SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2026
ORGANIZATION AND MANAGEMENT SERIES NO. 243

THE IMPACT OF CYBER THREAT EVOLUTION ON ENTERPRISE MANAGEMENT

Joanna ANTCZAK

Military University of Technology; joanna.antczak@wat.edu.pl, ORCID: 0000-0001-5691-2525

Purpose: The aim of the paper is to define the evolution of cyber threats in the years 2017-2025 and assess their impact on enterprise management, with a key emphasis on the need for transformation towards building cyber resilience.
Design/methodology/approach: The study is based on a comparative analysis of a case study of nine cyber incidents from 2017 to 2025 from the moment when ransomware became massive and destructive to modern, targeted attacks on infrastructure and supply chains.
Findings: Based on the analysis, it was concluded that cyberattacks have evolved towards total operational paralysis and attacks on the supply chain. Key takeaways for management include: the need to implement MFA as an absolute minimum, the urgent need for OT/IT network segmentation, and shifting management attention from security alone to vendor resiliency and liquidity management.
Research limitations/implications: The analysis is based on publicly available data and official company communications, which can lead to limitations in fully understanding the internal mechanisms and vectors of an attack. Further research may focus on the effectiveness of AI in repelling cyberattacks and the long-term impact of NIS2 regulation on enterprise risk management.
Practical implications: The article provides practical recommendations for boards, focusing on: Investing in BCP testing and total paralysis scenarios, recognizing the Cyber-CISO as an integral board member, Establishing supply chain audits as a critical process.
Social implications: The increase in attacks on Critical Infrastructure requires strengthening public-private partnerships and creating crisis communication standards to counter disinformation.
Originality/value: The work is distinguished by a holistic approach to the evolution of cyber threats (2017-2025) and the transfer of the emphasis of cybersecurity from technology to business management.
Keywords: enterprise management, cyber threats, cyber resilience.
Category of the paper: Case study.

1. Introduction

In the age of digitalization, where the boundaries between the virtual and real worlds are becoming increasingly fluid, cybersecurity has evolved from a niche area of concern to a key element of national, economic, and corporate security strategies. Enterprises, regardless of their size or industry, are on the brink of this change, facing increasingly complex and advanced digital threats. In a turbulent environment, characterized by rapid technological, political and social changes, cybersecurity management requires not only reactive actions, but above all a proactive attitude and adaptive strategies (Antczak, 2024). As a result, cybersecurity has become a fundamental strategic challenge, not just information technology, directly affecting operational continuity, reputation and market trust. The dynamic evolution of threats, especially in the area of hybrid warfare and attacks on supply chains, requires managers to fundamentally change their approach to risk.

The global cost of cybercrime is projected to reach $10.5 trillion annually by 2025. The average global cost of a data breach in 2024 was $4.88 million, an increase of 10% from the previous year. The healthcare sector remains the most costly in terms of data breaches, with an average cost of more than $9.77 million in 2024 (IBM Security. Cost of a Data Breach Report**,** 2024) The use of artificial intelligence (AI) and automation has made it possible to reduce the cost of data breaches by up to $1.88 million. (IBM Security. Cost of a Data Breach Report**,** 2024). Pshing remains the main breach vector, accounting for the majority of human incidents, which occurs in about 68% of cases, while the growing identity attacks, accounting for more than 99% of all attacks, are increasingly focused on circumventing Multi-Factor Authentication (MFA) (IBM Security. Cost of a Data Breach Report**,** 2024; Verizon – Data Breach Investigations Report, 2024; Microsoft – Digital Defense Report, 2024).

Generative AI has become a key tool for cybercriminals, the number of attacks based on algorithm-assisted social engineering has increased by 442%, and about half of criminal groups have incorporated AI into their strategies. At the same time, attacks on supply chains, the main consequence of which are financial losses, and ransomware, the number of which in the first quarter of 2025 increased by 126% compared to the previous year, reaching a record level (Fortinet – Cyberthreat Predictions**,** 2024; Fortinet **–** State of Operational Technology and Cybersecurity Report**,** 2024; SentinelOne – Annual Threat Hunting Report**,** 2024; Check Point Research – Cyber Security Report, 2024; Proofpoint – State of the Phish Report, 2024).

