DOI: https://doi.org/10.32782/2524-0072/2025-77-60

UDC 658

RECOMMENDATIONS FOR THE DEVELOPMENT OF A STRATEGIC FRAMEWORK FOR MANAGING DIGITAL TRANSFORMATION WITH CONSIDERATION OF CYBERSECURITY AT MANUFACTURING ENTERPRISES

РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБКИ СТРАТЕГІЧНОГО ФРЕЙМВОРКУ ДЛЯ УПРАВЛІННЯ ЦИФРОВОЮ ТРАНСФОРМАЦІЄЮ З УРАХУВАННЯМ КІБЕРБЕЗПЕКИ НА ВИРОБНИЧИХ ПІДПРИЄМСТВАХ

Mazorenko Oksana
Candidate of Sciences (Economic),
Associate Professor Management, Business and Administration Department,
Simon Kuznets Kharkiv National University of Economics
ORCID: https://orcid.org/0000-0003-1784-697X

Herman Yaroslav
Master Student,
Simon Kuznets Kharkiv National University of Economics
ORCID: https://orcid.org/0009-0009-2593-1278

Мазоренко Оксана Володимирівна, Герман Ярослав Євгенович
Харківський національний економічний університет імені Семена Кузнеця

The increasing digitalization of industry requires a forward-looking strategic management approach, with cybersecurity as a core concern. This paper examines theoretical foundations and mechanisms for managing digital transformation in manufacturing, integrating cybersecurity at every stage. A holistic framework is proposed, treating cybersecurity as an enabler of innovation. The study synthesizes literature and modeling, linking BPM, CMM, and socio-technical theory to align technology with secure practices. Key transformation archetypes are analyzed for compatibility with cybersecurity. A comparative analysis shows how neglecting security undermines long-term results. An industry case illustrates prevention of cyber risks. Findings provide guidance for enterprises to achieve resilience and competitiveness through secure digital transformation.

Keywords: digital transformation, cybersecurity, strategic management, business process management, capability maturity model, manufacturing.

Зростаюча цифровізація промислового середовища зумовлює необхідність комплексного та орієнтованого на перспективу підходу до стратегічного управління, особливо враховуючи те, що кібербезпека стає центральним аспектом ініціатив цифрової трансформації. Ця стаття відповідає на цю потребу шляхом дослідження теоретичних засад і стратегічних механізмів, необхідних для управління цифровою трансформацією виробничих підприємств із інтегрованими заходами кібербезпеки на всіх етапах. Ми пропонуємо цілісну концептуальну рамку, яка розглядає кібербезпеку не як зовнішній додаток, а як ключовий рушій цифрових інновацій. Методологічно дослідження ґрунтується на синтезі наявної літератури та концептуальному моделюванні, поєднуючи підходи управління бізнес-процесами (BPM), моделей зрілості можливостей (CMM) та соціотехнічної теорії систем для узгодження технологічного прогресу з надійними практиками безпеки. Визначено ключові стратегічні архетипи цифрової трансформації та проаналізовано їхню сумісність з інтеграцією кібербезпеки, що забезпечує врахування моделями організаційних змін еволюційних ландшафтів загроз і вимог до стійкості. Крім того, стаття пропонує порівняльний аналіз підходів до трансформації, демонструючи, як стратегії, що нехтують заходами безпеки, можуть підірвати довгострокові

результати. Для підтвердження практичної значущості запропонованої рамки наведено приклад галузевого сценарію, який ілюструє, як інтегрований підхід дозволяє запобігати кіберризикам у процесі цифрової модернізації виробництва. Результати дослідження надають практичні рекомендації та орієнтири для виробничих підприємств, що прагнуть досягти операційної стійкості та конкурентних переваг завдяки безпечній цифровій трансформації, тим самим заповнюючи суттєву прогалину в сучасній літературі зі стратегічного менеджменту. Для практиків робота пропонує необхідну дорожню карту одночасного впровадження інновацій та управління ризиками, а для академічного середовища вона закладає підґрунтя для майбутніх досліджень інтегративних цифрових стратегій.

