," Cisco Talos Blog, Cisco, Oct. 2024. [Online]. Available: https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/.

[36] MITRE Corporation, MITRE ATT&CK® Enterprise Matrix, v13.1. Bedford, MA, USA: MITRE Corporation, Apr. 2023. [Online]. Available: https://attack.mitre.org/versions/v13/.

[37] H. R. Nikkhah and V. Grover, "An empirical investigation of company response to data breaches," MIS Quarterly, vol. 46, no. 4, pp. 2163–2196, Dec. 2022. doi: 10.25300/MISQ/2022/16609.

[38] R. L. Heath and H. D. O'Hair, Eds., Handbook of Risk and Crisis Communication. New York, NY, USA: Routledge, 2009.

[39] D. A. Aaker, Building Strong Brands. New York, NY, USA: Free Press, 1996.

[40] S. Panda, S. C. Pandey, A. Bennett, and X. Tian, "University brand image as competitive advantage: a two-country study," *International Journal of Educational Management*, vol. 33, no. 2, pp. 234–251, 2019. doi: 10.1108/IJEM-05-2017-0119.

[41] X. Yaping, N. T. T. Huong, N. H. Nam, P. D. Quyet, C. T. Khanh, and D. T. H. Anh, "University brand: A systematic literature review," *Heliyon*, vol. 9, no. 6, p. e16825, 2023. doi: 10.1016/j.heliyon.2023.e16825.

[42] M. S. Balaji, S. K. Roy, and S. Sadeque, "Antecedents and consequences of university brand identification," *Journal of Business Research*, vol. 69, no. 8, pp. 3023–3032, 2016. doi: 10.1016/j.jbusres.2016.01.017.

[43] P. A. Rauschnabel, N. Krey, B. J. Babin, and B. S. Ivens, "Brand management in higher education: the university brand personality scale," *Journal of Business Research*, vol. 69, no. 8, pp. 3077–3086, 2016. doi: 10.1016/j.jbusres.2015.08.018.

[44] M. A. Mateus, A. G. Rincón, F. J. Acosta, I. R. Soler, and D. R. Valero, "Keys to managing university reputation from the students' perspective," *Heliyon*, vol. 10, no. 21, p. e38827, 2024. doi: 10.1016/j.heliyon.2024.e38827.

[45] P. Foroudi, Q. Yu, S. Gupta, and M. M. Foroudi, "Enhancing university brand image and reputation through customer value co-creation behaviour," *Technological Forecasting and Social Change*, vol. 138, pp. 218–227, 2019. doi: 10.1016/j.techfore.2018.09.030.

[46] W. T. Coombs, Ongoing Crisis Communication: Planning, Managing, and Responding, 4th ed. Thousand Oaks, CA, USA: Sage, 2014.

[47] International Organization for Standardization / International Electrotechnical Commission, Information Technology - Information Security Incident Management - Part 1: Principles and Process, ISO/IEC 27035-1:2023, 2nd ed. Geneva, Switzerland: ISO/IEC, Feb. 2023. [Online]. Available: https://www.iso.org/standard/78973.html.

[48] International Organization for Standardization, Security and Resilience - Business Continuity Management Systems - Requirements, ISO 22301:2019, 2nd ed. Geneva, Switzerland: ISO, Oct. 2019. [Online]. Available: https://www.iso.org/standard/75106.html.

[49] J. W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 4th ed. Thousand Oaks, CA, USA: Sage, 2014.

[50] J. F. Hair Jr, M. Page, and N. Brunsveld, *Essentials of Business Research Methods*, 4th ed. New York, NY, USA: Routledge, 2019.

[51] N. Jain, "Survey versus interviews: Comparing data collection tools for exploratory research," *The Qualitative Report*, vol. 26, no. 2, pp. 541–554, 2021. doi: 10.46743/2160-3715/2021.4492.

[52] I. Alam, "Fieldwork and data collection in qualitative marketing research," *Qualitative Market Research: An International Journal*, vol. 8, no. 1, pp. 97–112, 2005. doi: 10.1108/13522750510575462.