The U.S. remains a prime target for cyberattacks due to its economic, technological, and political importance, recording the highest number of data breaches and ransomware incidents and the highest costs averaging more than $9 million in 2024, with attacks focusing on industrial espionage, critical infrastructure, and the financial and technology sectors (IBM Cost of a Data Breach Report**,** 2024). The UK remains one of the most targeted countries in Western Europe, particularly in the financial, government and healthcare sectors, with many

incidents linked to Russian and Chinese APT groups using advanced economic and political espionage techniques (CERT-EU – Threat Landscape Report, 2024). The Eastern European region remains the most vulnerable to hybrid warfare cyberattacks, with Ukraine becoming the most attacked country since the beginning of the full-scale invasion, with 90% of sabotage activities carried out by groups linked to Russia. Poland, due to its role as a logistics center and NATO border, is a prime target for disinformation and attacks disrupting government, media and transport, recording one of the largest increases in the number of advanced attacks in Europe (Microsoft Digital Defense Report Microsoft Digital Defense Report, 2024 and 2025). Asian countries such as Japan and South Korea remain the main targets of cyberattacks targeting the manufacturing and technology sectors, particularly semiconductors, and many incidents linked to China and North Korea focus on intellectual property theft and supply chain violations (CERT-EU – Threat Landscape Report**,** 2024).

Modern business management is based on the assumption of operational stability. The evolution of cyber threats after 2017 completely invalidated this assumption. Cybersecurity has ceased to be the exclusive domain of IT departments and has become a major business risk that directly affects strategic goals, financial stability, and corporate reputation.

2. Literature review

The management of modern enterprises is characterized by high complexity and variability of conditions. On a daily basis, managers have to face such challenges as: globalization, dynamic ICT development, cultural diversity, variability of legal and systemic regulations, increasing dynamics of business processes and growing customer expectations. In these conditions, professionalization of management, consisting in creating system solutions and managing them with the use of specific tools, becomes a necessity. An intuitive approach, variability of operating rules, lack of vision and low efficiency of organizational processes are the main factors of failure in modern management (Czekaj, Ziębickiego, 2021). Enterprise management is an integrated set of activities, processes and functions aimed at planning, organizing, motivating and controlling an organization's resources (human, financial, technological) in order to achieve its strategic goals and maximize value for stakeholders (Fayol, 1949). Every company, in order to function properly in a competitive environment, must be properly managed. Management is a complex process that involves all links of an organization's operations. The specificity of the organization is always associated with a multifaceted management process. Management is about making the right management decisions, thanks to which the organization is able to function properly and achieve the assumed goals (Antczak, 2020).

In the context of risk analysis, enterprise management includes, m.in: corporate governance and risk management. Corporate governance deals with the ways in which suppliers of finance to corporationsassure themselves of getting a return on their investment (Shleifer, Vishny, 1997). As part of corporate governance, rules and a framework for supervision and decision-making structure are established, which is crucial for the placement of cybersecurity at the strategic level.

Risk management ensures that enterprise risk related to the use of information technology is identified, analyzed, and mitigated so that it is kept within acceptable levels and aligned with the enterprise's overall risk appetite and business objectives (ISACA, 2019).

As part of enterprise risk management, it is crucial to establish an IT governance and management framework that integrates technology risk into business objectives by systematically identifying and allocating resources to mitigate cyber threats. In the era of digital transformation, enterprise management includes not only the classic processes of planning, organizing and control, but also systematically taking into account cyber threats as a key element of the risk environment, affecting the stability and achievement of strategic goals.

National Intiative for Cybersecurity Careers Studies (NICCS) It defined cybersecurity as a strategy, policy and norms concerning both cyberspace security and activities in it, encompassing a full range of activities aimed at reducing threats, reducing vulnerability and deterrence, international engagement taking into account relevant operations in the computer network and providing information, activities of law enforcement agencies, diplomacy, military, intelligence services, relating to security and global stability information and communication infrastructure (Banasiński, 2023). Cybersecurity for the company is of great importance, in addition to, of course, the security of the company's assets and customer data, cyber defense has an impact on the valuation of a given company. It is a solid pillar ensuring the stability of operations, which is increasingly placed higher in the hierarchy of investment ratings by investors (Bolland). It is inextricably linked to cyberspace, understood as "[...] the global domain of the information environment consisting of the interdependent networks created by information technology (IT) infrastructure and the data contained therein, including the Internet, telecommunications networks, computer systems, as well as the processes and controllers embedded in them (Chałubińska-Jentkiewicz, 2019).

Cybersecurity management is a comprehensive strategic and operational process, including the identification, assessment and mitigation of risks related to cyber threats. Cybersecurity management integrates technologies, policies, procedures, and human resources to protect the integrity, confidentiality, and availability of data and information systems. Effective cybersecurity management involves continuous monitoring and analysis of threats, proactive implementation of protective measures, education and training of employees, as well as cooperation with external entities in the field of information exchange and best practices. The foundation of cybersecurity management is adaptation to the dynamically changing

technological and regulatory environment, taking into account the specifics of the organization's operations and its strategic business goals (Antczak, 2024).

A cyber threat is a potential threat or malicious intent that could exploit a vulnerability (weakness in a system, process, or control) to compromise the confidentiality, integrity, or availability of digital assets (data, systems, IT/OT infrastructure) (NIST, 2018).

