Mechanics Transport Communications

Academic journal http://www.mtc-aj.com

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
volume 22, issue 3/1, 2024
article № 2566

OPTIMISING CYBERSECURITY INVESTMENTS IN THE RAIL SECTOR TO REDUCE FINANCIAL RISKS

Angel Ivanov, Kalina Semova
achmore@gmail.com, ksemova@vtu.bg

Todor Kableshkov University of Transport
158 Geo Milev Str, Sofia 1574
BULGARIA

Key words: *cybersecurity in the rail sector, risks from cyber threats, cybersecurity investments, return on investment (ROI) of cybersecurity investments, digital transformation of the rail sector, EU Cybersecurity Strategy*

Abstract: *The article discusses the importance of cybersecurity in the rail sector. The integration of digital technologies exposes the sector to a multitude of cyber threats, necessitating proactive and robust security measures. The rail sector faces significant financial risks from cyber threats, including direct costs from service disruptions and recovery efforts, as well as indirect costs like reputational damage and loss of public trust, that can have lasting effects, reducing passenger confidence, and potentially leading to a decline in ridership, which in turn affects revenue and the financial stability of rail operators. Guided by European Unity Agency for Cybersecurity (ENISA) report and the Directive on measures for a high common level of cybersecurity across the European Union (NIS2 Directive) strategic investments in cybersecurity are the key to addressing these vulnerabilities. Cybersecurity should be viewed as a critical tool for ensuring the security of efficient rail operations. Proactive investments in cybersecurity can help prevent major financial losses from cyber incidents and enhance the sector's defenses against evolving threats. Cost-benefit analysis of cybersecurity investments in the rail sector is presented in the article and a formula for calculating the return on investment of cybersecurity investments is proposed.*

INTRODUCTION

Europe's rail sector is in the midst of a digital transformation, offering the promise of improved efficiency and connectivity. However, this evolution presents new challenges, especially in the realm of cybersecurity. With advanced technologies come heightened vulnerabilities, underscoring the urgent need for robust cybersecurity frameworks. Guided by the ENISA Report and the NIS2 Directive, strategic investments in cybersecurity are not just crucial; they are the key to addressing these vulnerabilities, ensuring compliance with EU regulations, and upholding operational resilience. (ENISA Report, p. 1; NIS2 Directive, p. 2).

IMPORTANCE OF CYBERSECURITY IN THE RAIL SECTOR

In the contemporary rail sector, cybersecurity is not just a technical requirement; it is a strategic asset. The integration of digital technologies exposes the sector to a multitude of

cyber threats, necessitating proactive and robust security measures. The ENISA Report underscores that cybersecurity should be viewed as a critical tool for ensuring the security of efficient rail operations. This is not just about data protection but about safeguarding the very infrastructure that enables rail networks to function smoothly (ENISA Report, p. 3 (1).

Cyber threats have the potential to disrupt operations, result in significant financial losses, and diminish public trust. In today's digital age, where rail networks are intricately interconnected with various digital systems, the risk of cyber-attacks rises. This underscores the critical importance of cybersecurity in rail operations to ensure safety and efficiency. The NIS2 Directive emphasises this by requiring robust cybersecurity measures for critical infrastructure, including rail networks (NIS2 Directive, p. 2 (5).

NEED FOR A STRATEGIC CYBERSECURITY FRAMEWORK

The need for a strategic cybersecurity framework tailored to the EU rail sector concerns the present and the future. This framework should be comprehensive, covering all aspects of cybersecurity, from risk identification and management to prevention, response, and continuous improvement. Most importantly, it should be dynamic and evolving, a testament to our sector's readiness to adapt to the ever-changing threat landscape.

The development of this framework is a proactive, multi-faceted approach. Robust risk identification and management processes enable us to assess and prioritise threats specific to the rail sector, ensuring we stay one step ahead. Our prevention and protection strategies, including the deployment of technological solutions and defensive measures, are designed to safeguard both digital and physical assets. Incident response and recovery strategies are in place to minimise operational impact when breaches occur. Finally, continuous improvement mechanisms ensure that our cybersecurity practices are regularly updated and refined to address new threats, providing a sense of security and confidence in our approach. This proactive approach puts us in control of our cybersecurity landscape (NIS2 Directive, p. 4 (5).