[53] E. Granot, T. G. Brashear, and P. C. Motta, "A structural guide to in-depth interviewing in business and industrial marketing research," *Journal of Business & Industrial Marketing*, vol. 27, no. 7, pp. 547–553, 2012. doi: 10.1108/08858621211257310.

[54] S. Kvale and S. Brinkmann, InterViews: *Learning the Craft of Qualitative Research Interviewing*, 2nd ed. Thousand Oaks, CA, USA: Sage, 2009.

[55] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students*, 8th ed. Harlow, UK: Pearson, 2019.

[56] V. Braun and V. Clarke, "Using thematic analysis in psychology," Qualitative Research in Psychology, vol. 3, no. 2, pp. 77–101, 2006. doi: 10.1191/1478088706qp063oa.

[57] V. Braun and V. Clarke, "Reflecting on reflexive thematic analysis," Qualitative Research in Sport, Exercise and Health, vol. 11, no. 4, pp. 589–597, 2019. doi: 10.1080/2159676X.2019.1628806.

[58] Y. S. Lincoln and E. G. Guba, Naturalistic Inquiry. Beverly Hills, CA, USA: Sage, 1985.

[59] J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 5th ed. Thousand Oaks, CA, USA: Sage, 2018.

[60] IPLeiria, "About Us," Polytechnic Institute of Leiria, n.d. [Online]. Available: https://www.ipleiria.pt/en/about-us/institution/about-us/.

[61] E. Cruz, "Ataque informático deixa Politécnico de Leiria sem acesso a plataforma e-learning," Jornal de Leiria, May 2, 2023. [Online]. Available: https://www.jornaldeleiria.pt/noticia/ataque-informatico-deixa-politecnico-de-leiria-sem-acesso-a-plataforma-e-learning.

[62] Observador, "Politécnico de Leiria sem evidências de roubo de informação sensível após ataque informático," Observador, May 13, 2023. [Online]. Available:

https://observador.pt/2023/05/13/politecnico-de-leiria-sem-evidencias-de-roubo-de-informacao-sensivel-apos-ataque-informatico/.

[63] Público, "Polícia Judiciária investiga ataque informático no Instituto Politécnico de Leiria," Público, May 4, 2023. [Online]. Available: https://www.publico.pt/2023/05/04/local/noticia/policia-judiciaria-investiga-ataque-informatico-instituto-politecnico-leiria-2048468.

[64] FalconFeeds.io [@FalconFeedsio], "Akira #ransomware group added IPLeiria Student Branch to their victim list. #Portugal #Akira #darkweb #databreach," X (formerly Twitter), May 12, 2023, 02:30 UTC. [Online]. Available: https://x.com/FalconFeedsio/status/1656909570990813186.

[65] FalconFeeds.io, "Double Extortion Report - May 2025," FalconFeeds Threat Intelligence Platform, 2025. [Online]. Available: https://falconfeeds.io/reports/double-extortion-may2025.

Appendices

Appendix A – Interview Scripts

Contexto Geral

O Instituto Politécnico de Leiria foi alvo de um ataque de ransomware em maio de 2023, impactando diversos serviços essenciais da instituição. De forma a melhor compreender as consequências deste evento, a resposta por parte da instituição e as lições aprendidas, serão conduzidas entrevistas semi-estruturadas com diferentes partes interessadas.

O objetivo destas entrevistas é recolher informações detalhadas sobre o ataque a partir de três perspetivas focadas em impactos distintos: técnico, reputacional/comunicacional e operacional. Através destes testemunhos, pretende-se obter uma visão abrangente do impacto do ataque, identificar melhorias a implementar e reforçar a resiliência digital do IPLeiria.

Cada entrevista seguirá um guião adaptado ao grupo/indivíduo específico, abordando questões relevantes para o estudo e a análise do incidente, bem como para a mitigação de eventos futuros. A participação de todos os entrevistados será fundamental para extrair conclusões úteis e construir um plano de ação mais robusto.

