sustainability

MDPI

Article

Impact of Critical Infrastructure Cyber Security on the Sustainable Development of Smart Cities: Insights from Internal Specialists and External Information Security Auditors

Iryna Leroy [1,2,*], Iryna Zolotaryova [3] and Serhii Semenov [4]

[1] Quality and Management Department, Université de Lorraine, 54000 Nancy, France
[2] European Security and Defence Collage, 1000 Brussels, Belgium
[3] Information Systems Department, Simon Kuznets Kharkiv National University of Economics, 61166 Kharkiv, Ukraine; iryna.zolotaryova@hneu.net
[4] Cyber Security Department, University of the National Education Commission, ul. Podchorążych 2, 33-332 Kraków, Poland; serhii.semenov@uken.krakow.pl
* Correspondence: iryna.leroy@hneu.net

Abstract: This study aims to describe and assess the impact of critical infrastructure (CI) cybersecurity issues on the sustainable development of smart cities. This study highlights the integration of PayTech systems into the broader CI landscape, highlighting their impact on maintaining economic stability and ensuring the smooth operation of city services. Key companies within smart regions, particularly those operating in the payment industries, are essential to maintaining the functionality of critical services. These companies facilitate the processing of services provided to citizens, enabling access to vital municipal services. As key players in the PayTech and online e-commerce sectors, they form a crucial part of modern critical infrastructure, operating within an ever-evolving digital environment. This study examines the recovery processes employed after cyberattacks, focusing on the differing perspectives of internal and external professionals. It identifies significant differences in the perceptions of recovery strategies among internal stakeholders, such as investor relations (IR) teams, reputation management (RM) experts, and Chief Information Security Officers (CISOs), who represent critical infrastructure companies. Additionally, it explores the roles of external auditors, who provide impartial emergency support and perform specialized recovery tasks. Importantly, this study underscores the current attitudes toward future information security strategies and their influence on the financial recovery and reputation of reliable companies following cyber incidents. This research contributes to the existing knowledge by shedding light on the perspectives of both a company's internal and external specialists involved in the recovery process and cyber resilience strategies in critical infrastructure sectors.

Keywords: sustainable development of smart city; information security; critical infrastructure; information security assessment; digital; smart regions; reputation management; cyber autonomy; cyber resilience

Academic Editor: Maxim A. Dulebenets

Received: 12 December 2024
Revised: 17 January 2025
Accepted: 25 January 2025
Published: 1 February 2025

Citation: Leroy, I.; Zolotaryova, I.; Semenov, S. Impact of Critical Infrastructure Cyber Security on the Sustainable Development of Smart Cities: Insights from Internal Specialists and External Information Security Auditors. *Sustainability* **2025**, *17*, 1188. https://doi.org/10.3390/su17031188

1. Introduction

1.1. Motivation

Currently, the functioning of modern society is increasingly dependent on critical infrastructure (CI). Ensuring the resilience of smart regions requires integrating cybersecurity measures with effective recovery approaches, creating a foundation for sustainable growth while mitigating risks tied to their reliance on interconnected CI systems. This infrastructure includes systems that support the operation of key sectors of the economy, such as energy, transportation, finance, and communications. This inherent dependence creates significant risks related to cybersecurity. In the digital age, in which most transactions are conducted automatically through online payment systems and PayServices, FinTech companies play a pivotal role in supporting smart region ecosystems. These companies operate within a highly regulated market, closely monitored by governments and regional authorities, ensuring compliance and integration within the broader infrastructure of smart regions. Understanding the interplay between these ecosystems and the recovery approaches of internal and external professionals is crucial for improving response mechanisms and fostering resilient cybersecurity strategies. Ensuring the resilience of smart regions requires integrating cybersecurity measures with effective recovery approaches, creating a foundation for sustainable growth while mitigating risks tied to their reliance on interconnected CI systems.

In recent times, there has been a surge in cyber intrusions and cyberattacks on CI. The growing trend of cyberattacks is driven by the following factors:

1. Increasing complexity and interconnectedness of digital systems: Modern systems are becoming more complex, which provides more opportunities for malicious actors.
2. Greater accessibility of cybercrime: Cybercrime has become more accessible with the availability of ready-made tools and services, allowing even inexperienced hackers to launch attacks.
3. Increasing value of data: Data have become valuable assets, making them an attractive target for cybercriminals.

Cyberattacks on CI pose a serious threat that can lead to significant economic losses, social disruptions, and even threats to national security.

Despite the growing threat of cyberattacks, there remains a significant gap in understanding how companies operating in the CI sector recover from such incidents. The issue is particularly pronounced when comparing the approaches to recovery between internal specialists (investors, RM managers, and CISOs) and external information security auditors.

Existing research on CI cybersecurity primarily focuses on the technical aspects of protection against cyberattacks, paying insufficient attention to recovery after incidents and RM. In particular, there is a lack of deep understanding of how different groups of specialists involved in the recovery process perceive and implement recovery strategies, as well as how these differences affect the efficiency and speed of recovery.

Understanding the differences in recovery approaches between internal and external specialists after cyberattacks is crucial for developing more effective cybersecurity strategies and enhancing the resilience of CI.

1.2. State of the Art

As a cybersecurity awareness and education manager, Esther Solomon Edun's research, based on her Ph.D. in Cyber Security from Cranfield University, highlights the significance of stakeholder interactions in fostering positive cybersecurity behavior within organizations. The focus is on overcoming the information security barrier among top-level executives, information security experts, and non-IT professionals, with the ultimate aim of aligning security objectives with the broader business goals [1] In light of these challenges, "The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption" report shows that 80% of critical infrastructure organizations experienced a ransomware cyberattack. That causes staggering financial and societal repercussions when critical infrastructure is disrupted. The report also found that the combination of the ever-accelerating digital transformation and the limited availability of skilled cybersecurity workers has resulted in several high-profile attacks on critical infrastructure. In response, many C-suite executives have become heavily involved in the decision-making and oversight of their organization's cybersecurity practices. In fact, more than 60% of those who are centralizing IT governance report to the CISOs. In addition, 62% are supportive of government regulators enforcing mandatory and timely reporting of cybersecurity incidents. The report also found that the combination of the ever-accelerating digital transformation and the limited availability of skilled cybersecurity workers has resulted in several high-profile attacks on critical infrastructure [2]. There are cross-country differences in opinion regarding information security processes that could affect the assessment of the company's reputation among individuals in the Czech Republic and Belgium: 58% of Czech individuals "agree", whereas only 48% of those from Belgium agree. However, Belgian respondents are more unequivocally convinced of this need, encompassing 32% of the total mass of respondents, which is three times higher than the proportion of respondents in the Czech Republic who gave the same response. Given the intensity of public concern about information security, reputational issues should not be short-term, ad hoc, and defensive but should have a strategic view and long-term planning to defend an entity's reputation [3].

Given the importance of strategic planning in addressing reputational challenges in the context of information security [3], researchers have devoted significant attention to improving the security of smart cities and regions, as well as ensuring their sustainable development in the face of existing risks. This includes the analysis of unique threats, vulnerabilities, and protection strategies needed for critical infrastructure in these urban environments.

Recent studies have highlighted the multifaceted challenges faced by sustainable smart cities, encompassing technological, social, economic, and environmental aspects. The research [4] provides a comprehensive review of future trends and barriers to the implementation of smart cities. Using the Rapid Review methodology, the study identifies key obstacles such as data privacy issues, the necessity of citizen engagement, and challenges in adopting renewable energy sources. The authors argue that the interdependence of technology and sustainability plays a central role in urban planning, offering recommendations for improving governance mechanisms and developing collaborative policies to enhance resilience. These findings align with broader discussions on the need to integrate critical infrastructures such as energy, transportation, and PayTech systems to strengthen economic and social stability in smart urban environments.