Ключові слова: цифрова трансформація, кібербезпека, стратегічне управління, управління бізнес-процесами, модель зрілості можливостей, виробництво.

Statement of the problem. Manufacturing enterprises today are compelled to adopt digital transformation strategies to sustain competitiveness, enhance operational efficiency, and meet global technological standards. However, digital transformation is not a purely technological endeavor; it requires fundamental changes in business processes, decision-making structures, and organizational culture. The integration of advanced technologies (cloud computing, AI, IoT, etc.) offers unprecedented opportunities for process optimization and innovation, especially in manufacturing where efficiency and adaptability are vital. At the same time, greater digitalization introduces significant risks in terms of cybersecurity. The more interconnected and digitized an enterprise becomes, the more exposed it is to cyber threats ranging from data breaches to operational sabotage.

This duality – opportunity through digital innovation versus vulnerability through cyber-exposure – poses a strategic dilemma. Leadership must ensure that the benefits of digital transformation are not undermined by cyber threats. Strategic management of digital initiatives must therefore embed robust cybersecurity measures from the outset, rather than treating security as an afterthought. Failure to integrate security at a strategic level can negate the gains of digital transformation or even result in catastrophic disruptions.

Traditional management models built on hierarchical control, siloed functions, and slow change are misaligned with the demands of digital ecosystems. Digital ecosystems require agility, cross-functional collaboration, real-time data integration, and resilience against cyber-attacks. Some scholars highlight that digital enterprises increasingly function as decentralized markets, requiring flexible governance and security structures [6]. There is a pressing need for revised strategic frameworks that reconcile the complexity of digital transformation with the rigor of cybersecurity. Unfortunately, many manufacturing firms still treat digital transformation and cybersecurity as separate initiatives, leading to inconsistent implementation, redundant investments, and exposed vulnerabilities. This fragmentation highlights a critical gap in strategic management literature: the lack of a holistic approach to managing digital transformation with embedded cybersecurity.

Moreover, the integration of cybersecurity must consider evolving geopolitical and regulatory environments. Hybrid threats, cross-border data flows, and regulatory asymmetries demand anticipatory security postures rather than reactive fixes. For example, enterprises operating under extraordinary conditions like martial law or political instability face non-negotiable requirements for operational continuity and data sovereignty. Cybersecurity is especially critical in such environments, where sustained operations amidst conflict depend on resilient digital systems. In these contexts, aligning cybersecurity with enterprise-wide digital initiatives is not merely advisable but essential for systemic resilience.

Analysis of recent research and publications. Digital transformation has garnered substantial scholarly and practical attention over the past decade. Problems of digital transformation and integrated cybersecurity have been studied by Möller D.P.F. [4], Fischer M. [3], Kane G. C. [7], Saarikko T., Westergren U. H., Blomquist T. [17], Koch M., Illemann K. [8], Saeed S. [18], Benjamin L. B. [1], Lastauskaite A. [11], among others [9; 19]. Several of these contributions are indexed in Scopus, such as the works of Saarikko et al [17], Fischer et al. [3], and Saeed et al. [18], which provide peer-reviewed, high-impact perspectives on the intersection of digital transformation and cybersecurity. International organizations also emphasize security risk management as a foundation for digital prosperity [2].

Taken together, these studies provide important insights into different aspects of this

problem. Researchers consistently emphasize that digital transformation must be managed with a dual focus on innovation and security to ensure resilient outcomes in the manufacturing context.

For example, Möller [4] analyzed the integration of cyber-physical technologies into industrial systems and demonstrated how digital transformation increases exposure to cyber threats. Kane et al. [7] argued that strategy, rather than technology alone, drives digital transformation, thereby underscoring the importance of management-driven approaches. Saarikko, Westergren, and Blomquist [17] proposed several strategic recommendations for effective digital transformation, such as collaboration, standardization, and responsible data governance, which implicitly contribute to stronger cybersecurity. Fischer et al. [3] emphasized the role of Business Process Management (BPM) in redesigning processes during transformation and identified three strategy archetypes that organizations may adopt, which can be adapted to integrate security considerations.