Hacking into an end device, i.e. a smartphone, tablet, laptop, computer, printer, or multifunctional device, connected to a company or official network, used by an employee or official, is a simple way for a hacker to steal closely guarded internal data and information, or even a possibility of endangering the functioning of an entire organization or an important structure of the state. To do this, cybercriminals are using increasingly sophisticated methods, often based on carelessness and carelessness in the use of modern devices by their users (Cyberbezpieczeństwo w Polsce, 2019).

Cyberattack methods include, m.in: bots and viruses, phishing and pharming, ransomware, juice jacking, clickjacking, eavesdropping and man-in-the-middle (MITM) attacks, SPAM (shoulder pork and ham), advanced targeted attacks (APT – advanced persistent threat), denial of service/distributed denial of service (DoS/DDoS) attacks, malware data leaks, employee data theft, data leakage due to theft or loss of media or mobile devices, application bug attacks, attacks on wireless networks, data theft due to physical security breaches, hacking of mobile devices (Antczak, 2024).

Cyber threats are a source of cyber risk, which is a measure of the likelihood and scale of a negative impact of an attack on a company's operations.

Cybersecurity risk is the effect of uncertainty about information and technology, referring to the potential loss of confidentiality, integrity or availability of data and information systems, as well as possible negative effects on the operations of an organization, its resources, individuals, other entities and the state (CSRC).

The evolution of cyber threats has shifted cyber risk from the operational to the strategic level, making it an integral part of enterprise risk management. Critical incidents prove that neglecting cyber hygiene is a strategic mistake that prevents business goals from being achieved. In accordance with the COSO ERM guidelines (COSO 2017), vertical and horizontal integration of technological risk is necessary with decision-making processes. Cyber threats are forcing executives to undergo organizational transformation in which resilience, rather than prevention itself, has become a new, overarching strategic value.

The evolution of cyber risk to the level of strategic risk and the blurring of the security boundary has been directly reflected in the European legal framework. Ensuring security in the company is also of key importance from the perspective of the applicable laws and regulations, especially the most important ones, established by the European Union. The NIS2 Directive (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union) establishes common standards for ensuring a high level of security of network and information

systems in the Member States. It requires organizations to implement risk management systems, report major security incidents, and maintain appropriate technical and organizational measures. The CER Directive (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC) complements the NIS2 regulations and focuses on the resilience of entities in charge of critical infrastructure. Its aim is to ensure the continuity of operations of essential services such as energy, transport, communications and healthcare, even in situations of disruption or cyberattacks. The General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) imposes an obligation on organizations to protect personal data by implementing appropriate technical and organizational measures. This regulation aims not only to ensure the privacy of EU citizens, but also to increase trust in digital services.

3. Methodology

The evolution of cyber threats has forced a strategic paradigm shift in enterprise management. The dynamic development of attack methods – from mass ransomware to targeted actions on Critical Infrastructure and supply chains – has made cyber risk a key element of Corporate Governance and Strategic Risk Management. The aim of the research is to define the evolution of cyber threats and assess its impact on the strategic priorities of the board.

Achieving the goal of the research was possible thanks to the use of methodological triangulation, including literature analysis, examination of existing documents and case studies.

The analysis covered nine cyberattacks from 2017 to 2025, which began with an attack on the National Health Service in 2017, where the target was an easy, widely available vulnerability (EternalBlue) and quick profit, and ended with an attack on Jaguar Land Rover in 2025, which caused paralysis of IT systems, several weeks of production shutdown in factories and financial losses:

1. On May 12, 2017, the National Health Service (NHS), the UK's public health service, Europe's largest employer and a key component of the state's critical infrastructure, was paralyzed by the WannaCry cyberattack. This attack exploited the EternalBlue vulnerability to automatically scan and infect the non-patched Windows operating system. The malware quickly encrypted files by demanding a ransom. The incident led to the paralysis of IT systems in medical facilities, resulting in the cancellation of thousands of appointments and surgeries, demonstrating how neglecting basic cyber hygiene can endanger public safety.