The study presented in article [5] focuses on the security of smart cities, including their cybersecurity, through the lens of interaction with critical infrastructure. The authors emphasize the importance of integrating security measures into the strategic planning of smart cities to ensure their long-term sustainability, including the use of smart systems for managing transportation, energy, and infrastructure. Unfortunately, the study covers only large and medium-sized cities in Poland, which somewhat limits the practical applicability of the findings in an international context.

The main objective of article [6] is to investigate cybersecurity issues in smart cities, including the analysis of the technologies used, key challenges, and providing future recommendations. The article focuses on such components of a smart city as smart grids, smart buildings, transportation systems, and healthcare, as well as the use of deep learning methods to ensure security. Most of the content is theoretical in nature, discussing potential threats and proposing solutions, but practical implementation is weakly covered. For example, there is no in-depth analysis of security integration with PayTech systems, which is an important aspect of critical infrastructure.

One of the important aspects of the sustainable development of smart regions is the integration of financial technologies, such as mobile payment systems Apple Pay and Samsung Pay, into critical infrastructure. Research [7] shows that mobile payment services have a significant impact on the value of firms involved in downstream and upstream alliances, especially through increased innovation capacity and recovery resources. These results emphasize the importance of embedding financial technologies in critical components of smart city infrastructure, which can strengthen resilience to cyber threats and increase citizens' trust in digital services.

Article [8] aims to explore the role of digital finance in sustainable economic development, focusing on its impact on financial inclusion, environmental sustainability, and macroeconomic stability. The article also analyses the regulatory challenges and priorities facing digital finance in an era of accelerated digital transformation. At the same time, the article discusses digital finance in a broad context but does not provide a detailed analysis of specific technological solutions such as PayTech systems.

A study [9] found that the security of mobile payment services (MPS) platforms and technologies has a significant impact on users' perception of metrics such as convenience, interoperability, and trust, which ultimately contributes to the sustainable development of smart cities. The paper uses an online survey of 356 users to evaluate the mobile payment security model, which allows us to draw conclusions based on concrete empirical data. Unfortunately, most of the data used in the paper are related to the South Korean market, which may limit their applicability in a global context.

Article [10] provides a valuable overview of the key challenges and potential solutions for ensuring cybersecurity in smart cities, but it lacks a deeper analysis of specific threats to PayTech systems and financial sustainability. The use of the proposed solutions by external auditors and specialists could contribute to increasing citizens' trust in urban services and minimizing cybersecurity risks, thereby promoting long-term sustainable development.

The authors of article [11] explore the relationship between financial technologies and security by conducting a statistical analysis of various variables, such as technology culture, competencies and skills, and experience in information security. However, the adaptation of FinTech factors to the operating conditions of critical infrastructure systems in smart cities is not addressed in the article.

In the context of smart cities, where the integration of PayTech and other digital technologies is becoming increasingly prevalent, the issues of security and post-attack recovery gain particular significance. Smart cities require a comprehensive approach to cybersecurity that considers both protection and effective recovery from incidents to ensure the resilience and trustworthiness of digital services.

Traditional cybersecurity methods prioritize protection through technologies like firewalls, encryption, and intrusion detection. In contrast, this research focuses on post-attack recovery, particularly the roles of internal and external specialists in managing reputation and business continuity. This study's focus is on the unique FinTech field and its specialists, highlighting differences in perceptions among IR, RM, and CISO specialists, as well as external information security auditors, regarding recovery strategies and responses to persistent cyberattacks and their aftermath.

Our research [12] provides a comprehensive analysis of technologies that can contribute to the development of smart cities, emphasizing the importance of citizen participation and the use of decentralized technologies such as blockchain and ICT to improve urban processes. However, the absence of specific examples and insufficient attention to financial infrastructure (PayTech) limits the practical application of the proposed solutions. In the context of sustainable development of smart cities, articles like this can serve as the foundation for implementing strategies aimed at increasing transparency and trust, which are important for long-term stability and growth.

Although the implication of cybersecurity stretches across all business regions, most of the focus on cybersecurity in the business world centers on the PayTech financial sector (or PayTech—technology-driven solutions for electronic payments, transactions, and financial services) because financial information attack leads to a negative stock market reaction [13]. Moreover, compliance with security standards, especially for companies operating in the finance and payment industries, is the "license to operate". These companies must employ external cyber auditors, as well as involve their own internal employees—cybersecurity specialists. This study addresses a significant gap in understanding recovery strategies after cyberattacks on critical infrastructure, particularly by comparing the approaches of internal stakeholders and external auditors. While the research highlights divergent perspectives among internal specialists, such as IR, RM, CISOs, and external auditors, several challenges emerge.

In connection with these differing perspectives, research shows that external auditors pay more attention to cybersecurity incidents and can also apply more pressure, as external auditors are responsible for providing reasonable financial assurance statements that a company is presented fairly and in conformity with information security standards [14]. Nevertheless, for example, according to an Ernst and Young survey, only 7% of Fortune 100 companies disclosed that they perform cyber incident simulations or tabletop exercises, and only 16 percent of companies disclosed the use of an external independent consultant to help management with cybersecurity-related practices [15].

Consistent with prior studies, in this research, within our analyses, we have identified a few current problems: the disparity in approaches to recovering from cyberattacks between internal company stakeholders and external information security auditors, particularly in the strategy for recovering a company's reputation that has been damaged by cyber incidents. Emphasizing the need for a better understanding of different approaches and the prevention of information security breaches and reputation damage caused by cyber incidents, this study proposes two research questions (RQs): RQ1: Do internal stakeholders (IR, RM, and CISOs) and external auditors differ in their viewpoints on recovery strategies following cyberattacks? This issue is important because differences in approach can make it difficult to coordinate recovery from cyberattacks. For example, internal professionals, such as CISOs and reputation managers, focus on maintaining the continuity of operations and minimizing reputational risk. External auditors, on the other hand, may emphasize compliance and independent assessment. Understanding these differences allows for more balanced and effective recovery strategies. RQ2: Do internal stakeholders (IR, RM, and CISOs) and external auditors differ in their viewpoints on reputation defense and the role of the European Union (EU) outside its jurisdiction in cyberattacks? This problem raises the important issue of the cross-border nature of threats, especially for critical infrastructure companies operating in international markets. The EU's role in protecting infrastructure outside its jurisdiction is to provide regulatory and organizational support. By examining these aspects, it is possible to identify coordination gaps and develop approaches that will strengthen global cyber resilience.

To address the research questions listed above, the current study contributes to existing research in several ways. First, we consider previous studies that focus on cyberattacks' impact on a company's reputation, which in turn impacts the company's share price, as serious business interruptions after a breach have a significant effect on the value of companies because of their impact on cash flow [16]. According to David Chinn, senior partner at McKinsey: "In most cases, company share prices bounce back from business interruption". In particular, such damage can be of greater importance and higher impact if the company is an essential part of critical infrastructures. New risks, vulnerabilities, and threats can result in political confrontations; therefore, critical infrastructure must be protected and resilient [17].

Second, we consider existing frameworks and regulations to enforce several information security frameworks and regulations that information security specialists must follow whenever they are internal or external employees. For instance, the European Central Bank (ECB) imposes specific information security practices that are crucial for ensuring cybersecurity in critical infrastructure companies [18].

