

CALL FOR PAPERS: MONOTHEMATIC ISSUE 2027 E & M ECONOMICS AND MANAGEMENT

Cybersecurity, Resilience and Digital Trust

This monothematic issue establishes a foundation for interdisciplinary research in the domain of cybersecurity, digital trust, and the economic implications of cyber threats. The accelerated digitalization of businesses, public administration, and society as a whole is an unparalleled escalation in cyber risks, which exert a direct influence on the economy, security, business continuity, and public administration. The objective of this edition is to compile original research and innovative approaches that will facilitate a more profound comprehension of contemporary challenges and enhance the resilience of the digital ecosystem.

Guest Editors

Josef Horálek (Associate Professor)

Faculty of Informatics and Management, University of Hradec Králové (Czech Republic)

(email: josef.horalek@uhk.cz)

Risk management, industrial system security, AI security, cybersecurity management

Filip Holík (Associate Professor)

Department of Information Security and Communication Technology, Norwegian University of Science and Technology (Norway)

(email: filip.holik@ntnu.no)

Cybersecurity, communication networks, programmable data plane, smart grid, industrial networks

Important Dates

Submission open date: June 1, 2026

Manuscript submission deadline: October 31, 2026

The submission of the articles is accepted through the journal's editorial system:

<https://rizeni.ekonomie-management.cz/en/cms/review-process>

After uploading the article, please inform the Editorial Office that the submitted manuscript is intended for the Monothematic Issue (journal@tul.cz).

Publishing of articles: September 2027

Background and Objectives

Despite considerable investments in cybersecurity, the practical implementation of security frameworks in organisations remains mostly inadequate. The increasing digitisation of the world, the proliferation of the Internet of Things (IoT), the pervasive use of artificial intelligence, and intricate supply chains have rendered conventional security methodologies ineffective. Concurrently, the sophistication of cyberattacks is escalating, transcending the confines of mere technical challenges and manifesting as significant economic, social, and geopolitical concerns.

The following issues are of particular significance:

- i. It is evident that there is an absence of adequate integration of technical, organisational and economic perspectives within the domain of cyber risk management practices;
- ii. It is evident that there is a paucity of preparedness among organisations, most notably SMBs and public administrations, for the increasing prevalence of ransomware, supply chain, and AI-enhanced attacks;
- iii. The absence of measurable frameworks for digital trust is a matter of concern, given its importance for business, innovation, and the adoption of new technologies;

- iv. It is evident that the implementation of European regulations, including NIS2, DORA and the AI Act, in practice has been inadequate, particularly with regard to their economic impacts and the management of compliance.

Moreover, a discernible absence of research exists that systematically links cybersecurity, economic models and organisational management. This gap in the extant literature limits the capacity to predict the impact of cyber incidents on the economy, value chains and market stability.

The objectives of this monothematic issue are therefore to:

- i. Enhance comprehension of the socio-technical character of cyber risks;
- ii. Provide support for research endeavours that establish a linkage between technical, managerial and economic aspects;
- iii. Contribute to the creation of frameworks, methodologies, and decision-making models that will help increase the resilience of organisations and strengthen digital trust.

Aim of the Monothematic Issue and Topics

This monothematic issue focuses on a broad spectrum of research perspectives on cybersecurity and digital resilience. We welcome contributions from the fields of IT/IS, economics, management, public administration, law, and behavioral sciences. We expect original empirical studies, theoretical articles, case studies, and review papers.

Welcome topics include, but are not limited to:

Technologies, systems, and threats:

- Next-generation cyberattacks (AI-driven threats, deepfake-based frauds);
- Resilience & incident response in hybrid and multicloud environments;
- IoT and OT security in critical infrastructure;
- Zero Trust security architectures.

Economic and managerial perspectives:

- Economic impacts of cyber incidents;
- ROI and cost-benefit analyses in cybersecurity;
- Risk management, governance, and cyber culture in organizations;
- Behavioral cybersecurity (human factor, decision-making, awareness).

Regulation, compliance, and policy:

- Impacts of NIS2, DORA, GDPR, and AI Act on organizations;
- Cybersecurity in public administration and e-government;
- Standardization, audits, and measurement of cybersecurity levels.

Digital trust and society:

- Digital identity, privacy, and data protection;
- Ethics in cybersecurity;
- Trust in digital services and the trust economy;
- The role of education and the academic sector in strengthening cybersecurity.

References

- Aarland, M. (2025). Cybersecurity in digital supply chains in the procurement process: Introducing the digital supply chain management framework. *Information & Computer Security*, 33(1), 5–24. <https://doi.org/10.1108/ics-10-2023-0198>
- Aiche, A., Winer, Z., & Cohen, G. (2024). Constructing cybersecurity stocks portfolio using AI. *Forecasting*, 6(4), 1065–1077. <https://doi.org/10.3390/forecast6040053>
- Castiglione, G., Santamaria, D. F., Bella, G., Brisindi, L., & Puccia, G. (2025). Guiding cybersecurity compliance: An ontology for the NIS 2 Directive. *Computers & Security*, 157, 104617. <https://doi.org/10.1016/j.cose.2025.104617>
- Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, 13(2), C1–C9. <https://doi.org/10.2308/ciia-52419>

Ji, F., Zhou, Y., Zhang, H., Cheng, G., & Luo, Q. (2025). Navigating the digital odyssey: AI-driven business models in Industry 4.0. *Journal of the Knowledge Economy*, 16(1), 5714–5757. <https://doi.org/10.1007/s13132-024-02096-4>

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In *Cyber resilience of systems and networks* (pp. 1–25). Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3_1

Mahmood, S., Chadhar, M., & Firmin, S. (2024). Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector. *Journal of Contingencies and Crisis Management*, 32(1), e12549. <https://doi.org/10.1111/1468-5973.12549>

Schreiber, A., & Schreiber, I. (2025). AI for cyber-security risk: Harnessing AI for automatic generation of company-specific cybersecurity risk profiles. *Information & Computer Security*, 33(4), 520–546. <https://doi.org/10.1108/ics-08-2024-0177>

Senarak, C. (2025). Toward sustainability and digital resilience: A circular economy cybersecurity framework for seaports. *Cleaner Logistics and Supply Chain*, 15, 100220. <https://doi.org/10.1016/j.clscn.2025.100220>

Teichmann, F. M. J. (2026). Platform governance under NIS2 and the Cyber Resilience Act: Cybersecurity by design as social practice. *Information, Communication & Society*, 1–14. <https://doi.org/10.1080/1369118x.2025.2609780>

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, 23(3), 1695–1719. <https://doi.org/10.1007/s10207-023-00811-x>

Yu, J., Shvetsov, A. V., & Hamood Alsamhi, S. (2024). Leveraging machine learning for cybersecurity resilience in Industry 4.0: Challenges and future directions. *IEEE Access*, 12, 159579–159596. <https://doi.org/10.1109/access.2024.3482987>

Editors' biography



Josef Horálek (Associate Professor)

Faculty of Informatics and Management, University of Hradec Králové (Czech Republic)

(email: josef.horalek@uhk.cz)

Risk management, industrial system security, AI security, cybersecurity management



Filip Holík (Associate Professor)

Department of Information Security and Communication Technology, Norwegian University of Science and Technology (Norway)

(email: filip.holik@ntnu.no)

Cybersecurity, communication networks, programmable data plane, smart grid, industrial networks