Entrevista com DSI – Perspetiva Técnica

Esta entrevista tem como finalidade obter uma visão técnica detalhada do ciberataque que afetou o IPLeiria. Pretende-se compreender como o ataque foi detetado, quais as vulnerabilidades exploradas, as medidas adotadas para mitigar os danos e de que forma a instituição pode reforçar a sua postura de cibersegurança no presente e futuro. Esta conversa será essencial para uma análise aprofundada da resposta técnica ao incidente.

Blocos Temáticos

A. Contextualização do ataque

- Como e quando foi detetado o ataque?
- Que mecanismos de monitorização de eventos estavam implementados? São geridos internamente ou por um prestador externo?
- Identificaram alguma falha nos processos de monitorização e deteção?
- Qual foi a primeira resposta da equipa técnica ao identificar a ameaça?
- Existiram sinais prévios ou alertas que pudessem ter antecipado o ataque?
- Em que momento perceberam que se tratava de um ataque de ransomware e não outro tipo de ameaça?
- Houve alguma dificuldade inicial em obter recursos ou apoio externo para lidar com o ataque?
- O ataque foi comunicado e acompanhado pelas autoridades competentes?
- O IPLeiria dispunha de uma Política de Segurança da Informação e/ou plano de contingência ativo (ou algum tipo de preparação para eventos desta natureza) à data do incidente?
- Seguem atualmente alguma framework ou standard de gestão de incidentes reconhecido internacionalmente, como ISO 27035, NIST, ENISA, SANS, ou outros?

B. Natureza e extensão do ataque

- Qual foi o vetor de entrada do ransomware Akira?
- Que sistemas e infraestruturas foram mais afetados?
- Foi identificada alguma tentativa de exfiltração de dados?
- Existem indícios de que o ataque tenha sido direcionado especificamente ao IPLeiria, ou terá sido um ataque oportunista?
- Houve contacto direto com os atacantes ou exigência de pagamento de resgate? Se sim, qual foi a estratégia adotada?

C. Resolução e mitigação

- Quais foram as principais ações tomadas para conter e eliminar a ameaça?
- Que ferramentas ou procedimentos foram utilizados na recuperação dos sistemas?
- Quanto tempo foi necessário para restaurar os serviços críticos?
- Quais os principais desafios técnicos enfrentados durante o processo de recuperação?

- Foi necessário recorrer a especialistas ou empresas externas para vos apoiar durante o processo de recuperação?

D. Lições aprendidas e estratégias de prevenção

- Quais foram as principais lições retiradas deste incidente?
- Que medidas de segurança foram implementadas após o ataque, com base nas lições aprendidas?
- O incidente originou alterações nas políticas internas de cibersegurança ou nos processos de gestão de incidentes?
- Como avalia a capacidade de resposta da equipa? Que áreas podem ser melhoradas?
- A equipa recebeu formação ou capacitação específica após o incidente?
- Considera que a cultura de cibersegurança da instituição deve ser reforçada? Se sim, de que forma?
- Há alguma consideração adicional que gostaria de partilhar?

Entrevista com Departamento de Comunicação – Perspetiva Reputacional

Esta entrevista tem como objetivo compreender o impacto do ataque na reputação e imagem institucional do IPLeiria, pretendendo-se analisar a forma como a comunicação da crise foi gerida, os desafios enfrentados na transmissão da informação à comunidade académica e ao público em geral, e as medidas implementadas para restaurar a confiança na instituição.

Blocos Temáticos

A. Comunicação de crise

- Pode fazer uma breve descrição cronológica daquilo que aconteceu no período do ataque?
- Já existia algum plano de contingência (ex: Manual de Crise, protocolos, etc.) ou preparação para o evento? Se sim, foi seguido nos momentos de crise e pós-crise?

- Como foi gerida a comunicação interna e externa durante e após o ataque?
- Quais foram as principais preocupações ao comunicar a situação?
- Que canais foram utilizados para manter a comunidade informada?
- Foi necessário recorrer a assessoria externa para gerir a crise?
- Houve dificuldades em articular uma mensagem clara e transparente sobre o ataque?