In the EU is the Network and Information Systems Directive, Version 2 (NIS2) directive (proposed by the National Institute of Standards and Technology), which aims to establish a common level of cybersecurity in the EU, with the aim of ensuring the technological and digital sovereignty of the European Union in the cyber field, as well as managing risk and reputation. It requires the EU Member States to identify and assess risks to the security of network and information systems and to take appropriate measures to manage those risks [19]. This is particularly important for financial markets and company reputation recovery after cyberattacks [20]. Furthermore, firms with stronger reputations are more likely to weather market volatility better than those with weaker reputations.

Third, this research examines the view on the boundary conditions for implementing recovery steps after cyber incidents, such as project management methodologies and collaboration with EU authorities. This holistic approach ensures that risk-based decision-making is integrated into every aspect of the organization, from the strategic to the tactical level. The PM^2 project management methodology (project management methodology promoted by the European Commission), which was developed and supported by the European Commission, emphasizes the importance of risk management in recovering from cyberattacks. According to the European Commission, the PM^2 methodology uses a structured risk management process that includes identifying risks, assessing their impact, and developing and implementing mitigation measures to minimize their impact. In addition to the PM^2 methodology, Lean Six Sigma offers a continuous improvement methodology for managing risks in the cybersecurity context. This methodology begins with quantifying risk and then focuses on prevention, detection, and remediation. Consequently, Lean Six Sigma is used to mitigate risks in three ways, including preventing incidents from happening, detecting incidents as early as possible, and minimizing the impact of incidents that occur [21]. By focusing on these three elements, organizations can minimize the damage caused by cyberattacks and improve their resilience to future threats.

Finally, our study aims to address the research questions listed above by examining different viewpoints on different viewpoints on reputation defense and the utilization of RM tools, which have the potential to restore the value of a company's shares following a cyber incident. Such RM tools include transparency in revealing cyberattack incidents within 24 h, constant communication with key stakeholders through regular channels, maintaining company news channels for higher-frequency communication, conducting training for company management and employees on incidents and communication, maintaining security through secure backup systems and system design review, continuous improvement through feedback analysis and addressing concerns, and reporting actions taken before, during, and after incidents.

Dealing with information security attacks requires broad knowledge and involves people with knowledge from different fields, including IR, reputation relations, and information security; each of these areas must have a specialist or single point of contact for these tasks. For example, IR managers are responsible for effectively communicating an organization's cybersecurity initiatives and risk management practices to investors, building trust and confidence in the company's ability to prevent cyberattacks. Reputation managers (RM) play a vital role in protecting the organization's public image and brand reputation during and after a cyberattack, implementing strategies to manage the incident, and restoring trust with stakeholders. CISOs lead the prevention of cyberattacks by implementing comprehensive security measures, assessing risks, and developing proactive strategies to safeguard critical information and systems from potential threats [22].

Table 1 illustrates the relationship among cyberattacks, the dynamics of company stock, and RM. The analysis also demonstrates the impact of the participation of professionals, such as IR and RM specialists, as well as CISOs, on the recovery process.

Table 1. Relationship among cyberattacks, dynamic of company stocks, and RM. Analyses of cyberattacks/biggest data breaches in the US and the EU that affected companies with more than 10,000 customers or more than 1000 employees and trade on a stock market.

Groups	Number RM Tools Used	Share Price Recovery Time	Share Value Lost	Companies with Internal CISOs Position	Companies with Internal IR or RM Position
Companies with Successful RM	7 RM tools 100%	11.2 days	1.1%	92%	97%
Companies with Poor RM	4 RM tools 58%	19.5 days	2.3%	81%	91%

Source: Int. J. Electronic Security and Digital Forensics, 2022 [22].

1.3. Objectives and Contributions

The main objective of this study is to assess various approaches to recovery after cyberattacks in critical infrastructure companies and to develop recommendations for effective strategies and tools for managing reputation and security after cyber incidents.

Research tasks:

- Provide valuable insights into the differences in the perception of recovery strategies between internal and external specialists.
- Identify the need for the integration of regulatory frameworks to establish a unified cybersecurity standard.
- Develop recommendations for effective strategies and tools for managing reputation and security following cyber incidents.

While standards such as the ISO 27000 series [1] provide a common framework for cybersecurity management, they do not take into account differences in how internal and external professionals perceive tasks. This study aims to explore these differences, as well as to identify additional factors, such as the role of RM and cross-border coordination involving the EU, that are important for cyber resilience.

The present study is one of the first to focus on domain-specific areas requiring complex and sophisticated knowledge, particularly in the Financial Technology (FinTech) sector, which has become a critical infrastructure for many companies. By selecting a representative sample of countries with a high concentration of international FinTech companies (such as SWIFT, originally a Belgian company from Brussels, and Mall Group, the largest e-commerce group in Central and Eastern Europe located in Prague. Czech Republic), this research comprehensively covers potential cybersecurity vulnerabilities in the FinTech industry from both external and internal perspectives. This approach is significant because it examines operational recovery strategies and explores the perception and prioritization of reputation defense, which is crucial for financial recovery following a cyberattack.

The companies selected for this study conduct a significant portion of their activities outside EU jurisdiction. This makes them vulnerable to cross-border cyber attacks that could affect EU interests, even if the attack occurs outside the EU territory.

The sample size was limited due to the specific nature of the survey, which focused on high-level professionals with significant experience in cyber security and critical infrastructure management. Including more respondents who do not have the necessary competencies could have reduced the quality and relevance of the findings. Thus, the sample was focused on highly qualified individuals to ensure the validity of the results.

2. Impact of CI Cyber Security on the Sustainable Development of Smart Cities

PayTech systems, as an essential part of the FinTech sector, provide the financial foundation for the functioning of smart cities. They ensure connectivity with energy supply, healthcare, and transportation systems, allowing citizens to make secure payments for utilities, transportation costs, and medical services (Figure 1). PayTech infrastructure is closely integrated with the city's critical services, making its protection vital to maintaining the resilience of urban life.

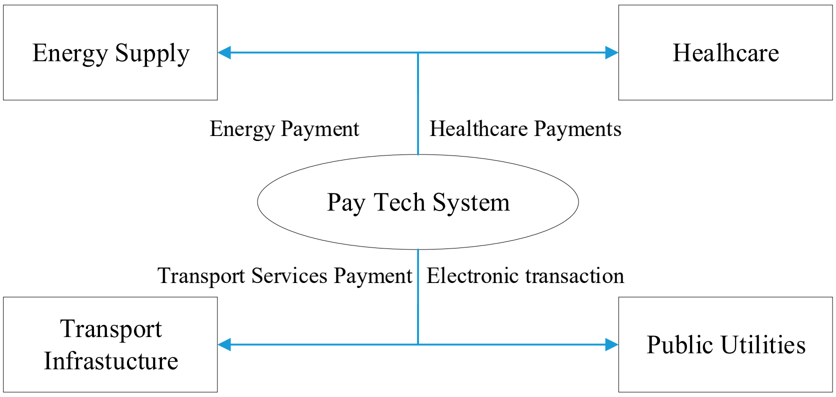

Figure 1. Integration of PayTech systems into the critical infrastructure of a smart city.

According to data collected through surveys among cybersecurity and FinTech professionals, both internal and external specialists recognize the importance of protecting financial systems for the sustainable functioning of all components of critical infrastructure. External auditors and information security specialists often focus on regulatory requirements and compliance with standards, such as GDPR, while internal specialists (e.g., CISOs) pay more attention to protecting operational processes and the company's reputation.