Koch, Illemann, and Riddarvinge [8] advanced this discussion by developing a socio-technical approach to secure digital transformation, recommending maturity models and SWOT/TOWS analysis to assess risks and shape strategies. More recently, Saeed et al. [18] proposed a cybersecurity readiness framework consisting of four maturity levels to help organizations strengthen their security posture throughout transformation. Similarly, Benjamin et al. [1] identified the main cybersecurity threats that small and medium-sized enterprises face during digitalization, such as phishing, malware, and data breaches. In parallel, Kraus et al. [9] and Sandhu K. [19] emphasized the balance between transformation speed and cybersecurity measures, illustrating the risks of neglecting resilience in pursuit of rapid innovation.

Highlighting previously unresolved parts of the overall problem. Despite these valuable contributions, the literature still reveals a critical gap: existing studies often address digital transformation and cybersecurity separately, or only superficially connect them. Few works offer a consolidated strategic framework that helps manufacturing enterprises concurrently manage digital growth and cybersecurity risks as an integrated program. This gap highlights the need for frameworks that treat cybersecurity not as a reactive add-on, but as a fundamental enabler of digital transformation in industrial contexts. Addressing this gap is the objective of the present study.

This research addresses that gap by synthesizing insights from digital transformation and cybersecurity literature into a unified strategic management framework. In doing so, it responds to calls for approaches that consider technological, organizational, and human factors concurrently. Enterprises stand to benefit from a strategy that treats cybersecurity not as a separate technical silo, but as an intrinsic enabler of digital transformation.

Formation of the objectives of the article (task statement). The aim of the article is to analyze digital transformation processes in manufacturing enterprises, determine the requirements for cybersecurity integration at all stages, and use strategic tools (BPM, CMM, socio-technical approach) to develop a holistic framework for secure digital modernization.

Summary of the main research material. Developing a strategic framework for secure digital transformation necessitates a layered conceptual foundation. At its core, digital transformation in manufacturing can be understood along multiple dimensions: the digitization of processes, the digitalization of business models, and the organizational capacity to sustain these shifts [13]. Cybersecurity, in this context, must be treated not as an external add-on but as an intrinsic component woven through all these dimensions. Evidence from manufacturing demonstrates that secure digital transformation directly improves firm performance [24].

Business Process Management (BPM) provides a structural basis for guiding integration. BPM emphasizes aligning an organization's strategy, processes, technologies, and people towards continuous improvement [16]. Table 1 outlines how cybersecurity considerations map onto each core element of BPM.

By explicitly addressing each BPM element, enterprises can ensure that security is built into the fabric of their process transformations. For instance, strategic alignment means that when formulating digital objectives (like implementing predictive maintenance or cloud-based MES), leadership also defines acceptable cyber risk levels and mitigation plans [9]. In terms of governance, new digital initiatives might require appointing cybersecurity champions in each department or updating policies to reflect digital workflows.

Complementing BPM, the Capability Maturity Model (CMM) provides a diagnostic lens to assess and guide progress.

Table 1

BPM Integration

BPM Element	Cybersecurity Integration Aspect
Strategic Alignment	Incorporation of cyber risk management into strategic goal formulation.
Governance	Clear definition of roles and responsibilities for security oversight.
Methods	Embedding secure process design principles and threat modeling techniques.
Information Technology	Secure IT architecture design, strict access controls, and continuous network monitoring.
People	Training programs and skill development in cyber hygiene and awareness for employees.
Culture	Cultivation of shared security values and norms (a “security-first” mindset).

Source: adapted by the authors based on comparative insights in Fischer et al. [3]

Organizations can evaluate their maturity across several domains – technical, procedural, cultural – and identify gaps inhibiting a secure digital transformation. Table 2 summarizes a tailored cybersecurity maturity model.

Using such a maturity model, a manufacturing firm can determine, for example, that it is currently at Level 2 (having some controls like firewalls and antivirus, but lacking full integration). This insight then guides the firm to Level 3 (Defined) by developing formal security policies, or to Level 4 (Managed) by implementing security analytics and incident response drills. The maturity progression ensures that as the company digitizes its operations, its security capabilities evolve in tandem, reducing the risk of a gap between what the technology enables and what the organization can protect [5].