2. On October 20, 2020, Sopra Steria, a European leader in technology and consulting services, a key part of the supply chain for sectors such as banking and defense, fell victim to a Ryuk ransomware attack. The attack, which likely began with a phishing email, led to the encryption of some systems throughout the organization. Despite reducing the scale of data leakage due to rapid network isolation, the company incurred significant operational costs related to restoring the efficiency of systems.
3. In December 2020, an unprecedented attack on SolarWinds, an American technology company whose network management software (Orion) is a critical point in the supply chain, was revealed. It was a sophisticated supply chain attack in which hackers (APT group) injected malicious code into a legitimate Orion software update. Once installed, this code opened a backdoor, allowing long-term, stealthy access and spying on the systems of thousands of customers around the world, including key government agencies.
4. On May 7, 2021, Colonial Pipeline, the largest fuel pipeline operator in the United States and a strategic component of Critical Infrastructure, supplying approximately 45% of the U.S. East Coast, was paralyzed by a DarkSide ransomware attack. The attack, which likely exploited stolen remote access credentials (VPNs) in the absence of MFA, prevented access to billing and operating systems. The company preemptively halted the entire pipeline, which triggered a fuel crisis and a buying panic, forcing the operator to pay a ransom to regain control.
5. On February 8, 2021, CD Projekt Red, a Polish video game development studio whose value is largely based on intellectual property (source codes for The Witcher and Cyberpunk 2077 games), fell victim to a ransomware attack. The attack led to the encryption of servers in the company's network and the theft of confidential data. The hackers demanded a ransom for the decryption key and not disclosing the stolen codes. The studio refused to pay, proceeding to restore systems from its own backups, demonstrating resistance to double extortion tactics.
6. On February 5, 2021, there was sabotage at the Florida Water Treatment Plant, a critical infrastructure utility facility whose operating systems (OT/ICS) control chemical processes and the distribution of drinking water. The hackers gained remote access through an unsecured connection and attempted to increase the level of poison in the water. This incident highlighted the direct threat to life and public health resulting from the lack of segmentation of the OT/ICS network.
7. On May 31, 2023, there was a massive attack on MOVEit Transfer software (from Progress Software), used globally to manage the Secure Transfer of Sensitive Files (MFT). The attack exploited a previously unknown Zero-Day vulnerability, allowing hackers to launch an SQL Injection attack. As a result, data was stolen from the databases of hundreds of customers and millions of people around the world were affected, making this incident an example of a large-scale attack on the supply chain.

8. On 29 May 2024, the Polish Press Agency (PAP) – the central, public news service and part of the Critical Communication and Media Infrastructure – fell victim to an act of disinformation and sabotage. The incident involved taking control of an account in the editing system (possibly by social engineering or malware), which made it possible to publish two false cables about military mobilization. The attack, although not ransomware, had a major social impact, demonstrating the use of cyberspace for information destabilization purposes.
9. On August 31, 2025, Jaguar Land Rover Group (JLR), a British multinational car manufacturer (a subsidiary of Tata Motors) that relies on a complex global supply chain and logistics, was attacked by ransomware. The attack began over the weekend, giving the attackers time to encrypt key IT systems, deliberately paralyzing production and logistics management systems. As a result, the factories were shut down, which immediately resulted in significant financial losses and leaks of confidential projects, exposing the vulnerability of Just-in-Time processes.

The analysis of selected cases was carried out on the basis of standardized comparative criteria, such as: type of incident, attack vector, effects of the event and the resulting management conclusions.

The selection of nine breakthrough cyberattacks from 2017 to 2025 provides a sufficient basis for a case study. The analyzed incidents do not serve statistical purposes, but focus on the most transformative moments that directly affected the global economy and national security, while forcing fundamental changes in the way risk management is evaluated in terms of business continuity, reputation, regulatory compliance and management decision-making processes.

4. Results

The analyzed attacks (Table 1) illustrate four main trends that shaped the landscape and indicated important directions for the evolution of cyber threats in the years 2017-2025:

1. The Dominance and Evolution of Ransomware - The trend shows how ransomware attacks have evolved from massive, untargeted infections (e.g. the NHS, exploiting common vulnerabilities like EternalBlue) to a dominant and targeted financial attack model. Nowadays (e.g. Colonial Pipeline, JLR) these attacks are aimed at maximizing losses and extorting ransoms, which in 2021 (e.g. Colonial Pipeline) proved that a cyberattack can cause a social and fuel crisis.
2. Operational Paralysis and Critical Infrastructure Targeting - there has been a shift from targeting only IT networks to attacking OT (Operational Technology) and Critical Infrastructure systems (e.g. Colonial Pipeline, Water Treatment Plant, JLR). The main

goal of these evolutionary attacks has ceased to be encryption itself, but has become a direct disruption of business processes and production halts (e.g. JLR). These effects go beyond financial losses, leading to physical hazards and a public crisis.

3. Increased supply chain risk – Supply chain attacks (e.g., SolarWinds, MOVEit Transfer, Sopra Steria) have become the most sophisticated method of infiltration. Using trust as a vector, hackers inject malicious code into legitimate software or exploit vulnerabilities in common tools. This allows hundreds or thousands of organizations to be compromised en masse and silently at once, making detection much more difficult.
4. Reputational, geopolitical and information warfare risk – the trend represents the evolution of attack targets beyond pure financial gain. The increase in the importance of information warfare (e.g. PAP) and political sabotage shows that cyberspace is used to destabilize society and lose trust in sources of information. The theft of key intellectual property (e.g. CD Projekt Red) is also treated on a par with ransom, and the result is a direct threat to the strategic stability of the organization.