The data collected in this study revealed several key threats to PayTech infrastructure that can significantly affect sustainable development (Figure 2).

1. Financial Fraud and Data Manipulation.

One of the most significant threats to PayTech systems is financial fraud. It includes the following attacks:

- Phishing attacks: Attackers use phishing emails and messages to trick users into voluntarily providing their credentials or payment information. This not only puts the personal finances of citizens at risk but also creates risks for the entire financial system of a smart city.
- Malware attacks: Malicious software can infect users' devices and compromise their payment data. Such attacks may include keyloggers that record keystrokes to capture credentials.
- Transaction manipulation: Attackers can exploit vulnerabilities in PayTech systems to manipulate payment transactions. This could involve modifying transaction details (e.g., amount or recipient), which leads to financial losses.

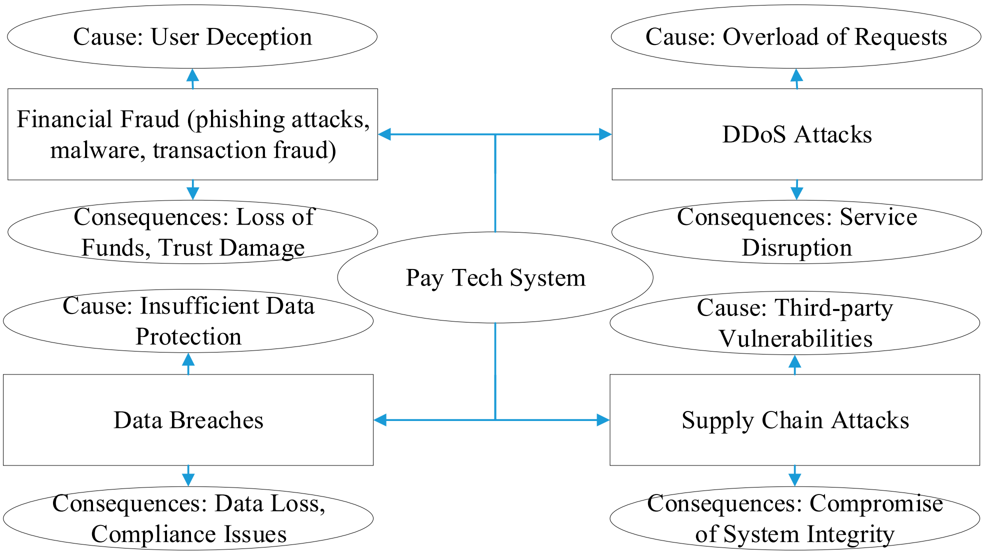
Cause: User Deception
Financial Fraud (phishing attacks, malware, transaction fraud)
Consequences: Loss of Funds, Trust Damage
Cause: Overload of Requests
DDoS Attacks
Consequences: Service Disruption
Pay Tech System
Cause: Insufficient Data Protection
Data Breaches
Consequences: Data Loss, Compliance Issues
Cause: Third-party Vulnerabilities
Supply Chain Attacks
Consequences: Compromise of System Integrity

Figure 2. Main security threats to PayTech systems and their impact on the sustainable development of smart cities.

These threats undermine citizens' trust in PayTech systems, which can negatively impact the socio-economic sustainability of smart cities.

2. Denial of Service Attacks (DDoS Attacks).

DDoS attacks are aimed at overloading the PayTech system servers, which leads to the unavailability of services for users. The consequences of DDoS attacks are as follows:

- Disruption of operations: During an attack, PayTech systems may be unavailable to users, making it impossible to conduct financial operations, including payments for utilities, transportation, and medical services. This can create serious problems for citizens, as many smart city services require timely payment.
- Loss of trust: Frequent DDoS attacks can decrease trust in PayTech systems and lead users to abandon digital payments, which undermines the adoption of technologies in smart cities.

These attacks are often used as part of larger-scale cyberattacks to divert attention or paralyze security measures during other, more targeted attacks.

3. Data Privacy Breaches.

Data privacy is a fundamental factor for PayTech systems. Breaches of privacy can occur in the following cases:

- Personal data leakage: PayTech systems process a large amount of data, including the personal and financial information of users. Any data leak can lead to serious legal and financial consequences for the company and decrease user trust. Personal data leakage may occur due to both direct attacks and internal employee errors.
- Non-compliance with regulatory requirements: Under strict data protection regulations (e.g., GDPR), data leaks can lead to significant fines and losses for companies. External auditors involved in this study emphasize the importance of complying with regulatory requirements and implementing appropriate measures to protect data.

4. Attacks on Trust Chains and Supply Chains.

Many PayTech systems depend on trust chains and integration with third-party suppliers.

- Supply chain attacks: Attackers can target suppliers that provide software or services to PayTech systems. For example, compromising the security of a service provider can become an entry point for attackers into the main PayTech system.

- Trust chain attacks: Using unreliable partners or integrating with insufficiently protected systems can lead to data loss or compromise of PayTech systems. External auditors emphasize the importance of verifying trusted partners and constantly monitoring their security.

The conducted studies have shown that PayTech financial systems significantly impact the sustainable development of smart cities. In this regard, the following aspects of sustainability, directly formed by the financial system, can be highlighted:

- Economic Sustainability: The perception of financial sustainability, according to surveyed specialists, depends on the ability of PayTech systems to minimize the costs associated with cyberattacks. The sustainable development of cities directly depends on the ability to prevent financial losses and ensure access to critical financial services for businesses and citizens.
- Social Sustainability: PayTech infrastructure contributes to maintaining citizens' trust in the digital services of smart cities. During the surveys, RM specialists emphasized the importance of proper response to incidents to maintain social trust in PayTech systems and prevent users from switching to less convenient and less transparent forms of payment (e.g., cash).
- Environmental Sustainability: PayTech reduces the use of paper money and contributes to the transparency of cash flows. However, the data show that internal specialists particularly emphasize the need for the enhanced protection of these systems to ensure the sustainability and reliability of digital financial resources.

Figure 3 presents the chain economic consequences of cyberattacks and security breaches of PayTech systems as an element of critical infrastructure.

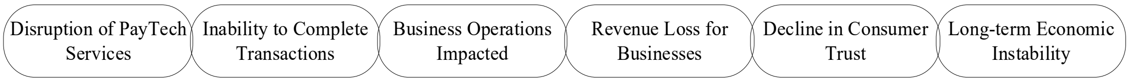
Disruption of PayTech Services
Inability to Complete Transactions
Business Operations Impacted
Revenue Loss for Businesses
Decline in Consumer Trust
Long-term Economic Instability

Figure 3. Chain economic consequences of PayTech system failures.

Thus, it is highlighted that protecting PayTech infrastructure from threats ensures the financial, social, and environmental sustainability of the critical infrastructure elements of a smart city, as well as maintains citizens' trust in urban services. The conducted studies, which include both internal and external perspectives of professionals in the FinTech field, emphasize the need to develop comprehensive approaches to protecting PayTech aimed at ensuring the long-term stability and sustainable growth of smart cities.

3. Data Collection

This section outlines the data collection process and methodology employed, which focuses on the distinct classification of specific roles, such as IR, RM, CISOs, and external information security auditors. The data were collected through the distribution of anonymous questionnaires among professionals belonging to these relevant occupational groups. Respondents were given assurance that their responses would be kept anonymous and confidential. The participants were divided into two groups based on their affiliation as either external or internal employees of a critical infrastructure company, enabling comparative analysis.