FINANCIAL RISKS FROM CYBER THREATS

The rail sector faces significant financial risks from cyber threats, including direct costs from service disruptions and recovery efforts, as well as indirect costs like reputational damage and loss of public trust. Real-world examples from the EU and Poland illustrate the severe economic impacts of cyber incidents. For example, a cyber attack in Poland in 2022 caused major operational disruptions, highlighting the critical need for strong cybersecurity investments (3). Service disruptions can result in significant financial losses due to halted operations and the costs of restoring services. Additionally, reputational damage can have lasting effects, reducing passenger confidence and potentially leading to a decline in ridership, which in turn affects revenue and the financial stability of rail operators. Therefore, the rail sector must understand and mitigate these financial risks for its sustainability.

STRATEGIC INVESTMENT IN CYBERSECURITY

Investing in cybersecurity is not just about protecting data; it's a financial necessity. The EU Cybersecurity Strategy highlights the importance of regular security updates and strategic investments to reduce financial risks and strengthen economic resilience. Proactive investments in cybersecurity can help prevent major financial losses from cyber incidents and enhance the sector's defences against evolving threats. These investments are vital for maintaining the operational and financial well-being of the rail sector (EU Cybersecurity Strategy for the Digital Decade, p. 6 (2).

A strategic investment in cybersecurity encompasses several key areas. Firstly, a commitment to continuous security updates is essential to ensure that systems are shielded from the latest threats. Secondly, investments in advanced security technologies, such as AI

and machine learning for threat detection, can yield significant benefits. Thirdly, improving incident response capabilities ensures that rail operators can promptly and effectively handle breaches, minimising damage and recovery time. Lastly, ongoing training and awareness programs for employees are crucial, as human error continues to pose a significant risk in cybersecurity (ENISA Report, p. 3 (1).

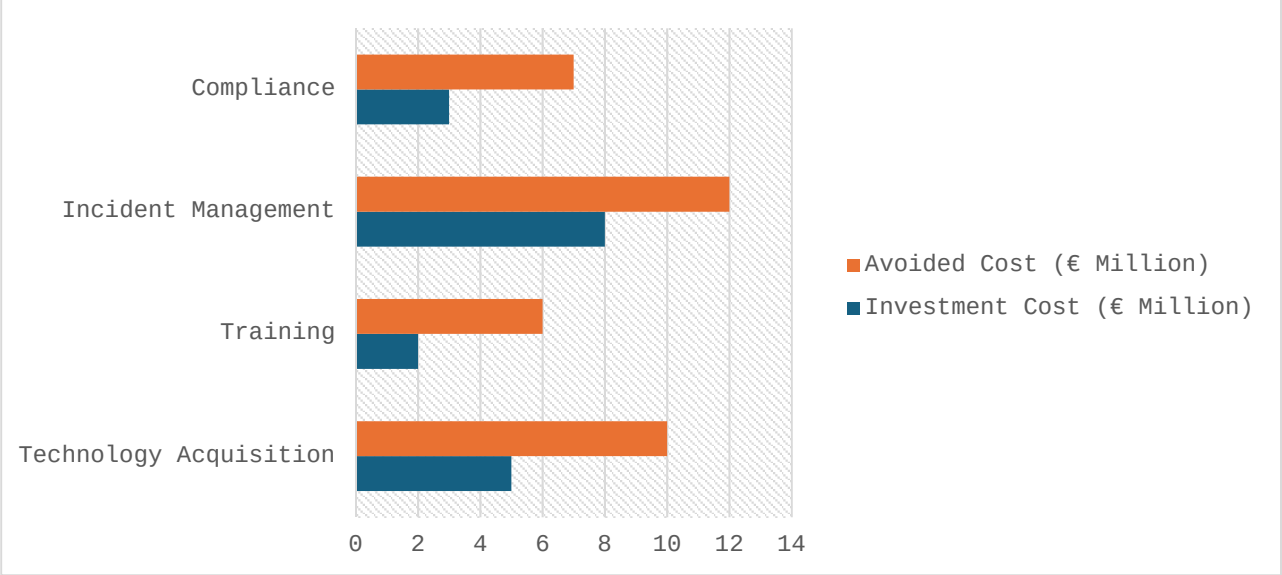

Figure 1 - Cost-Benefit Analysis of Cybersecurity Investments in the Rail Sector

Source: "ENISA Threat Landscape 2023" and "JC 2023 86 - Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework."

CYBERSECURITY CHALLENGES IN THE RAIL SECTOR

Modern rail systems are highly complex and interconnected, integrating various technologies that provide numerous entry points for cyber attackers. Additionally, the increasing use of IoT devices, which play a crucial role in enhancing operational efficiency, also presents potential entry points for cyber threats if not properly secured (3).