Table 1.
Analysis of selected cyberattacks from 2017-2025

Attack	Incident type	Attack vector	Effects of the attack	Conclusions for management
National Health Service (NHS) (2017)	Ransomware (WannaCry)	Exploitation of an unpatched bug (vulnerability) in Windows systems (EternalBlue vulnerability).	Cancelled near Paralysis of the NHS, cancellation of thousands of surgeries, global financial losses	The need to immediately patch management and withdraw obsolete software.
Sopra Steria (2020)	Ransomware (Ryuk)	Initial infection (possibly via Phishing or remote access).	Limited data leakage but significant operational disruption (a few weeks to fully restore systems).	Network segmentation and improvement of detection and rapid response to new malware variants.
SolarWinds (2020)	Supply Chain Attack / Espionage (APT)	Introduction malicious code for a legitimate Orion software update (the so-called *backdoor*).	To compromise thousands of organizations around the world, including U.S. government agencies. Long-lasting, hidden data leakage.	Verify and monitor code in the software supply chain and strengthen oversight of third-party program permissions.
Colonial Pipeline (2021)	Ransomware (DarkSide)	Probably through hijacked user account/VPN, no MFA.	Suspension of fuel supplies on the East Coast of the USA, buying panic. A ransom of $4.4 million was paid.	Separation of OT/IT systems and mandatory implementation of strong authentication (MFA) in remote access systems.
CD Projekt (2021)	Ransomware	Undisclosed, but typically by phishing or exploitation of a remote access vulnerability.	Network encryption and leakage of confidential company data (game source codes, employee documents). Refusal to pay the ransom.	Restriction of privileged accounts and improvement of secure backup processes.

Cont. table 1.

Water Treatment Plant (2021)	Sabotage of the water supply system	Hacking into OT systems through unsecured remote access.	Potential water contamination, a direct threat to life and public health.	Absolute segmentation of OT/ICS networks from IT; implementation of NIS2 standards and audits
MOVEit (2023)	Supply Chain Attack / Data Leak	Exploitation of the Zero-Day SQL Injection vulnerability in MOVEit.	Stealing the data of millions of people and hundreds of companies that are MOVEit customers.	Immediate patching of zero-day vulnerabilities and caution when using third-party data management software.
Polish Press Agency (PAP) (2024)	Disinformation / Sabotage	Using malware to infiltrate and take over an employee's account.	Publishing two false cables about the alleged mobilization. Major information disruption.	Strengthening pre-publication identity verification protocols and educating staff in social engineering.
Jaguar Land Rover (JLR) (2025)	Ransomware	Probably phishing or exploitation of a VPN/Remote Access vulnerability (no MFA).	Paralysis of production for several weeks, billions in financial losses, leakage of confidential projects and data.	Separation of OT/IT systems, implementation of the principle of least privilege and provision of isolated backups (immutable backups).

Źródło: opracowanie własne na podstawie: https://www.avast.com/pl-pl/business/resources/what-is-hospital-ransomware; https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure-security-agency-0; https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft; https://businessinsider.com.pl/wiadomosci/falszywa-depesza-pap-o-mobilizacji-prawdopodobnie-rosyjski-cyberatak/5xpvswx; https://sekurak.pl/atak-ransomware-na-operatora-rurociagu-w-usa-tworza-sie-kolejki-na-stacje-benzynowe-w-kolejnych-stanach-zostaje-ogloszony-stan-wyjatkowy/; https://www.money.pl/ gospodarka/atak-na-cd-projekt-przestroga-dla-biznesu-hakerzy-tylko-czekaja-na-szanse-6608799701908288a.html; https://www.soprasteria.com/docs/librariesprovider2/sopra-steria-corporate/cp/211020_information-on-a-cyberattack-en.pdf?sfvrsn=313205dc_4; https://new.org.pl/1054,breczko_solarwinds.html

The evolution of cyber threats between 2017 and 2025 is a transformation of motivations and attack vectors from massive, opportunistic ransomware (e.g. the NHS) to targeted and strategic actions. These activities focus on achieving operational paralysis (e.g., Colonial Pipeline, JLR, Water Treatment Plant), using the supply chain as the main channel of infiltration (e.g., SolarWinds, MOVEit, Sopra Steria), intellectual property theft (e.g., CD Projekt), and geopolitical destabilization (e.g., attack on PAP). This evolution is forcing the Board to shift priorities from security alone to enterprise-wide resiliency management.

5. Discussion

This article is part of the dominant trend of scientific literature in the years 2024-2025 (e.g. Antczak, 2024; Banasiński, 2023; Al-Shattarat et al., 2025), which redefines cybersecurity from a technological problem to a key challenge of corporate governance. This phenomenon, described in the literature as a transition to strategic resilience (cyber-resilience), emphasizes

that in the era of regulations such as NIS2 and DORA, the responsibility for operational continuity lies directly with management bodies, which requires them to develop the so-called dynamic adaptability (Li, Liu, 2021).

