CYBER THREATS EVOLUTION IN INDUSTRIAL ENVIRONMENTS AND FOUNDATIONS OF CYBERSECURITY INTEGRATION INTO RISK MANAGEMENT

First A. Drd. Corina-Maria Ciobanu, *National University of Science and Technology POLITEHNIC, Bucharest, ROMANIA*
Second B. Prof. dr. ing. Oana Roxana CHIVU, *National University of Science and Technology POLITEHNIC, Bucharest, ROMANIA*
Third B. Prof. dr. ing. Liviu Marius CÎRȚÎNĂ, *National University of Science and Technology POLITEHNIC, Bucharest, ROMANIA*
Fourth B. Drd. Andrei Ștefan IACOB, *National University of Science and Technology POLITEHNIC, Bucharest, ROMANIA*
Fiveth B. Conf. dr. ing Marinela Nicoleta MARINESCU., *National University of Science and Technology POLITEHNIC, Bucharest, ROMANIA*
Sixth B. Conf. dr. ing.. Larisa BUȚU, *National University of Science and Technology POLITEHNIC, Bucharest, ROMANIA*

ABSTRACT: The rapid digitalization of industrial processes, along with the increasing interdependence between information technology (IT) and operational technology (OT) systems has fundamentally transformed the industrial risk profile. This study explores how cyber threats against industrial environments have evolved, showing a clear transition from data-centered breaches to incidents that directly affect production continuity, safety functions, and managerial control. By leveraging a review of contemporary research and real-world security breaches, this investigation isolates five principal trends, namely IT/OT integration, supply-chain exploitation, ransomware evolution, IIoT and cloud exposure, and safety-system manipulation, and develops a clear, structured classification of cyber threats relevant to industrial settings.

KEY WORDS: cybersecurity, risk management, industrial systems, procedures, cyber threats

1. INTRODUCTION

The accelerated digital transformation of industrial enterprises is driven by the indispensable convergence of operational technology (OT) and information technology (IT), the expansive deployment of Industrial Internet of Things networks, and the use of cloud and edge services, yielding unprecedented gains in productivity and operational agility.

This indispensable integration introduces a formidable challenge, a significantly expanded cyber-attack surface, which threatens the safety and continuity of critical industrial processes through novel and evolving vulnerabilities.

Existing risk management frameworks (ISO 31000, COSO) and security standards (IEC 62443, ISO/IEC 27001) address complementary objectives but seldom intersect in practice.

This paper reviews how industrial cyber threats have evolved and outline the foundations for embedding cybersecurity strategy into holistic enterprise risk management, thereby substantially strengthening industrial resilience against contemporary digital threats.