B. Impacto na imagem e confiança da instituição

- O incidente foi divulgado nos meios de comunicação social. O que foi dito? Essa divulgação tevem repercussões que agravaram a crise?
- Com um foco particular nas redes sociais (e.g., X, Facebook, entre outros), houve alguma monitorização daquilo que foi falado pela comunidade acerca do evento? Houve alguma atividade/reação ao ataque nas redes sociais? Se sim, que conclusões foram retiradas?
- Como avalia a reação dos estudantes, docentes e outros stakeholders?
- A instituição enfrentou críticas ou desconfiança por parte da comunidade?
- Foram identificados impactos na captação de novos estudantes ou parceiros?
- Houve impacto na perceção da segurança digital da instituição?

C. Lições aprendidas e estratégias futuras

- Com base nas lições aprendidas, que melhorias puderam/podem ser feitas na comunicação institucional para futuras crises?
- O ataque influenciou a estratégia de marca do IPLeiria? Se sim, de que forma?
- Foram implementadas novas diretrizes de comunicação para eventos de cibersegurança?
- Que tipo de mensagens institucionais foram mais eficazes na recuperação da confiança da comunidade?
- Foi criado algum plano de comunicação preparado especificamente para futuros incidentes de naturezas similares?
- Alguma mensagem final que queira partilhar?

Appendix B – Selection of National Media Coverage of the IPLeiria Ransomware Incident

SOCIEDADE

Ataque informático deixa Politécnico de Leiria sem acesso a plataforma e-learning

2 MAI 2023 17:10

Instituição de ensino superior desconhece ainda danos provocados pelo ciberataque

Instituição já tinha sido alvo de algumas tentativas de phishing

Ricardo Graça/Arquivo

https://www.jornaldeleiria.pt/noticia/ataque-informatico-deixa-politecnico-de-leiria-sem-acesso-a-plataforma-e-learning

Suspeita de ataque informático condiciona atividade do Politécnico de Leiria

Este artigo tem mais de 2 anos

Ataque informático ao Politécnico de Leiria provoca constrangimentos no acesso às plataformas da instituição de ensino superior.

0

https://observador.pt/2023/05/03/suspeita-de-ataque-informatico-condiciona-atividade-do-politecnico-de-leiria/

PIRATARIA INFORMÁTICA

Polícia Judiciária investiga ataque informático no Instituto Politécnico de Leiria

Ataque informático pôs 14 mil alunos sem acesso à Internet nas escolas e residências do Instituto Politécnico de Leiria. Foi criado um *site* provisório, mas as aulas estão condicionadas.

Marta Leite Ferreira

4 de Maio de 2023, 17:03

O acesso à internet está cortado desde terça-feira nas escolas e residências do Instituto Politécnico de Leiria por causa de um ataque informático REUTERS/DADO RUVIC

https://www.publico.pt/2023/05/04/local/noticia/policia-judiciaria-investiga-ataque-informatico-instituto-politecnico-leiria-2048468

CIBERCRIME

Politécnico de Leiria entre as vítimas da operação de *ransomware* Akira

Um grupo a usar o golpe de *ransomware* Akira identificou o Instituto Politécnico de Leiria entre as vítimas numa nota na *dark web*, após um ataque informático no começo de Maio.

Karla Pequenino

12 de Maio de 2023, 23:26 (actualizado a 13 de Maio de 2023, 4:42)

Página do grupo Akira na *dark web* - partilhada pela Falcon Feeds DR

https://www.publico.pt/2023/05/12/tecnologia/noticia/politecnico-leiria-vitimas-operacao-ransomware-akira-2049524

Politécnico de Leiria sem evidências de roubo de informação sensível após ataque informático

Este artigo tem mais de 2 anos

Ainda "não foram detetadas" quaisquer evidências de que tenha sido roubada informação sensível do Politécnico de Leiria, informa a instituição. No dia 2, o IPL foi alvo de um ataque informático.

https://observador.pt/2023/05/13/politecnico-de-leiria-sem-evidencias-de-roubo-de-informacao-sensivel-apos-ataque-informatico/