In the publication, Y. Harel1 and A. Carmeli similarly argue that cybersecurity is a "dynamic capability" that must be constantly renegotiated by the board (Harel, Carmeli, 2025). The authors analyze strategic supervision as a dynamic management capability. They point out that cybersecurity must evolve from technical aspects to tools for creating long-term value**.** This article complements this theory with practical evidence, indicating that cybersecurity has become a major business risk affecting strategic goals and reputation. M. Alshammari et al., on the other hand, analyze the evolution from "cybersecurity" to "cyber resilience", which confirms that in a turbulent environment, it is impossible to avoid an attack, so management must focus on the ability to survive (Alshammari et al., 2023). What has been analyzed on the example of JLR and CD Projekt Red). This article corresponds with the latest findings of Abdullah et al. (Abdullah et al., 2025) on the evolution of cyber threats. Abdullaha et al. present a broad historical and statistical background for AI-driven attacks targeting supply chains. This article fills a gap in the area of management sciences, translating these trends into specific models of management responsibility and decision-making processes in the era of implementation of the NIS2 directive. M. Smith, P. Daniel focus mainly on fiduciary duties and financial consequences of ransomware attacks, this article expands this approach to include the dimension of strategic management and organizational theory (Smith, Daniel, 2025). By analyzing cases such as Jaguar Land Rover (2025), the paper shows that modern cybersecurity is not just a matter of oversight, but a process of continuous reconfiguration of resources in order to maintain business continuity in a turbulent geopolitical environment, which is an important complement to the achievements presented in current market analyses.

Al-Shattarata et al. analyze a review of the literature in the field of business and accounting (Al-Shattarat et al.2025), while this article is an analysis of the study of cyberattacks on the decision-making processes of management boards. Both works agree on a key paradigm shift: cybersecurity has ceased to be a technical issue for IT departments, becoming the foundation of corporate governance and strategic resilience of the company.

Based on the analysis of cyberattacks (Table 1), the following conclusions can be drawn:

1. Operational resilience (in the IT/OT area) is becoming a new priority, replacing security itself as the main goal of cybersecurity activities.
2. The supply chain has now become one of the main attack vectors used by cybercriminals.
3. Businesses are entering a new era of risk, where geopolitical threats and reputational loss are critical to security.

Incident analysis (Colonial Pipeline, JLR, Water Station) proves that the main goal of attacks is to completely paralyze key operations, not just steal data. The hacking of water treatment plants and attacks on IK (Colonial Pipeline) show that operational technology

systems must be completely isolated from the office network. Lack of segmentation is treated as critical negligence. The attack on Colonial Pipeline was made possible by a breach of a VPN account without multi-factor authentication (MFA). MFA has become an absolute, mandatory minimum of cyber hygiene for every user, including remote and privileged access. The attack on JLR, which halted production, shows that management needs to test Business Continuity Plan / Disaster Recovery (BCP/DR) plans for a scenario of total paralysis, not just the loss of individual servers.

The attacks on SolarWinds, MOVEit Transfer and Sopra Steria have proven that the weakest link in security is often the supplier. Management must treat the risks associated with third-party software and services on an equal footing with insider risk. This requires tough audits of suppliers (e.g. compliant with NIS2 standards) and regular assessment of their cyber maturity. The WannaCry attack and the Zeroday vulnerabilities in MOVEit show that keeping your software up-to-date and quickly patching known vulnerabilities (even for systems withdrawn from support) is crucial for global security.

The attacks on CD Projekt Red and PAP indicate that the motivation of cybercriminals is increasingly to destabilize and steal a competitive advantage, and not just ransom. The attack on the Polish Press Agency (PAP) proves that managers must think in terms of hybrid warfare. It is necessary to develop Crisis Communication procedures aimed at combating disinformation and quickly regaining control over the narrative. The CD Projekt Red incident (source code leak) confirms that knowledge-based companies need to strengthen Data Loss Prevention (DLP) mechanisms and tightly control access to critical intellectual property. Ransomware can only be a cover for a more destructive target, which is industrial espionage.

The analysis of 9 cyberattacks clearly shows that effective enterprise protection is based on a culture of resilience that goes beyond traditional security. As a result, effective business management requires constant measurement of resilience levels and incorporating cyber risk into every strategic business decision, from supplier selection to expansion planning.

6. Summary and conclusions

On the basis of the analyzed incidents, the following key conclusions can be drawn in the field of enterprise management in the area of cybersecurity:

1. Managers should treat basic cyber hygiene (such as MFA and Patch Management) as a strategic priority, as neglecting these elements is still the main attack vector (conclusion from cyberattacks: NHS, Colonial Pipeline, Water Treatment Plant).
2. Enterprises should implement strict network segmentation (Zero Trust) so that malware cannot automatically spread from the infected part of the network to key production

systems (OT) and backup servers (conclusion from cyberattacks: JLR, CD Projekt, Water Treatment Plant).