2. THEORETICAL FOUNDATIONS ABOUT RISK MANAGEMENT AND INDUSTRIAL CYBERSECURITY

Risk management in industrial context:
Constituting a core discipline, risk management is defined as the systematic process utilized for detecting, evaluating, and mitigating vulnerabilities and threats that stand against the achievement of organizational goals, the preservation of assets, and the safeguarding of stakeholders' interests [1].
In industrial contexts, the scope of risk management practice transcends conventional concerns like financial stability and regulatory compliance. Instead, there are included vital areas such as operational resilience, human safety and environmental protection [2]. The nature of industrial operations, continuous processes, safety-critical systems, and interdependent supply chains, requires risk decisions that balance residual exposure with productivity, availability and regulatory constraints. This complex task is supported by structured frameworks like ISO 31000 and COSO ERM. ISO 31000 supplies the universal principles and a procedural lifecycle for managing risk [3], while COSO ERM emphasizes integration with corporate strategy and performance [4]. Collectively, these frameworks serve to institutionalize a systematic, transparent and proactive approach to risk, thereby supporting governance, accountability, and continuous improvement across organizational levels.
Cybersecurity relevance in industry: The effort to protect systems, networks, and digital assets from threats that could compromise the confidentiality, integrity, or availability of information [5]. Evolving into a multidisciplinary field encompassing computer science, risk management, and governance, its primary goal is to ensure resilience and continuity across interdependent socio-technical systems.
In industrial context, cybersecurity mandates the protection of Operational Technology (OT), including industrial control systems (ICS), supervisory control and data acquisition (SCADA) networks, and programmable logic controllers (PLCs) which govern physical operations [6]. Unlike traditional IT networks, these systems operate under strict real-time, safety, and availability constraints, often using legacy protocols that were not designed with security in mind.
Mitigating cyber risk must therefore address the potential for both digital intrusion and severe physical outcomes, including critical infrastructure damage and risks to human safety. This critical function is standardized by specialized international frameworks, including the IEC 62443 series for industrial automation, the management system requirements of ISO/IEC 27001 [7], and the ICS-specific guidance of NIST SP 800-82. These standards facilitate the essential implementation of a multi-layered security strategy aligned with enterprise governance [8].
Integrating cybersecurity into the enterprise risk management lifecycle: Despite sharing the fundamental goals of protecting assets, ensuring continuity, and informing decision-making, the disciplines of risk management and cybersecurity frequently operate in organizational isolation [9]. Risk management frameworks traditionally emphasize governance, strategy, and enterprise-wide oversight, whereas cybersecurity often remains limited to technical controls and compliance. This structural dichotomy frequently results in a governance deficiency where cyber risks are mistakenly reduced to technical issues rather than being considered core elements of the enterprise risk portfolio [10].
To achieve genuine industrial resilience, institutional research strongly advocates for embedding cybersecurity within the broader risk management lifecycle [11]. This integrated model facilitates the consistent assessment of cyber threats using a unified structure for determining likelihood, impact, and treatment priorities. By translating technical vulnerabilities into business-oriented risk indicators, organizations can align cyber-defense measures with their overall risk appetite and tolerance threshold. From a practical perspective, integration is established by correlating the procedural steps of ISO 31000 directly against the technical and governance controls found in IEC 62443 [12] and ISO/IEC 27001. This mapping ensures that technical cybersecurity activities directly contribute to the relevant enterprise

risk management functions, which is supported by the NIST Cybersecurity Framework.

3. EVOLUTION OF CYBER THREATS IN INDUSTRIAL ENVIRONMENTS

Driven by technological advancements in automation, integrated control systems, and data-centric production, industrial enterprises are undergoing a profound digital transformation that has radically altered their risk exposure. The convergence of operational technology (OT) and information technology (IT) ensures that digital vulnerabilities are no longer limited to data loss but can directly compromise physical control systems, manufacturing integrity, and personnel safety. The historical progression of cyber threats against industrial environments can be analyzed across three major phases, mirroring advances in technology together with increasing sophistication in adversarial tactics.

Phase 1 - from isolated systems to connected networks (Before 2010)

In the early stages of industrial automation, before 2010, most control systems operated in air-gapped or standalone configurations. Security relied predominantly on physical access restrictions and the protection of proprietary software. Cyber exposure stemmed largely from opportunistic malware or misconfigurations originating from corporate IT networks, such as Morris Worm, Code Red or SQL Slammer that caused Denial-of-Service through HMI or workstation failure [13]. Furthermore, the lack of inherent security mechanisms like encryption and authentication in legacy industrial protocols posed a fundamental weakness. Crucially, risks were heightened by insider threats and operator error, as unintentional actions or the introduction of infected media (USB drives) by authorized personnel could circumvent physical controls.

While direct, motivated manipulation of physical processes was rare due to adversaries lacking domain-specific OT knowledge, these collateral and internal threats were sufficient to compromise system availability and integrity.

This convergence represents a critical enabler for industrial resilience, granting strategic accountability, forming a critical foundation for operational safety and business continuity.

Phase 2 – the rise of targeted industrial attacks (2010-2020)

A decisive shift occurred with the emergence of targeted, state-sponsored or highly organized campaigns specifically engineered to manipulate physical processes. The 2010 Stuxnet incident [14] demonstrated that industrial control systems could be weaponized, establishing a precedent for subsequent sophisticated attacks, including Havex, BlackEnrgy, Industroyer and Triton/Trisis [15]. The indicators of the period 2010-2020, include the exploitation of supply-chain channels, advanced persistence techniques across IT and OT boundaries and the ability to subvert safety instrumented systems.

This period also saw the professionalization of ransomware groups and the introduction of double-extortion tactics, further complicated the risk landscape by merging financial motivation with potential industrial sabotage. As a result, industrial sector began to recognize cybersecurity as a core operational, non-IT-risk.

