Article

Not peer-reviewed version

Approaches of Critical Infrastructure Companies to Recover from Cyber-Attack: Insights from Internal Specialists and External In-Formation Security Auditors

Iryna Leroy *, Iryna Zolotaryova *, Serhii Semenov *

Posted Date: 26 September 2024

doi: 10.20944/preprints202409.2129.v1

Keywords: information security; information security assessment; digital; reputation management; cyber autonomy; cyber resilience

Article

Approaches of Critical Infrastructure Companies to Recover from Cyber-Attack: Insights from Internal Specialists and External Information Security Auditors

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

[1] Université de Lorraine, Nancy, France European Security and Defence College Brussels, Belgium (I.L.)
[2] Information Systems Department of Simon Kuznets Kharkiv National University of Economics Kharkiv, Ukraine (I.Z.)
[3] Cyber Security Department, University of the National Education Commission, ul. Podchorążych 2, Kraków, Poland (S.S.)
* Correspondence: irynaleroy@hotmail.com

Abstract: Companies operating in the PayTech and online e-commerce sectors play a crucial role in critical infrastructure, functioning within the dynamic digital landscape. This study focuses on the recovery process after cyber-attacks and examines the contrasting perspectives of internal and external professionals. The research reveals notable differences in the perceptions of recovery strategies between internal stakeholders such as investor relations, reputation management, and Chief Information Security Officers, representing companies belonging to critical infrastructure and external auditors, who provide just and emergency support and perform specific tasks. Importantly, the study underscores the current attitudes towards 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: information security; information security assessment; digital; reputation management; cyber autonomy; cyber resilience

1. Introduction

1.1. Motivation

Currently, the functioning of modern society is increasingly dependent on critical infrastructure (CI). 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 recent times, there has been a surge in cyber intrusions and cyberattacks on CI. The growing trend of cyberattacks is driven by several 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 has become a valuable asset, making it 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.

 doi:10.20944/preprints202409.2129.v

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, reputation management managers, chief information security officers) 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 reputation management. 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 behaviour within organizations. The focus is on overcoming the information security barrier between 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 research "The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption" report shows that 80% of critical infrastructure organizations experienced a ransomware cyber-attack. 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 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% who are centralizing IT governance are under the Chief Information Security Officers (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 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 assessment of the company's reputation among individuals in Czech Republic and Belgium: 58% of Czech individuals "agree" with that competing to 48% from Belgium. However, Belgian respondents are more unequivocally convinced of this need which is 32% of the total mass of respondents and is three times higher than the data for the same response of respondents in the Czech Republic. Given the intensity of public concern about information security, reputational issues could not be short term, hoc and defensive but should have strategic view and long-term planning to defend reputation [3].

Although the implication of cybersecurity stretches across all business regions, the most attention of the cybersecurity in the business world focuses 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 [4]. In connection with that, research shows that external auditors pay more attention to cybersecurity incidents and also can 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 [5]. Nevertheless, for example, according to an Ernst & *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 [6].

 doi:10.20944/preprints202409.2129.v

Consistent with prior studies, in this research within our analyses, we have identified a few current problems: the disparity in approaches to recovering from cyber-attacks between internal company stakeholders and external information security auditors, particularly in the strategy for recovering the company's reputation that is damaged by cyber incidents. Emphasizing the need for a better understanding between different approaches and prevention of information security and reputation that is damaged by cyber incidents, this study proposes two research questions (RQs): RQ1: Do internal stakeholders (investor relations, reputation management, and Chief Information Security Officers) and external auditors differ in their viewpoints on recovery strategies following cyber-attacks? RQ2: Do internal stakeholders (investor relations, reputation management, and Chief Information Security Officers) and external auditors differ in their viewpoints on reputation defense and role that the European Union (EU) has outside its jurisdiction from cyber-attacks?