3. Risk management should include rigorous audits and continuous monitoring of the security of vendors' services and software, as each vendor is a potential attack vector for the organization (conclusion from cyberattacks: SolarWinds, MOVEit, Sopra Steria).
4. Effective defense requires the provision of isolated, immutable backups and regular testing of recovery plans to enable a quick recovery from a successful attack, while minimizing reputational and disinformation losses (conclusion from cyberattacks: JLR, Colonial Pipeline, PAP).

Recommendations for management:

1. Recognizing operational paralysis and physical sabotage as a major strategic threat.
2. Prioritize funding and implement isolation of OT/ICS networks from IT networks.
3. Implement MFA as an absolute policy for every remote access and adopt a Zero Trust model for the entire network.
4. Establish a rigorous Vendor Risk Management (VRM) and monitor the Patch Compliance Rate in short timelines.
5. Investments in isolated, immutable backups (3-2-1 strategy) to ensure reproducibility after a ransomware attack.
6. Annual, mandatory testing of BCP/DR plans in "scorched earth" scenarios to shorten the RTO.
7. Investments in modern EDR/XDR systems to quickly detect and isolate ongoing attacks.
8. Development and testing of the Crisis Communication Plan (anti-disinformation procedure) and implementation of DLP systems for the protection of key intellectual property.

The implementation of these recommendations requires the recognition of cybersecurity as a business risk, not just a technical one, and the active involvement of the management and supervisory boards.

Methodological limitations can be identified in the study. The subjective selection of the nine breakthrough incidents focuses mainly on large organizations such as JLR, SolarWinds and the NHS, which, despite their representativeness, is a limitation of the study by potentially omitting the specific challenges of the SME sector. The data from the years 2017-2025 used in the article is a time limitation. The dynamic development of artificial intelligence means that the forecasts contained in it may need to be updated very quickly.

The results of the research have important implications for the wider field of management and can be used in management education and in audit and compliance. The results obtained from the research may form the basis for further research in the field of management in hybrid threat conditions.

References

1. Abdullah, M., Nawaz, M.M., Saleem, B., Zahra, M., Ashfaq, E.b., Muhammad, Z. (2025). Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. *Analytics*, *4*(3), 25. https://doi.org/10.3390/analytics4030025
2. Alshammari, M.A., Alshammari, M.S., Alshammari, A.S. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability, 15(18),* 13369. https://doi.org/10.3390/su151813369
3. Al-Shattarat, W., Benameur, K.B., Mostafa, M.M., Hassanein, A., Hamed, R.S. (2025). A decade of cybersecurity research in business, management, and accounting: bibliometric analyses and future research directions. *Cogent Business & Management, 12(1),* 2544230. https://doi.org/10.1080/23311975.2025.2544230
4. Al-Shattarat, W., Benameur, K.B., Mostafa, M.M., Hassanein, A., Hamed, R.S. (2025). A decade of cybersecurity research in business, management, and accounting: bibliometric analyses and future research directions. *Cogent Business & Management, 12(1).* https://doi.org/10.1080/23311975.2025.2544230
5. Antczak, J. (2020). *Zarządzanie przedsiębiorstwem w cyberprzestrzeni*. Warszawa: Akademia Sztuki Wojennej.
6. Antczak, J. (2024). *Zarządzanie cyberbezpieczeństwem w przedsiębiorstwie - doświadczenia wybranych państw Unii Europejskiej.* Warszawa: Difin.
7. *Atak na CD Projekt przestrogą dla biznesu. Hakerzy tylko czekają na szansę*. Retrieved from: https://www.money.pl/gospodarka/atak-na-cd-projekt-przestroga-dla-biznesu-hakerzy-tylko-czekaja-na-szanse-6608799701908288a.html, 02.10.2025.
8. *Atak na SolarWinds. Prawdopodobnie największy hack w historii* Retrieved from: https://new.org.pl/1054,breczko_solarwinds.html, 02.10.2025.
9. *Atak ransomware na operatora rurociągu w USA. Tworzą się kolejki na stacje benzynowe, w kolejnych stanach zostaje ogłoszony stan wyjątkowy*. Retrieved from: https://sekurak.pl/atak-ransomware-na-operatora-rurociagu-w-usa-tworza-sie-kolejki-na-stacje-benzynowe-w-kolejnych-stanach-zostaje-ogloszony-stan-wyjatkowy/, 02.10.2025.
10. *Atak ransomware na szpitale NHS.* Retrieved from: https://www.avast.com/pl-pl/business/resources/what-is-hospital-ransomware, 02.10.2025.
11. Banasiński, C. (ed.) (2023). *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.
12. Bolland, E. *Social Engineering Explained: Reduce Your Employee Cyber-Security Risk.* Retrieved from: https://blog.usecure.io/employee-social-engineering, 26.07.2025.
13. *CERT-EU – Threat Landscape Report 2024*. Retrieved from: https://cert.europa.eu/publications/threat-intelligence/tlr2024/, 26.07.2025.