Recent studies also note that AI/ML-enhanced cybersecurity solutions play an important role in advancing organizations from basic to optimized maturity levels [22]. Practical assessments of enterprise cybersecurity systems also confirm the need to align technical maturity with organizational risk management [10].

Strategic archetypes add another layer of refinement by mapping out organizational pathways for transformation. For instance, Fischer et al. [3] identify several archetypes:

– The communication/learning archetype encourages distributed innovation and continuous learning. In applying this to secure transformation, it would emphasize widespread security awareness and peer learning networks to disseminate cybersecurity knowledge along with digital skills.

– The unification/optimization archetype seeks standardized, efficient processes enterprise-wide. This naturally aligns with uniform security controls – e.g., a single identity management system across all digital platforms, or a centralized security operations center (SOC) monitoring all facilities.

– The certification/automation archetype values control, precision, and compliance. It might resonate with manufacturers in highly regulated sectors. Here, rigorous compliance with standards (ISO 27001, NIST CSF) and extensive use of automated security tools (for threat detection and response) would be key features.

Table 2

Maturity Levels

Maturity Level	Characteristics of Cybersecurity Practice
Level 1: Ad-hoc	Informal, reactive security practices; no defined process.
Level 2: Repeatable	Basic security controls implemented, but integration with business processes is partial.
Level 3: Defined	Documented and standardized security processes organization-wide.
Level 4: Managed	Security effectiveness is monitored and measured; data-driven improvements in place.
Level 5: Optimized	Continuous improvement of security; predictive analytics and threat intelligence actively inform strategy.

Source: adapted by the authors

By analyzing which archetype best fits a given enterprise's goals and culture, the framework can provide tailored guidance. A company focused on agility and innovation might follow the communication/learning archetype, but must institute mechanisms for distributed security (such as empowering local units to handle certain security tasks and share threat information). Conversely, a company driven by standardization might implement enterprise-wide cybersecurity solutions in lockstep with process optimization initiatives.

Using these structured models (BPM, CMM, archetypes), we developed a comprehensive framework for secure digital transformation. In practice, this framework guides managers to concurrently consider how a given digital initiative (say, deploying IoT sensors on the shop floor) affects business processes and what new vulnerabilities it introduces – and then to address those vulnerabilities through both technical controls and workforce preparation.

A pivotal aspect of successful transformation is organizational change management, especially given the human factor in cybersecurity. No matter how advanced the technical safeguards, their effectiveness relies on consistent, informed behavior across the organization. Thus, managing the human side of change is critical.

First, leadership must articulate a compelling vision that balances efficiency/innovation with resilience/security. This vision should be clearly communicated: employees need to hear not just about new digital tools improving production, but also how these tools will be secured and why that matters for the company's survival and reputation [3]. By framing cybersecurity as an integral part of being a modern, digitally-driven manufacturer (and not as a hindrance), leaders can foster buy-in.

Second, workforce development is essential. Employees at all levels must be trained in both the operation of new digital systems and the corresponding security protocols. For example, if a new analytics dashboard is introduced for machine data, employees should be trained on using it and on properly handling the sensitive data it contains (access restrictions, reporting anomalies, etc.). Cyber awareness programs need to go beyond occasional compliance checklists; they should encourage a proactive security culture where employees feel personally responsible for safeguarding assets. This might involve regular phishing simulation exercises, recognition for employees who report security issues, and integrating security topics into daily shift briefings.

Third, cross-functional collaboration should be institutionalized. Digital transformation projects in manufacturing often span multiple departments (IT, production, maintenance, quality, etc.), each with its own legacy systems and priorities. Without deliberate coordination, security can fall through the cracks (e.g., an OT engineer might assume IT is handling network security, while IT assumes OT systems are isolated). Establishing a transformation steering committee, as mentioned, with representatives from all key areas, ensures that issues are raised and addressed collectively. This body can also resolve conflicts (such as when a security measure might initially slow down a production process) by finding acceptable trade-offs or alternative solutions. Such participatory governance models have been shown to significantly reduce resistance and miscommunication [12].