To address the above research questions, the current study contributes to existing research in several ways. First, considering the previous researches that focuses on cyber-attacks impact a company's reputation, which in turn impacts the company's share price as serious business interruptions after a breach have one of the largest effects on the value of companies because of its impact on cash flow [7]. 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 [8].

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 [9].

In the EU is the NIS2 directive (proposed by National Institute of Standards and Technology) – that aims to establishes 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 the risks to the security of network and information systems, and to take appropriate measures to manage those risks [10]. This is particularly important for financial markets and company reputation recovery after cyber-attacks [11]. Furthermore, firms with stronger reputations are more likely to weather market volatility better than those with weaker reputations.

Third, the 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 PM² project management methodology, developed and supported by the European Commission, emphasizes the importance of risk management in recovering from cyberattacks. According to the European Commission the PM² 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 PM² 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 used to mitigate risks in three ways such preventing incidents from happening, detecting incidents as early as possible, and minimizing the impact of incidents that do occur [8]. By focusing on these three elements, organizations can minimize the damage caused by cyber-attacks and improve their resilience to future threats.

Finally, our study aims to address the above research questions by examining different viewpoints on different viewpoints on reputation defense and the utilization of reputation management tools, which have the potential to restore the value of a company's shares following a cyber incident. Such a reputation management tools includes: transparency in admitting cyber-attack

 doi:10.20944/preprints202409.2129.v

incidents within 24 hours, constant communication with key stakeholders through regular channels, maintaining own news channels with higher frequency for communication, conducting trainings 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 include people with knowledge from different fields, including investor relations, reputation relations and information security and each of these areas must have a specialist or single point of contact for these tasks. For example, Investor relations (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 cyber-attack, implementing strategies to manage the incident and restore trust with stakeholders. Chief information security officers (CISOs) lead the prevention of cyber-attacks by implementing comprehensive security measures, assessing risks, and developing proactive strategies to safeguard critical information and systems from potential threats [11].

Table 1 above illustrates the relationship between cyber-attacks, the dynamics of company stock, and reputation management. The analysis also demonstrates the impact of the participation of professionals such as investor relations (IR), reputation management (RM) specialists, together with Chief Information Security Officers (CISOs), on the recovery process.

Table 1. The relationship between cyber-attacks, dynamic of company's stocks and reputation management. Analyses of cyberattack / biggest data breaches in US and EU that affected companies which have 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 CISO position*	*Companie 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.

1.3. Objectives and Contributions

The main objective of the 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.

2. Data Collection

This section outlines the data collection process and methodology employed, which focused on the distinct classification of specific roles such as investor relations (IR), reputation management (RM), chief information officers (CISO) or external information security auditors. The data was collected through the distribution of anonymous questionnaires among professionals belonging to

 doi:10.20944/preprints202409.2129.v

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.

3. Methodology

We processed the data in two stages. On the first level, we used mainly 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 concept analysis of 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, CISO and external information security auditors. Prior to participation, respondents were provided with information about the survey and invited to collaborate further.

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 only across three companies that operates in similar domains. First company Mall Group a.s. based in Czech Republic, second company Worldline S.A. based in Belgium (including their EU offices), and Advantio Ltd. - qualified security assessor that mainly based in Ireland. Advantio is company which 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 the respondent samples was 120 and within this number 47 are 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 cyber-attack, 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, the following hypotheses were built as follows:

Hypothesis 0: There are discernible differences in the perceptions of specialists’ roles in the recovery of cyber-attacks among investor relations (IR), reputation management (RM) and CISO (Chief Information Security Officer) specialists, and external information security auditors.

Hypothesis 1: The presence of reputation management tools can help restore the reputation of the company and, simultaneously, restore the value of its shares.

Hypothesis 2: Active intervention by the European Union (EU) is imperative to safeguard critical infrastructure entities based outside the EU from cyber-attack.