Phase 3 – business interruption and supply-chain exploitation (2020-present)

The contemporary threat landscape is defined by the hyper-connectivity and expansive attack surface resulting from industrial digitalization and cloud integration. Threat actors now prioritize disrupting business continuity not only through data encryption but also by deliberately triggering operational shutdowns to prevent ransomware lateral spread into OT environments. Incidents like the 2021 Colonial Pipeline and JBS Foods attacks highlight how IT ransomware can trigger cascading operational consequences, resulting in service interruption and significant financial loss [16].

Modern industrial attacks frequently exploit supply-chain dependencies, third-party remote access, and cloud misconfigurations. The complexity of IIoT ecosystems introduces additional exposure through

insufficient device authentication, insecure firmware, and unmonitored connectivity to external platforms. This systemic shift mandates moving away from security focused purely on confidentiality toward models that prioritize system availability and safety integrity.

4. KEY TRENDS AND CLASSIFICATION OF INDUSTRIAL CYBER THREATS

Recent studies present that industrial cybersecurity has evolved along several recurring patterns that effectively blend technological convergence with systemic vulnerabilities [17]. These emerging patterns underscore the critical shift in modern threats, which increasingly compromise not just information assets but also production continuity and operational safety. This evolution reflects the increasing integration of digital technologies within industrial ecosystems, where the convergence of IT/OT has blurred traditional security boundaries. As digital transformation progresses, industrial systems are now connected to enterprise networks, cloud infrastructures and external service providers.

To support risk assessment, these developments can be organized into a classification of recurring industrial cyber threat patterns. Each trend reflects a cluster of related vulnerabilities, typically attack vectors, and corresponding implications for enterprise risk management.

Tabel 1. Synthesis of industrial cyber threat evolution and associated risk management response

Trend/ Threat category	Description	Implication for risk management
IT/OT convergence	Integration of corporate IT and industrial OT networks breaks down old barriers, opening up common weak spots.	Requires unified risk assessment across digital and physical assets and incidents must be analyzed for operational impact.
Supply-Chain exploitation	Attacks increasingly compromise environments by exploiting vulnerabilities in trusted ecosystem partners, including software updates, remote access portals, and vendor maintenance channels.	Demands supplier risk evaluation, contractual security clauses, and continuous monitoring of third-party access.
Ransomware and destructive malware	Ransomware campaigns now shift focus toward live systems, aiming to halt key functions so hackers can demand bigger payouts.	Prioritize business-impact analysis, tested backups, and integration of incident response planning into continuity management.
Cloud and IIoT expansion	More use of connected sensors (IIoT), intelligent gadgets, or outside cloud systems greatly widens the area and messiness of potential threats.	Needs clear inclusion of cloud safety oversight, solid plans for verifying devices and managing entry, along with constant checks of setup details within the risk management approach.
Safety-critical implications	Cyber attacks might cause dangerous situations or harm nature by altering how systems are controlled.	Experts urge combining safety checks with cyber risk reviews using ISO 31000, while matching practices from IEC 61511.

The classification in Table 1 shows cyber threats in industry are not jut technological glitches anymore, they are now tangled with how companies operate. Instead of rare problems, they have grown into bigger issues affecting entire systems. What used to be separate incidents now connect deeply with management choices. These shifts mean security is not just and IT matter, but involves multiple departments in an organization. As operations rely more on digital tools, weak spots multiply across departments. When tech systems and operational networks link up more tightly, problems can spread through digital setup, physical operations, along with human actions, leading to money losses and risks at once.

These changes show industrial cybersecurity ties closely into overall business risk handling every new shift shapes the way risks get spotted, studied, then acted on through the ISO 31000 method.

5. IMPACT ON INDUSTRIAL PROCESSES AND IMPLICATIONS FOR RISK MANAGEMENT

The ramification of cyber attacks within industrial environments are extensive, moving far beyond the simple loss of informational assets. On the operational front, the primary impact is on availability and production throughput. The compromise of IT systems, frequently via ransomware or encryption, often mandates the precautionary shutdown of interdependent OT networks. This action decreases production efficiency and extends the duration of recovery due to necessary safety validations and qualification protocols. Concurrently, process safety and product quality are at risk, as a cyber event can manipulate control setpoints, suppress critical alarms, or introduce cognitive overload for human operators, thereby increasing the probability of unsafe conditions and procedural errors. Furthermore, these breaches generate significant regulatory and contractual exposure. Mandatory reporting obligations, unmet compliance standards, and breaches of customer Service-level agreements all amplify the resulting financial penalties and reputational damage. Consequently, the full cost needs to include immediate costs like investigations and fixes, but also hidden losses such as lost uptime, weakening brand trust, or higher insurance bills.