Finally, organizations must address resistance to change, which often stems from fear of the unknown or concerns about job security. Inclusion and transparency are key: involving employees early in the design of new digital workflows or in pilot projects gives them a sense of ownership. When people understand why a change is happening and have input into how it's implemented, they are far more likely to embrace it. For instance, inviting a group of machine operators to help select a new tablet interface for shop-floor data entry (and discussing security features like user authentication with them) turns potential skeptics into change champions. From a socio-technical viewpoint, balancing structural change with human adaptability means designing systems that are not only technically robust but also user-friendly and empowering for staff [8; 21].

To contextualize the importance of integrating cybersecurity, consider three broad approaches to digital transformation in manufacturing, compared in the table below.

In the traditional model, companies pursue digital projects mainly for cost reduction or automation benefits, and cybersecurity is often bolted on later. The organization might see quick efficiency gains, but because security wasn't built-in, they remain vulnerable – a successful cyber-attack could disrupt operations and erase those gains.

In a technology-centric but security-light model, firms push rapid digital adoption (e.g. moving quickly to cloud, IoT, etc.) and apply only

Table 3

Comparison of Digital Transformation Approaches

Feature	Traditional DT	DT with Minimal Security	Secure Integrated DT
Focus	Efficiency and automation	Speed and innovation	Resilience and adaptability
Cybersecurity Integration	Post-implementation (afterthought)	Superficial or siloed (patchy)	Embedded and systemic (by design)
Risk Management	Reactive (firefighting)	Isolated technical fixes	Proactive and strategic
Organizational Culture	Technological optimism (assumes technology will fix itself)	Compliance-driven (security seen as checkbox)	Security-aware and adaptive (continuous learning)
Employee Engagement	Low to moderate (top-down change)	Task-specific training only	Cross-functional and aligned (everyone involved)
Long-term Sustainability	Moderate (improvement plateaus)	Low (vulnerabilities undermine gains)	High (robust, resilient growth)

Source: developed by the authors

minimal security (perhaps installing antivirus and basic encryption). This approach can create a false sense of innovation: things move faster initially, but hidden security gaps (like unpatched IoT devices or misconfigured cloud servers) accumulate as technical debt. Studies on SMEs undergoing fast digitalization show that neglecting security often leads to breaches that cost far more than the initial digital investments [1]. In other words, such firms may achieve short-term innovation but at the expense of long-term viability.

By contrast, a secure integrated approach treats cybersecurity as a core component of transformation. Every initiative is evaluated for risk alongside benefits. While this approach might seem to slow down projects slightly (due to risk assessments, security testing, etc.), it pays off through higher sustainability. The company is better protected against downtime, data loss, and compliance penalties, thereby safeguarding the value created by digital innovation. This approach aligns with the idea that trust (from customers, partners, stakeholders) becomes a strategic differentiator – being able to confidently say your smart factory is secure can be a market advantage.

The comparative analysis underscores that only the integrated approach truly balances innovation with protection. Traditional models emphasizing solely efficiency may overlook modern threat realities. And speed-driven transformations without adequate security often incur high costs later, whether through breaches or the massive effort required to retrofit security into complex systems [19]. In the secure integrated model, security enables innovation by ensuring that new technologies can be deployed without inviting disaster.

To illustrate the framework in action, consider a mid-sized manufacturing enterprise implementing a cloud-based Manufacturing Execution System (MES) integrated with IoT sensors across its production line:

– Under a traditional approach, management might focus on throughput gains and wide sensor coverage. The MES and sensors get deployed quickly, improving data collection and productivity. However, little attention is given to security during design. Perhaps only after deployment do they realize the IoT devices were installed with default passwords or that the MES's API endpoints are exposed to the internet without proper authentication. This leaves the system vulnerable to attackers who could disrupt production or exfiltrate sensitive data.