The present study is one of the first to focus on domain-specific areas requiring complex and sophisticated knowledge, particularly in the Financial Technology (FinTech) sector, which has become a critical infrastructure for many companies. By selecting a representative sample of countries with a high concentration of international FinTech companies (such as SWIFT, originally a Belgian company, and Mall Group, the largest e-commerce group in Central and Eastern Europe), this research comprehensively covers potential cybersecurity vulnerabilities in the FinTech industry from both external and internal perspectives. This approach is significant because it examines operational recovery strategies and explores the perception and prioritization of reputation defense, which is crucial for financial recovery following a cyberattack.

4. Methodology

We processed the data in two stages. On the first level, we mainly used a statistical analysis of the responses from the survey participants, which is based on the statistical methods. Then, in order to compare the differences, we utilized a concept analysis of the survey data, synthesis, and data deduction. The collection of data was carried out through the distribution of anonymous questionnaires among professionals belonging to relevant occupational groups of IR, RM, CISOs, and external information security auditors. Prior to participation, respondents were provided with information about the survey and invited to collaborate further.

Traditional cybersecurity methods prioritize protection through technologies like firewalls, encryption, and intrusion detection. In contrast, this research focuses on post-attack recovery, particularly the roles of internal and external specialists in managing reputation and business continuity. The originality of this study lies in its focus on the unique FinTech field and its specialists, highlighting differences in perceptions among IR, RM, and CISO specialists, as well as external information security auditors, regarding recovery strategies and responses to persistent cyberattacks and their aftermath.

While existing frameworks focus on attack prevention and detection, this study highlights divergent recovery approaches. External auditors tend to prioritize compliance and regulation, while internal teams focus on rapid response and reputation defense. This reveals a critical gap in existing frameworks, which may overlook the importance of reputational and financial recovery after a cyberattack.

Given the limited number of companies in the cybersecurity payment and FinTech sector, this study addresses potential vulnerabilities by examining countries with a dense presence of payment industry firms, allowing for insights from both internal and external viewpoints. The sample size of 120 participants, while appearing limited, is appropriate given the specific focus of this study on the niche field of FinTech and payment system cybersecurity. The companies surveyed represent critical players within the PayTech industry, which is particularly relevant, as these organizations are directly involved in digital financial transactions—one of the highest-risk areas for cyberattacks. Additionally, these companies operate in multinational environments, adding diversity to the sample, as they deal with varying regulatory frameworks, including European cybersecurity standards that are crucial to follow for FinTech companies who want to operate in the EU market.

The respondents were requested to indicate their level of agreement with ten statements using the Likert scale method, which encompasses a six-point scale ranging from "bad" to "positive". The survey was conducted across three companies that operate in similar domains. The first company, Mall Group a.s., is based in the Prague, Czech Republic, the second company, Worldline S.A., is based in Belgium, Bruselles (including their EU offices), and Advantio Ltd. is a qualified security assessor that is mainly based in Dublin, Ireland. Advantio is a specialized organization that has been certified and authorized for Payment Card Industry (PCI) security assessments. These companies operate within the PayTech and online e-commerce sectors, which play a critical role in essential infrastructure functioning within a dynamic digital landscape. The respondents have expertise and experience in their fields. Respondents received assurance that all responses were anonymous and confidential. The respondents were divided into two groups according to their professional roles. Survey data were collected between December 2022 and February 2023. The total number of respondent samples was 120, and of these, 47 were provided by external information security auditors.

The results obtained were used to draw conclusions. A comparative analysis among the companies revealed similarities in their respective domains of work, specifically their involvement in the PayTech industry and critical infrastructure business operations.

Due to the limited research conducted on recovery approaches for critical infrastructure companies after a cyberattack, particularly concerning insights from IR, RM, and CISO specialists and external information security auditors, and the absence of a definitive conclusion regarding these two groups, this research aims to address this gap in the academic literature. To fill this gap, this study's hypotheses are defined as follows:

Hypothesis 1. *There are discernible differences in the perceptions of specialists' roles in the recovery of cyberattacks among IR, RM, and CISO specialists and external information security auditors. The results of this study confirmed that the differences in the perceptions of cyberattack recovery professionals are significant. These differences highlight the need for coordination between internal and external actors to create integrated strategies that address both operational and regulatory aspects.*

Hypothesis 2. *The presence of RM tools can help restore the reputation of a company and simultaneously restore the value of its shares. While the results confirm the partial impact of RM tools on shareholder value recovery, further research is needed to assess the long-term effect of these tools. This may include analyzing industry specifics and the timeframes for incident recovery.*

The findings for hypothesis H1 emphasize the importance of RM tools, which are not adequately addressed in standards such as ISO 27000. These tools play a key role in restoring trust and minimizing financial losses after incidents.

Hypothesis 3. *Active intervention by the European Union (EU) is necessary to protect critical infrastructure owned by the EU but located outside its jurisdiction.*

The European Union's role in protecting critical infrastructure located outside its jurisdiction is driven by the global interconnectedness of economies and infrastructures. Cyberattacks on such facilities can lead to serious economic and social consequences, affecting both the companies themselves and EU states. EU engagement in these processes helps to equalize international cybersecurity standards and strengthen the resilience of global systems.

The survey methodology involved the incorporation of specific questions aligned with each hypothesis, as outlined in the subsequent numbering within the resultant table. These questions were designed to empirically assess the hypotheses in question (Table 2). Notably, the statistical analysis aimed to scrutinize the disparities in evaluations provided by distinct groups of experts. In line with this goal, the questions for the hypotheses were distributed as follows:

H1. *The questions pertinent to this hypothesis encompass Question 1, Question 2, Question 3, and Question 5.*

H2. *The hypothesis denoted as H1 is evaluated through the inclusion of Question 1, Question 2, Question 4, and Question 5.*

H3. *The assessment of H2 is contingent upon the responses to Question 4, Question 5, Question 6, and Question 7.*

Table 2. Companies' short profiles.

Company	Mall Group	Worldline SA	Advantio
Country	Czech Republic	Belgium	Ireland
Primary domain of business operations	E-commerce and online retail	Payment processing and digital solutions	Cybersecurity
Critical infrastructure operations	Full range of digital e-commerce services for the international market.	Marchant and acquirer solution	PCI security assessments

Source: crunchbase.com; bloomberg.com.

The questionnaire was developed using a Likert scale [23], which allowed standardized and reliable data to be collected. This approach is widely used in studies aimed at measuring the opinions of professionals. We limited the questionnaire to seven questions to minimize the cognitive load on respondents working in high-stress environments and to focus on key aspects, such as recovery strategies and RM. Future research involves extending the questionnaire for more in-depth analyses.

Subsequent to the statistical analysis, the results of the survey were synthesized into a final table. This table encapsulates the outcomes of the survey responses, ultimately portraying the correlation between the posed questions and the established hypotheses.

Calculation method: We calculated the mean, variance, and standard deviation. The calculation of the mean and random error was based on Student's *t*-test hypothesis test statistic. This method, developed by statistician William Sealy Gosset, was most commonly applied when the test statistic would follow a normal distribution of the value [16]. Student's *t*-test is expressed as follows:

$$t = \frac{\overline{x} - \overline{y}}{\sqrt{\sigma\ (n_x - 1)\sigma_x^2 + (n_y - 1)\sigma_y^2}} \cdot \sqrt{\frac{(n_x + n_y - 2)}{n_1 + n_2}} \tag{1}$$

The calculated test statistic for our sample is: $t = 4.095$;
Number of degrees of freedom: $d_f = 12$;
The critical values of the parameters:
$p \leq 0.05\ t_{kp} = 2.18$
$p \leq 0.01\ t_{kp} = 3.06$
$t > t_{kp}$;
Depression:
$Dx = \sigma_x^2 = 0.211$
$Dy = \sigma_y^2 = 0.079$;
The root-mean-square deviation
$\sigma_x = 0.459$
$\sigma_x = 0.281$;
Number of questions:
$n_\mathrm{x} = n_\mathrm{y} = 7$.