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 conducted aimed to scrutinize the disparities in evaluations provided by distinct groups of experts. In line with this, the question for the hypotheses were distributed as follows:

H0: The questions pertinent to this hypothesis encompass Question number 1, Question 2, Question 3, and Question 5.

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

 doi:10.20944/preprints202409.2129.v

H2: 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 ecommerce services for the international market.	Marchant and acquirer solution	PCI security assessments

Source: crunchbase.com; bloomberg.com.

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: Calculations of mean, variance and standard deviation. Calculation of the mean and random error based on Student's 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 [12]. Student's t-test:

$$t = \frac{\bar{x} - \bar{y}}{\sqrt{\sigma\,(nx-1)\sigma x^2 + (ny-1)\sigma y^2}} \cdot \sqrt{\frac{(nx + ny - 2)}{n1 + n2}}$$

The calculated test statistic for our sample is: t = 4.095

Number of degrees of freedom: df = 12

The critical values of the parameters:

$p \le 0.05$ tkp = 2.18

$p \le 0.01$ tkp = 3.06

t > tkp

Depression:

$Dx = \sigma^2 x = 0{,}211$

$Dy = \sigma^2 y = 0{,}079$

The root-mean-square deviation

$\sigma x = 0.459$

$\sigma y = 0.281$

Number of questions:

$nx = ny = 7$

Table 3. Statistical analysis. Mean ratings.

Question	*Internal IR/RM specialists, CISO*	*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	$\bar{x} = 3.59$	$\bar{y} = 3.2$

4. Results

 doi:10.20944/preprints202409.2129.v

The study presents an analysis of the collected data collected between December 2022 and February 2023, focusing on the approaches employed by specialists, including investor relations (IR) specialists, reputation management (RM) and CISO specialists as well as external auditors representing the company that provide information security audit for critical infrastructure companies that operates in the PayTech and e-commers domains. Additionally, the research explores the option of the utilization of the project management methodologies by different groups of professionals and attitudes to intervention by the European Union (EU) after cyber-attack 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. Comparison of insights from IR, RM and CISO specialists, and external information security auditors.

Question number	*Questions*	*Internal* *IR/RM specialists, CISO*					*External* *Information security auditors*				
		1	2	3	4	5	1	2	3	4	5
1	In the event of a cyberattack, are there reputation management 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 cyber-attack?	0%	0%	40%	57%	3%	20%	10%	40%	25%	5%
4	Should CISOs be limited to	2%	57%	36%	5%	5%	10%	15%	60%	15%	0%

 doi:10.20944/preprints202409.2129.v

	individuals with only an IT background?										
5	Is it advisable to base reputation defense after cyber-attacks and stock price recovery strategies on methodologies such as Agile, Lean Six Sigma, PRINCE2, or PM²?	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 = don't know. The tables show a percent (%) of the total number of respondents in the whole sample.

The study highlights the considerable challenges involved in preparing and responding to cyber-attacks, emphasizing the importance of implementing robust security measures within critical infrastructure companies. The insights 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, PM².) and the role they play, as well as the significance of reputation management within the context of stock price recovery strategies.

In line with the proposed hypotheses the findings highlight contrasting perspectives on the roles of specialists involved in the recovery of cyber-attacks. While a substantial portion of IR, 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 CISO position, along with IR and RM specialists within critical infrastructure organizations, is sufficient to effectively mitigate reputation damage following a cyber-attack". For divergence in the mean ratings, we applied 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, CISO) and external (Information security auditors), has revealed a substantial disconnect between

 doi:10.20944/preprints202409.2129.v

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.

Perceptions regarding the importance of reputation defense and stock price recovery strategies, based on reputation management 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. The 60% of IR, RM and CISO "strongly agree" that the presence of reputation management 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 cyber-attacks. 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 cyber-attacks.

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 PM², can serve as a foundation for reputation defense and stock price recovery strategies following cyber-attacks. Interestingly, the information security auditors showed even higher levels of agreement, with 45% and 30% "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.