The magnitude of these operational consequences provides a compelling rationale for the strategic shift from viewing cybersecurity as a standalone function to integrating it fully into enterprise risk management. To successfully adapt methodologies like ISO 31000 and COSO ERM for industrial contexts, specific cybersecurity criteria must be woven into the risk process stages:

- Finding the starting point means making sure every physical device is part of the risk setup, using standards were keeping systems running and operations safe matter just as much as data accuracy.
- Risk identification and analysis lean on know threat types (Table 1) to fill up the risk log, to assess the how likely an attack is and what would mean for business results through expert input and historical incidents.
- Prioritization and treatment is based on operational criticality and safety proximity. Mitigation steps should tie back to industrial security measures from guidelines such as IEC 62443 and NIST Cybersecurity Framework. This treatment strategy emphasizes key controls, including robust network segmentation and the development of verified system recovery plans.
- Monitoring and governance require keeping one common risk log covering both IT and OT areas, assigning clear ownership for choices, while weaving insights from past incidents straight into management rules over time.

This crucial convergence ensures that cybersecurity transcends a mere technical defense, enabling industrial entities to achieve risk-informed resilience and maintain high levels of safety and productivity.

6. CONCLUSIONS

This paper investigated the evolution of cyber threats within industrial settings, highlighting the raised impact on key areas, keeping operations continuity, ensuring process safety, and shaping company oversight. A synthesis of the most critical trends, including IT/OT integration, broader supply chain weaknesses, also ransomware tactics, allowed for the development of a concise threat taxonomy that defines the modern industrial risk landscape.

The subsequent analysis highlighted the capacity of established risk frameworks, specifically ISO 31000, COSO ERM, and IEC 62443, to serve as a robust, structured foundation for incorporating cybersecurity into enterprise-level decision making. By systematically weaving cyber risk assessments throughout the entire management lifecycle, industrial companies are empowered to abandon reactive security models in favor of risk-informed resilience, thereby sustaining high levels of productivity and safety while managing traditional information risks.

REFERENCES

[1] Hopkin, P. Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. Kogan Page, 2018.

[2] Hillson, D. Practical Project Risk Management: The ATOM Methodology. Management Concepts, 2020.

[3] ISO 31000:2018. Risk Management - Guidelines. International Organization for Standardization, 2018.

[4] COSO. Enterprise Risk Management - Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission, 2017.

[5] ENISA. Industrial Control Systems Security. European Union Agency for Cybersecurity, 2023.

[6] Von Solms, R. & Van Niekerk, J. (2013). "The Concept of Cybersecurity." Computers & Security, 31(1), 97-102.

[7] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27001: Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems - Requirements, Geneva: ISO/IEC, 2022.

[8] NIST SP 800-82 Rev. 2. Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology, 2015.

[9] Linkov, I. & Trump, B. (2019). The Science and Practice of Resilience. Springer.

[10] Von Solms, R. & Van Niekerk, J. (2013). "The Concept of Cybersecurity." Computers & Security, 31(1), 97–102.

[11] NIST Cybersecurity Framework (CSF) 2.0 Draft. National Institute of Standards and Technology, 2024.

[12] International Electrotechnical Commission (IEC), IEC 62443 Series: Industrial Automation and Control Systems Security — Part 1 to 4, Geneva: IEC, 2018.

[13] Zou, C. C., Gao, L., Gong, W., Towsley, D., Monitoring and Early Warning for Internet Worms, University of Massachusetts Amherst, Department of Computer Science, 2003.

[14] Trautman, L.J., & Ormerod, P.C., Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things, 72 U. Miami L. Rev. 761, 2018.

[15] Mekdad, Y., Bernieri, G., Conti, M., El Fergougui, A., The Rise of ICS Malware: A Comparative Analysis, ResearchGate / 2023.

[16] Cybersecurity and Infrastructure Security Agency (CISA). "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years." U.S. Department of Homeland Security, 2023.

[17] Firoozjaei, M. D., et al. An Evaluation Framework for Industrial Control System Cyber-Incidents in the Energy and Power Industries. Energy Reports, Elsevier, 2022.