As for data collection, the use of anonymous questionnaires is limiting, and future studies should incorporate pre-testing and validation to ensure reliability. The inclusion of qualitative methods, such as interviews or focus groups, would provide richer data, allowing for a more nuanced understanding of the participants' experiences and views, especially in a complex field like cybersecurity. The statistical analysis, particularly Student's *t*-test, was applied to compare the mean ratings of these two groups, and the significant divergence observed confirms the initial hypothesis that internal and external specialists view recovery strategies differently (Table 3). Internal specialists, such as IR and RM professionals, are more inclined to support frameworks like Lean Six Sigma and PRINCE2 because these methodologies align with their focus on rapid recovery, reputation defense, and operational continuity. Their proximity to the company means that they are directly impacted by the reputational and financial outcomes of cyberattacks.

Table 3. Statistical analysis: mean ratings.

Question	Internal IR/RM Specialists, CISOs	External Information Security Auditors
1	3.5	2.75
2	3.5	2.9
3	3.63	2.85
4	2.69	2.8
5	3.97	3.35
6	4.3	3.55
7	3.55	2.95
Mean ratings	$\overline{x} = 3.59$	$\overline{y} = 3.2$

5. Results

This study presents an analysis of the data collected between December 2022 and February 2023, focusing on the approaches employed by specialists, including IR, RM, and CISO specialists, as well as external auditors representing the company, who provide information security audits for critical infrastructure companies that operate in the PayTech and e-commerce domains. Additionally, this research explores the option of the utilization of project management methodologies by different groups of professionals and attitudes to intervention by the European Union (EU) after cyberattacks on entities that are based outside the EU. The findings shed light on the strategies and practices employed by these specialists and highlight the significance of effective project management in ensuring the resilience of EU critical infrastructure (Table 4).

This study highlights the considerable challenges involved in preparing and responding to cyberattacks, emphasizing the importance of implementing robust security measures within critical infrastructure companies. The insights were obtained from IR, RM, and CISO specialists, along with external information security auditors, who often see the background of an internal CISO position and IR and RM specialists differently. Furthermore, the analysis reveals notable differences in the perception of project management methodologies (such as Agile, Lean Six Sigma, PRINCE2, PM^2) and the role they play, as well as the significance of RM within the context of stock price recovery strategies [24].

In line with the proposed hypotheses, the findings highlight contrasting perspectives on the roles of specialists involved in recovery after cyberattacks. While a substantial portion of IR and RM specialists and CISOs expressed agreement (40%) or strong agreement (57%), information security auditors, who serve as external auditors, showed a tendency to "strongly disagree" (20%) or "disagree" (10%) that an internal CISOs position, along with IR and RM specialists within critical infrastructure organizations, is sufficient to effectively mitigate reputation damage following a cyberattack. To address divergence in the mean ratings, we applied a statistical examination through the application of the Student's *t*-test. In the context of the current study, the investigation into the contrasting perspectives held by internal and external specialists, namely, internal (IR/RM specialists, CISOs) and external (information security auditors), has revealed a substantial disconnect between their mean ratings. This pivotal disparity strikes at the heart of the null hypothesis initially posited for this research. As the mean ratings of these two specialized groups fail to align, the conditions required for the H0 hypothesis to hold true are not met.

Table 4. Comparison of insights from IR, RM, and CISO specialists and external information security auditors.

Question Number	Questions	Internal IR/RM Specialists, CISOs					External Information Security Auditors				
		1	2	3	4	5	1	2	3	4	5
1	In the event of a cyberattack, are there RM tools that can assist in restoring the company's reputation and simultaneously recovering its share value?	0%	10%	30%	60%	0%	0%	25%	40%	20%	5%
2	Do you believe companies providing critical infrastructure should establish their own internal CISO position, as well as dedicated IR and RM specialist positions?	3%	0%	43%	52%	2%	10%	20%	40%	30%	0%
3	Do you believe that having an internal CISO position, along with IR and RM specialists, within critical infrastructure organizations is sufficient to effectively mitigate reputation damage following a cyberattack?	0%	0%	40%	57%	3%	20%	10%	40%	25%	5%
4	Should CISOs be limited to individuals with only an IT background?	2%	57%	36%	5%	5%	10%	15%	60%	15%	0%
5	Is it advisable to base reputation defense after cyberattacks and stock price recovery strategies on methodologies such as Agile, Lean Six Sigma, PRINCE2, or PM^2?	2%	3%	30%	26%	39%	0%	15%	45%	30%	10%
6	Do you think that critical infrastructure businesses have industrial dependence on external IT vendors?	2%	10%	16%	72%	0%	0%	10%	25%	65%	0%
7	Do you agree that the European Union (EU) should play a vital role in safeguarding critical infrastructure entities located outside its jurisdiction?	0%	7%	33%	58%	2%	15%	10%	40%	35%	0%

Note: 1 = strongly disagree, 2 = disagree, 3 = agree, 4 = strongly agree, 5 = do not know. The tables show a percentage (%) of the total number of respondents in the whole sample.

Perceptions regarding the importance of reputation defense and stock price recovery strategies based on RM tools were supported differently by two groups of specialists in the research (H1). The findings yielded valuable insights into the perspectives of both internal and external specialists. A total of 60% of IR, RM, and CISOs "strongly agree" that the presence of RM tools can help restore the company's reputation and aid in the recovery of its share value. In comparison, only 20% of external auditors hold a different viewpoint, indicating a significant difference between the two groups. This divergence can be attributed to the natural interest of internal employees in maintaining the company's good reputation, as they are directly associated with the organization. Conversely, internal professionals recognize the importance of engaging external resources to effectively address reputation damage caused by cyberattacks. These contrasting perspectives shed light on the complex dynamics involved in mitigating reputation damage and underscore the need for comprehensive strategies that incorporate both internal and external expertise in the aftermath of cyberattacks.

The results reveal that a significant percentage (58%) of IR, RM, and CISO specialists, along with 35% of external information security auditors, "agree" or "strongly agree" with the notion that the EU should play an active role in securing EU critical infrastructure entities located abroad. These results thereby support H2.

In addition, we can highlight that a majority of IR and RM specialists and internal CISOs (26% and 39%, respectively) "agree" and "strongly agree" that standard industry best practices, such as Agile, Lean Six Sigma, PRINCE2, and PM^2, can serve as a foundation for reputation defense and stock price recovery strategies following cyberattacks. Interestingly, the information security auditors showed even higher levels of agreement, with 45% and 30% stating that they "agree" and "strongly agree", respectively, which can be attributed to their IT-oriented and process-driven backgrounds, often supported by IT-related certifications necessary for their roles in the information security audit domain.

The obtained results emphasize that ensuring the sustainability of smart cities requires the integration of critical infrastructure cybersecurity into strategic management. This is particularly relevant for systems such as PayTech, which provide financial support and serve as a connecting link between key components of a smart city, including energy, transportation, and healthcare. The reliable operation of PayTech systems contributes to strengthening economic sustainability by reducing financial risks, improving social sustainability by enhancing citizens' trust in digital services, and maintaining environmental sustainability by promoting transparency and minimizing resource usage.