5. Conclusion

This article addresses the question of whether internal and external professional who represent PayTech and online e-commerce sectors has differed in their viewpoints on recovery strategies following cyber-attacks. 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 reputation management tools. Additionally, the research supports the notion that the EU should play an active role in securing EU critical infrastructure entities abroad. It also highlights the shared belief among specialists, both internal and external, in the value of industry best practices like Agile, Lean Six Sigma, PRINCE2, and PM² 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.

6. Contribution to the Field

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 cyber-attacks. The study emphasizes the importance of collaboration between internal employees, such as investor relations and reputation management specialists, and external auditors to ensure swift recovery

 doi:10.20944/preprints202409.2129.v

following a cyber incident. The results of the study revealed noteworthy discrepancies in viewpoints between internal professionals involved in reputation management 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 cyber-attacks and manage reputational risks.

7. Research Limitations

The opinions regarding the role and interaction of the European Union (EU) with critical infrastructure entities after a cyber-attack can differ between two groups and require separate analysis. These opinions can be compared in the context of cyber-attacks 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 cyber-attacks.

Author Contributions: Supervision and conceptualization: I.L.; methodology: I.Z.; experiments, result visualization and analysis: I.L., I.Z. 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: Not applicable.

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

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

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

References

1. Cartwright, A., Cartwright, E., & Solomon Edun, E. (2023) Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Computers & Security, Vol. 131, DOI:10.1016/j.cose.2023.103288
2. Claroty Ltd. (2022). Report: The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption. New York.
3. Velinov, E., Leroy, I., Cetlova, E. (2021) 'Marketing Process in Information Security Context: Comparison Between Czech Republic and Belgium'. In Proceedings of the International Conference Engineering Innovations and Sustainable Development. Chapter 64. Springer. Germany. ISBN 9783030908423.
4. Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, René M. Stulz, Risk management, firm reputation, and the impact of successful cyberattacks on target firms, Journal of Financial Economics, Volume 139, Issue 3, 2021, Pages 719-749, ISSN 0304-405X, https://doi.org/10.1016/j.jfineco.2019.05.019.
5. Shinichi K., Kang J., Jungmin Kim, Milidonis A., (2018) 'What is the Impact of Successful Cyberattacks on Target Firms?' SSRN Electronic Journal. 10.2139/ssrn.3135514. DOI: http://dx.doi.org/0.3386/w24409
6. Ernst & Young, 2019. What companies are disclosing about cybersecurity risk and oversight. 2019 [online]: https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/cbm/ey-cbm-cybersecurity-risk-oversight-final-eycom.pdf).
7. Hiles, A. (2011). Reputation Management: Building and Protecting Your Company's Profile in a Digital World. NY: Bloomsbury Publishing Plc. ISBN: 9781849300421
8. European Commission. (2016) PM² Project Management Methodology Guide. [online] https://op.europa.eu/en/publication-detail/-/publication/0e3b4e84-b6cc-11e6-9e3c-01aa75ed71a1

 doi:10.20944/preprints202409.2129.v

9. European Central Bank, (2022) Towards a framework for assessing systemic cyber risk. Financial Stability Review, Belgium.
10. European Commission (2016) Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union, Belgium.
11. Leroy, I. (2022) 'The relationship between cyber-attacks and dynamics of company stock. The role of Reputation Management'. Int. J. Electronic Security and Digital Forensics, Vol. 3(1), 24–25. ISSN: 17519128
12. Stephen Ziliak T. (2011) 'W.S. Gosset and Some Neglected Concepts in Experimental Statistics: Guinnessometrics II'. Journal of Wine Economics, 2011. Vol. 6 (2), pp.52–277. ISSN 1931-4361
13. Tran Nguen Bao Ngo & Andrea Tick (2021) 'Cyber-Security Risks Assessment by External Auditors', Interdisciplinary Description of Complex Systems, Vol. 19, no. 3, pp. 375 – 390.