– Under a technology-centric/minimal security approach, the company might be somewhat aware of risks and implement basic measures: e.g., they secure data transmission with encryption and use a VPN for remote MES access. These are good steps, but without a centralized oversight or incident response plan they are insufficient [15]. Moreover, the adoption of IoT, ML, and AI without systemic cybersecurity introduces sector-specific risks [23]. If an anomaly is detected (say a sensor starts sending strange readings, possibly due to malware), there is no clear procedure to diagnose or contain it. Each team (IT, OT, production) might respond in

isolation, potentially missing the broader threat pattern.

– Applying the secure integrated framework, the enterprise takes a coordinated, multi-departmental approach from the start. Before deployment, cybersecurity teams collaborate with operations engineers to perform a risk assessment on the new MES+IoT system. They identify risks like unauthorized access to sensor data and potential malware infecting the control network. To mitigate these, they define strict access policies (only whitelisted devices and users can connect), segment the network (so sensors are isolated from core IT systems), and embed anomaly detection tools into the MES analytics platform. Recent studies demonstrate that resilient detection at the device level is critical for industrial control environments [14]. They also update governance structures: a cross-functional committee (IT, OT, plant managers, security officers) meets regularly during the rollout to ensure policies are followed and to address issues in real time. Continuous training is conducted – production floor staff are briefed on how to recognize and report phishing emails or suspicious device behavior, since a compromised operator account could be as damaging as malware. Additionally, they require all vendors supplying the IoT devices to adhere to the company's cybersecurity standards (e.g., no hardcoded passwords, regular patch updates), making security an element of supplier contracts.

In this scenario, the outcome is that the enterprise achieves the operational benefits (real-time production monitoring, reduced downtime through predictive maintenance, etc.) and maintains a strong security posture. If a particular IoT sensor starts acting anomalously, the anomaly detection triggers an alert; the incident response playbook (prepared in advance) is executed, isolating that sensor's segment. The team analyzes the issue without needing to shut down the entire production line, minimizing disruption. This contrasts sharply with the other approaches, where either the issue might not be caught at all (traditional), or it causes panic and ad-hoc responses (minimal security approach).

Overall, the scenario demonstrates how operational efficiency and cyber resilience can be achieved concurrently through strategic alignment and organizational synergy. The secure integrated approach might require more upfront planning and cross-team communication, but it pays dividends by preventing costly incidents and building a culture of trust in technology.

Conclusions. The convergence of digital transformation and cybersecurity presents a complex strategic challenge that demands more than just technical solutions. For manufacturing enterprises, it is imperative to cultivate a unified vision in which innovation and protection co-exist as complementary priorities. This paper has shown that such integration is not only feasible but advantageous, through a structured application of BPM principles, CMM diagnostics, and strategic archetype alignment. By embedding cybersecurity considerations across all dimensions of transformation – from governance and methods to people and culture – companies can establish a foundation for resilient growth.

The proposed framework emphasizes that cybersecurity should be viewed as a core enabler of digital transformation rather than an external constraint. Maturity models help organizations benchmark their capabilities and plot a clear roadmap for improvement. Adaptable strategy archetypes provide flexibility, allowing each firm to tailor the integration according to its context (e.g., regulatory environment, market pressure) while still adhering to best practices. In essence, the approach supports both technical efficacy (the digital tools work as intended) and organizational coherence (the whole company is aligned and prepared to secure those tools).

Our findings also reinforce the need for ambidextrous leadership that bridges technological innovation with risk governance. Leaders overseeing digital transformation must evaluate new technologies not only for operational benefits, but also through the lens of cyber resilience, regulatory compliance, and stakeholder trust. Recent scholarship on digital leadership underlines that such dual-competency leadership is a decisive factor in sustaining transformation in volatile, interconnected environments. In practice, this might mean CIOs and CISOs working hand-in-hand, or even developing hybrid roles (e.g., a Chief Digital Security Officer) that ensure security strategy is developed in tandem with digital strategy.

Looking ahead, future research should explore sector-specific adaptations of this framework. Different manufacturing sub-sectors (automotive, pharmaceuticals, electronics, etc.) have unique process requirements and threat profiles that may require tailored controls or emphasize certain framework components over

others. Empirical validation is another crucial step: conducting case studies or longitudinal surveys on manufacturers who pursue integrated strategies could yield insights into best implementation practices and common pitfalls.