These devices, which range from smart sensors to automated control systems, enhance operational efficiency but also expand the attack surface. Ensuring the security of these devices is critical to maintaining the overall security of the rail network. This includes securing the data collected by IoT devices, as compromised data can lead to incorrect decisions and actions, further jeopardising rail operations (ISO/IEC 27005: Risk Management, p. 9 (4). The digital transformation of the rail sector introduces several cybersecurity challenges.

The complexity of modern rail systems is a double-edged sword. While it enhances capabilities and efficiencies, it also creates more opportunities for cyber threats. Attackers can exploit interconnected systems, such as signalling, communication, and control systems. It's crucial to stress that legacy systems, which were not designed with cybersecurity in mind, are particularly vulnerable. This vulnerability underscores the urgent need for significant upgrades to meet current security standards.

ECONOMIC IMPACT OF CYBER THREATS

Cybersecurity incidents can inflict severe economic consequences on the rail sector. The impact is not limited to operational downtime, hefty incident response costs, and fines for non-compliance with cybersecurity regulations. It extends to indirect effects such as

reputational damage, loss of competitive advantage, and decreased investment, all of which can significantly disrupt the sector's financial stability (3).

Furthermore, non-compliance with cybersecurity regulations can result in substantial fines, adding to the financial burden. Indirect impacts, such as reputational damage, can erode public trust and reduce ridership, further affecting revenue.

Proactive investment in cybersecurity measures is essential to mitigate these risks. This includes adopting advanced security technologies, enhancing incident response capabilities, and conducting continuous risk assessments.

MITIGATING ECONOMIC RISKS WITH PROACTIVE INVESTMENT

Proactive investment in cybersecurity measures can significantly mitigate financial risks. This involves adopting advanced security technologies, enhancing incident response capabilities, and conducting continuous risk assessments.

Advanced security technologies, such as AI and machine learning, can provide significant benefits by enhancing threat detection and response capabilities. These technologies can analyse vast amounts of data in real-time, identifying potential threats before they can cause significant damage. Continuous risk assessments are essential to identify vulnerabilities and ensure that security measures are up to date.

Public-private partnerships play a crucial role in enhancing cybersecurity. Collaboration with government agencies and private sector partners can provide access to additional resources and expertise, improving the rail sector's overall security posture. These partnerships can also facilitate information sharing, helping to identify and mitigate threats more effectively (ISO/IEC 27005: Risk Management, p. 9 (4).

CALCULATING THE ROI OF CYBERSECURITY INVESTMENTS

Investing in cybersecurity delivers tangible financial returns. Demonstrating a positive ROI is essential for rail operators to justify sustained and increased investment in cybersecurity.

Calculating the ROI involves several steps. First, could you identify the costs associated with cybersecurity investments, including initial investment costs for technology acquisition, training, and consultation? Ongoing operational costs for maintenance and updates should also be considered. Next, identify the benefits, such as avoided costs of incidents, operational continuity, enhanced reputation, and regulatory compliance. Finally, calculate the ROI using the formula:

$$ROI = \frac{\text{Cost of Investment}}{\text{Net Benefits of Investment}} \text{ x } 100$$

Demonstrating a positive ROI helps rail operators justify ongoing and increased investment in cybersecurity (ENISA Report, p. 10 (1).

CONCLUSION AND NEXT STEPS

The rail sector's digital transformation brings huge benefits but also comes with significant cybersecurity challenges. It is crucial to make strategic investments in cybersecurity, following the guidelines of the ENISA Report and the NIS2 Directive, to enhance resilience, ensure compliance, and maintain financial stability. Moving forward, it's important to develop a customised cybersecurity framework, improve risk assessment tools, utilise advanced technologies for threat detection, and establish continuous cybersecurity training programs. By taking these steps, the rail sector can effectively handle the complexities of the digital age and protect itself against cyber threats (NIS2 Directive, p. 11 (5).

REFERENCES:

[1] ENISA Report on Railway Cybersecurity. https://www.enisa.europa.eu/publications/railway-cybersecurity

[2] EU Cybersecurity Strategy for the Digital Decade.

[3] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade

[4] Paklerska A., Cyber Threats in Rail Traffic in Poland. DOI:doi.org/10.13166/jms/176679, JOURNAL OF MODERN SCIENCE (jomswsge.com), volume 4/53/2023

[5] ISO/IEC 27005:2022 Information Security, cybersecurity and Privacy Protection – Guidance on managing information security risks. https://www.iso.org/standard/80585.html

[6] Directive (EU) 2022/2555 (NIS2 Directive). https://www.nis-2-directive.com