These aspects of sustainability should become key benchmarks for the development and implementation of recovery strategies after incidents. They confirm that the effective management of cyber threats not only protects infrastructure but also fosters the long-term development of smart cities, ensuring their economic and social stability.

6. Conclusions and Discussion

The cybersecurity of infrastructure is an integral element of the sustainable development of smart regions. Smart city systems include various components, such as energy supply, transportation, healthcare, and financial systems—all of which must function in a secure and stable environment to ensure sustainability and growth. In this context, it is especially important to pay attention to the integration of PayTech systems as part of the entire critical infrastructure of smart cities.

PayTech systems are deeply integrated into the critical infrastructure and provide financial support, playing a connecting role between various components of the smart city. The majority of transactions in modern society are conducted automatically through online payment systems and PayServices, demonstrating the growing reliance on digital financial platforms for day-to-day operations. This enables FinTech companies to play a foundational role in building smart region ecosystems where interconnected services provide efficient, secure, and sustainable solutions for citizens and businesses alike.

These facts make the cybersecurity of financial transactions not just one of the tasks but a key element in ensuring the sustainable development of all other components. The reliable operation of PayTech systems contributes to both economic and social sustainability, maintaining citizens' trust in urban services.

This article addresses the question of whether internal and external professionals who represent PayTech and online e-commerce sectors have differing viewpoints on recovery strategies following cyberattacks. Notably, the findings underscore the contrasting perspectives between internal specialists, including IR, RM, and CISO professionals, and external information security auditors, highlighting the divergent views on the effectiveness and importance of reputation defense and stock price recovery strategies based on RM tools.

Additionally, this research supports the notion that the EU should play an active role in securing EU critical infrastructure in smart cities and smart ecosystems.

It also highlights the shared belief among specialists, both internal and external, regarding the value of industry best practices like Agile, Lean Six Sigma, PRINCE2, and PM^2 as foundations for reputation defense and stock price recovery strategies. This study explores the evolving landscape of cyber threats and the involvement of both internal professionals and external specialists in formulating effective response strategies. It specifically analyzes the divergent viewpoints between external auditors, who assess a company's compliance with information security standards and regulations, and internal CISO positions, along with other aspects of the company's recovery strategy following a cyber incident.

The findings underscore divergent perspectives between internal and external professionals; however, the practical implications of these differences are not fully explored. This paper emphasizes that companies may need to integrate external auditing processes more deeply into their incident response plans to ensure that both internal operations and external compliance measures are aligned. On the other hand, external auditors prioritize compliance, regulation, and objective adherence to standards like the NIST Cybersecurity Framework. They may not view internal methodologies like Lean Six Sigma as central to their audit or recovery roles, which explains their lower agreement rates. The differences in their responses underline the need for collaboration between these groups, as internal specialists focus on business continuity and reputation defense, while external auditors ensure that regulatory requirements and compliance are upheld. The results suggest that combining both perspectives is critical for developing comprehensive cyber recovery strategies.

On the other hand, external auditors prioritize compliance, regulation, and objective adherence to standards like the NIST Cybersecurity Framework. They may not view internal methodologies like Lean Six Sigma as central to their audit or recovery roles, which explains their lower agreement rates. The differences in their responses underline the need for collaboration between these groups, as internal specialists focus on business continuity and reputation defense, while external auditors ensure that regulatory requirements and compliance are upheld. The results suggest that combining both perspectives is critical for developing comprehensive cyber recovery strategies.

Considering the rising number of legislations and regulations at the EU level, particularly in the domains of information security, e-commerce, and the payment industry, the role of external auditors has become vital for overall information security strategies and the mitigation of cyberattacks. This study emphasizes the importance of collaboration between internal employees, such as IR and RM specialists, and external auditors to ensure swift recovery following a cyber incident. The results of this study reveal noteworthy discrepancies in viewpoints between internal professionals involved in RM defense and external auditors. Additionally, external auditors hold distinct expectations from internal CISOs, which may require essential alignment prior to conducting an information security assessment. This disparity provides valuable insights for organizations aiming to effectively respond to cyberattacks and manage reputational risks.

It should be noted that the limitation of the researcher sample is due to the need to obtain data exclusively from professionals with in-depth knowledge and experience in RM, cybersecurity, and critical infrastructure. Including more respondents without this level of training could have skewed the results of this study by adding subjective or less accurate responses. Thus, the main contribution of this study can be summarized through the following points.

The findings highlight several key gaps in current security standards, such as ISO 27000. Firstly, the standards do not take into account the different priorities between internal and external specialists, which can lead to inconsistencies in dealing with cyber incidents. Second, insufficient attention is paid to RM as a key aspect of recovering from attacks. Finally, cross-border coordination, especially in the context of protecting EU critical infrastructure outside its jurisdiction, remains an unresolved challenge. These findings emphasize the need to complement existing standards with new recommendations that take into account real challenges and perspectives.

1. Enhancing Sustainable Cyber Resilience through Recovery Approaches: Differences in the recovery approaches between internal and external specialists allow for a deeper understanding of protection and recovery mechanisms. Internal specialists focus on safeguarding reputation and sustainable operational continuity, while external auditors emphasize compliance with regulatory requirements and independent evaluation. This understanding helps develop comprehensive recovery strategies that include both internal and external aspects, thereby contributing to the sustainable development of smart cities.
2. Supporting Sustainable Economic Resilience: This study also shows that financial transactions facilitated by PayTech systems play a key role in maintaining the sustainable economic resilience of smart regions. The security and reliability of financial operations ensure the continuity of critical services, such as payment for utilities and transportation expenses, which, in turn, reduces economic risks and enhances the sustainable resilience of urban infrastructure.
3. Strengthening Sustainable Social Resilience: The reliable functioning of PayTech systems helps maintain citizens' trust in digital urban services. In this study, RM specialists emphasized the importance of proper incident response to maintain sustainable social trust in PayTech systems, which helps prevent users from switching to less convenient payment methods, such as cash transactions.

A future iteration of this study could delve into specific recovery strategies by analyzing individual cyberattack incidents on FinTech companies, examining internal management responses and the role of external auditors. This approach would enhance comprehensiveness and provide deeper insights.

The opinions regarding the role and interaction of the European Union (EU) with critical infrastructure entities after a cyberattack can differ between two groups and require separate analysis. These opinions can be compared in the context of cyberattacks to assess alignment. The other limitation is that the current research only concentrated on examining viewpoints regarding reputation defense within the specific financial domain, specifically in areas such as PayTech and e-commerce. This focus was driven by the recognition of the heightened compliance requirements imposed by regulatory bodies like the European Central Bank and international information security operational standards. These stringent standards serve as essential guidelines for businesses in securing and safeguarding consumers' assets and personal data. Also, future research should delve deeper into the specific challenges faced by organizations and explore additional factors that influence reputation defense and stock price recovery in the aftermath of cyberattacks. In addition, future research will focus on expanding the sample by involving more companies and respondents. At the same time, the key selection criterion will remain a high level of competence of the participants in order to maintain the quality and accuracy of the data collected.

This research is a pilot study aimed at identifying key differences in approaches to recovering from cyberattacks among internal and external professionals. Despite the limited number of respondents, the results emphasize the importance of coordination and the need to integrate recovery and RM strategies.

To further develop the research topic, it is planned to expand the sample to include more companies from different industries and regions. This will allow the views of professionals working in different environments and with different cybersecurity expertise to be taken into account.