14. Chałubińska-Jentkiewicz, K. (2019), Cyberbepieczeństwo – zagadnienia definicyjne, *Cybersecurity and Law*, *nr 2*.
15. *Check Point Research – Cyber Security Report 2024*. Retrieved from: https://www.checkpoint.com/resources/report-3854/report--cyber-security-report-2024-3a0a, 26.07.2025.
16. COSO (2017). *Enterprise Risk Management—Integrating with Strategy and Performance.* The Committee of Sponsoring Organizations of the Treadway Commission. Retrieved from: https://www.slideshare.net/slideshow/2017-cosoermintegratingwithstrategyand performanceexecutivesummary/81372772, 26.07.2025.
17. Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań. *Cyfrowa Polska, styczeń 2019*. Warszawa.
18. *Cybersecurity Risk – Glossary*. Retrieved from: https://csrc.nist.gov/glossary/term/ cybersecurity_risk, 26.07.2025.
19. Czekaj, J., Ziębickiego, B. (2021). *Współczesne zarządzanie. Koncepcje, metody, systemy*, Kraków: Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie.
20. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148. Retrieved from: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555, 25.10.2025.
21. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE.
22. *Fałszywa depesza PAP o mobilizacji*. *"Prawdopodobnie rosyjski cyberatak"*. Retrieved from: https://businessinsider.com.pl/wiadomosci/falszywa-depesza-pap-o-mobilizacji-prawdopodobnie-rosyjski-cyberatak/5xpvswx, 26.09.2025.
23. Fayol, H. (1949). *General and industrial management*. London: Sir Isaac Pitman & Sons, Ltd.
24. *Fortinet – 2024 State of Operational Technology and Cybersecurity Report*. Retrieved from: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf
25. *Fortinet – Cyberthreat Predictions 2024*. Retrieved from: https://www.fortinet.com/ content/dam/fortinet/assets/threat-reports/report-threat-prediction-2024.pdf, 26.07.2025.
26. Harel, Y., Carmeli, A. (2025). A strategic cybersecurity oversight framework: a board's imperative. *Journal of Cybersecurity*, *11*(1), https://doi.org/10.1093/cybsec/tyaf021
27. *IBM Security. Cost of a Data Breach Report 2024*. Retrieved from: https://www.ibm.com/think/insights/whats-new-2024-cost-of-a-data-breach-report, 26.07.2025.

28. *Information on a cyberattack*. Retrieved from: https://www.soprasteria.com/docs/librariesprovider2/sopra-steria-corporate/cp/211020_information-on-a-cyberattack-en.pdf?sfvrsn=313205dc_4, 26.10.2025.
29. ISACA (2019). *COBIT 2019 Framework: Governance and Management Objectives*. Information Systems Audit and Control Association.
30. Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA). Retrieved from: https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure-security-agency-0, 26.10.2025.
31. Li, Y., Liu, Y. (2021). Cybersecurity as a dynamic capability: Antecedents, resources and performance. *Information & Management, 58(8),* 103409. https://doi.org/10.1016/j.im.2020.103409
32. *Microsoft – Digital Defense Report 2024*. Retrieved from: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024, 06.11.2025.
33. *Microsoft Digital Defense Report Microsoft Digital Defense Report 2024.* Retrieved from: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024, 06.11.2025.
34. *Microsoft Digital Defense Report Microsoft Digital Defense Report 2025.* Retrieved from: https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/, 06.11.2025.
35. NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).* National Institute of Standards and Technology. Retrieved from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, 06.11.2025.
36. *Proofpoint – State of the Phish Report 2024.* Retrieved from: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish, 06.11.2025.
37. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
38. *SentinelOne – Annual Threat Hunting Report 2024*. Retrieved from: https://www.sentinelone.com/resources/reports/annual-threat-hunting-report-2024/, 16.11.2025.
39. Shleifer, A., Vishny, R.W. (1997). A Survey of Corporate Governance. *The Journal of Finance*, *52(2),* 737-783. DOI: 10.1111/j.1540-6261.1997.tb04820.x

40. Smith, M., Daniel, P. (2025). *Why Cybersecurity Should Be a Boardroom Priority*. Retrieved from: https://www.researchgate.net/publication/394400809_WHY_CYBERSECURITY_SHOULD_BE_A_BOARDORM_PRIORITY, 10.02.2026.
41. *Verizon – Data Breach Investigations Report 2024*. Retrieved from: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf, 06.11.2025.
42. *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*. Retrieved from: https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft, 06.11.2025.