Thus, this research provides a basis for further research on cyberattack recovery strategies and RM in the face of cyber threats. Future studies will expand the sample of respondents to include companies from different industries and regions, as well as analyze real-life cyberattack cases to provide a more in-depth and informed perspective.

For better clarity, the main findings of this study are summarized in the table below (Table 5). It consolidates the core aspects, including distinctive features, achieved objectives, and recommendations for future research.

Table 5. Key findings of this study.

Key Aspects	Description
Scientific Novelty	A comparative analysis of recovery approaches after cyberattacks between internal and external specialists (IR, RM, CISOs, and external auditors) is conducted for the first time. Differences in priorities and approaches are identified, which were previously insufficiently covered in the literature.
Significance of this Study	This study emphasizes the importance of integrating internal and external approaches to enhance the resilience of critical infrastructure in smart cities. Practical recommendations are proposed for reputation protection, compliance, and recovery after attacks.
Achieved Results	The significance of reputation management (RM) in restoring stock value after cyberattacks is confirmed. Methodologies (Lean Six Sigma, PRINCE2, PM^2) are recognized as key for effective recovery project management. The EU's critical role in protecting critical infrastructure is highlighted.
Distinctive Features	This analysis focuses on PayTech and FinTech companies, enabling the extrapolation of findings to an essential sector of critical infrastructure. A combined methodology of surveys and statistical analysis ensures the reliability of the results.
Achievement of Research Goals	The research goals are achieved. The impact of cyber threats on the sustainable development of smart cities is assessed, and recommendations for reputation management and infrastructure recovery are developed.
Recommendations for Future Research	Expanding the sample size by including representatives from other critical infrastructure sectors. Analyzing specific cyberattack cases to develop targeted recovery strategies.

Author Contributions: Supervision and conceptualization: I.L.; methodology: I.Z.; experiments, result visualization and analysis: I.L., I.Z. and S.S.; verification of theoretical and experimental conclusions: I.L.; writing—original draft: S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board of Université de Lorraine, Nancy, France—protocol approval accordingly, the national order of 25 May 2016.

Informed Consent Statement: Informed consent was obtained from all subjects involved in this study.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors appreciate the scientific society of the consortium and, in particular, the staff of the Université de Lorraine, Nancy, the Information Systems Department of Simon Kuznets Kharkiv National University of Economics Kharkiv, Ukraine, and the Cyber Security Department, University of the National Education Commission, ul. Podchorążych 2, Kraków, Poland (S.S.) for invaluable inspiration and creative analysis during the preparation of this paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Cartwright, A.; Cartwright, E.; Solomon Edun, E. Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Comput. Secur.* **2023**, *131*, 103288. [CrossRef]
2. Claroty Ltd. *Report: The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption*; Claroty Ltd.: New York, NY, USA, 2022.
3. Velinov, E.; Leroy, I.; Cetlova, E. Marketing Process in Information Security Context: Comparison Between Czech Republic and Belgium. In *Proceedings of the International Conference Engineering Innovations and Sustainable Development*; Springer: Berlin/Heidelberg, Germany, 2021; Chapter 64; ISBN 9783030908423.
4. Paes, V.d.C.; Pessoa, C.H.M.; Pagliusi, R.P.; Barbosa, C.E.; Argôlo, M.; de Lima, Y.O.; Salazar, H.; Lyra, A.; de Souza, J.M. Analyzing the Challenges for Future Smart and Sustainable Cities. *Sustainability* **2023**, *15*, 7996. [CrossRef]
5. Moch, N.; Wereda, W. Smart Security in the Smart City. *Sustainability* **2020**, *12*, 9900. [CrossRef]
6. Ma, C. Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Rep.* **2021**, *7*, 7999–8012. [CrossRef]
7. Son, I.; Kim, S. Mobile Payment Service and the Firm Value: Focusing on both Up- and Down-Stream Alliance. *Sustainability* **2018**, *10*, 2583. [CrossRef]
8. Beirne, J.; Fernandez, D.G. Digital Finance and Sustainability: Impacts, Challenges, and Policy Priorities. *Sustainability* **2023**, *15*, 14830. [CrossRef]
9. Hwang, Y.; Park, S.; Shin, N. Sustainable Development of a Mobile Payment Security Environment Using Fintech Solutions. *Sustainability* **2021**, *13*, 8375. [CrossRef]
10. Habib, M.Y.; Qureshi, H.A.; Khan, S.A.; Mansoor, Z.; Chishti, A.R. Cybersecurity and Smart Cities: Current Status and Future. In Proceedings of the 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T), Bahawalpur, Pakistan, 9–11 January 2023; pp. 1–7. [CrossRef]
11. Al Duhaidahawi, H.M.; Zhang, J.; Abdulreda, M.S.; Sebai, M.; Harjan, S. The Financial Technology (Fintech) and cybersecurity. *Int. J. Res. Bus. Soc. Sci. (2147-4478)* **2020**, *9*, 123–133. [CrossRef]
12. Oliveira, T.A.; Oliver, M.; Ramalhinho, H. Challenges for Connecting Citizens and Smart Cities: ICT, E-Governance and Blockchain. *Sustainability* **2020**, *12*, 2926. [CrossRef]
13. Kamiya, S.; Kang, J.K.; Kim, J.; Milidonis, A.; Stulz, R.M. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *J. Financ. Econ.* **2021**, *139*, 719–749. [CrossRef]
14. Kamiya, S.; Kang, J.K.; Kim, J.; Milidonis, A.; Stulz, R.M. What is the Impact of Successful Cyberattacks on Target Firms? NBER Working Paper No. w24409. 2018. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143314 (accessed on 13 January 2025).
15. Ernst & Young. What Companies Are Disclosing About Cybersecurity Risk and Oversight. 2019. Available online: https://www.ey.com/en_us/board-matters/cyber-disclosure-trends (accessed on 1 September 2024).
16. Hiles, A. *Reputation Management: Building and Protecting Your Company's Profile in a Digital World*; Bloomsbury Publishing Plc.: New York, NY, USA, 2011; ISBN 9781849300421.
17. European Commission. PM^2 Project Management Methodology Guide. 2016. Available online: https://op.europa.eu/en/publication-detail/-/publication/0e3b4e84-b6cc-11e6-9e3c-01aa75ed71a1 (accessed on 1 September 2024).
18. European Central Bank. *Towards a Framework for Assessing Systemic Cyber Risk*; Financial Stability Review; European Central Bank: Bruxelles, Belgium, 2022.
19. European Commission. Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union. 2016. Available online: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed on 15 January 2025).
20. Leroy, I. The relationship between cyber-attacks and dynamics of company stock. The role of Reputation Management. *Int. J. Electron. Secur. Digit. Forensics* **2022**, *3*, 24–25. [CrossRef]
21. Ziliak, S.T. W.S. Gosset and Some Neglected Concepts in Experimental Statistics: Guinnessometrics II. *J. Wine Econ.* **2011**, *6*, 252–277. [CrossRef]

22. Bao Ngo, T.N.; Tick, A. Cyber-Security Risks Assessment by External Auditors. *Interdiscip. Descr. Complex Syst.* **2021**, *19*, 375–390. [CrossRef]
23. Pearson, B.; Lacombe, D.; Khatun, N. Likert Scale Variables in Personal Finance Research: The Neutral Category Problem. *Econometrics* **2024**, *12*, 33. [CrossRef]
24. Yu, Z.; Gao, H.; Cong, X.; Wu, N.; Song, H.H. A Survey on Cyber–Physical Systems Security. *IEEE Internet Things J.* **2023**, *10*, 21670–21686. [CrossRef]

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