Additionally, emerging technologies open new frontiers for both digital innovation and cybersecurity. Developments in AI-driven threat anticipation, such as machine learning models that predict cyber-attacks before they occur, could be integrated into the strategic framework to enhance proactive defense. Similarly, as quantum computing looms on the horizon, quantum-safe cybersecurity standards will become important to protect encrypted data in digital manufacturing systems. Research on how to incorporate these cutting-edge solutions into a cohesive transformation strategy will be invaluable.

In conclusion, the strategic management of digital transformation with integrated cybersecurity is both a necessity and an opportunity. It is a necessity because modern manufacturers face sophisticated threats that can derail digital progress if ignored. It is an opportunity because those firms that successfully marry innovation with security can achieve a competitive edge – they operate efficiently, adapt quickly, and maintain the trust of customers and partners in a world where trust is paramount. By following a holistic framework as outlined in this paper, manufacturing enterprises can confidently navigate their digital journeys, knowing that resilience underpins every step of innovation.

REFERENCES:

1. Benjamin L. B. et al. Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, 2024, vol. 19, no. 2, pp. 134–153. DOI: https://doi.org/10.30574/gjeta.2024.19.2.0084 (accessed August 11, 2025).

2. Companion Document to the OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. *Digital Security Risk Management for Economic and Social Prosperity*, 2015, pp. 17–69. DOI: https://doi.org/10.1787/9789264245471-2-en (accessed June 02, 2025).

3. Fischer M. et al. Strategy archetypes for digital transformation: Defining meta objectives using business process management. *Information & Management*, 2020, vol. 57, no. 5, p. 103262. DOI: https://doi.org/10.1016/j.im.2019.103262 (accessed December 11, 2024).

4. Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. Springer, 2023. DOI: https://doi.org/10.1007/978-3-031-26845-8 (accessed August 15, 2025).

5. Humphrey W. S. Characterizing the software process: a maturity framework. *IEEE Software*, 1988, vol. 5, no. 2, pp. 73–79. DOI: https://doi.org/10.1109/52.2014 (accessed July 02, 2025).

6. Is Your Company Ready to Operate as a Market? *What the Digital Future Holds*, 2018. DOI: https://doi.org/10.7551/mitpress/11645.003.0011 (accessed August 02, 2025).

7. Kane G. C., Palmer D., Phillips A. N., Kiron D., Buckley N. Strategy, not technology, drives digital transformation. *MIT Sloan Management Review*, 2015. Available at: https://sloanreview.mit.edu/projects/strategy-drives-digital-transformation/ (accessed December 24, 2024).

8. Koch M., Illemann K., Riddarvinge D. Strategic Planning for Secure Digital Transformation: A Socio-Technical Approach. *Proceedings of the 5th International Workshop on Socio-Technical Perspective in IS Development (STPIS 2019) co-located with 27th European Conference on Information Systems (ECIS 2019)*, Stockholm, Sweden, June 10, 2019, pp. 34–41. Available at: https://www.semanticscholar.org/paper/Strategic-Planning-for-Secure-Digital-A-Approach-Koch-Illemann/b7d01150bc57e660e84bd7facf1fa7896595e5c8 (accessed August 11, 2025).

9. Kraus K., Kraus N., Shtepa O. Digital Transformation of Cyber Security at the Micro-Level under Martial Status. *Innovation and Sustainability*, 2022, pp. 26–37. DOI: https://doi.org/10.31649/ins.2022.3.26.37 (accessed June 11, 2025).

10. Kuzior A. et al. Company Cybersecurity System: Assessment, Risks and Expectations. *Production Engineering Archives*, 2023, vol. 29, no. 4, pp. 379–392. DOI: https://doi.org/10.30657/pea.2023.29.43 (accessed August 11, 2025).

11. Lastauskaite A., Krusinskas R. Digitalization and Productivity: Evidence from EU Manufacturing Sector. *European Journal of Economics*, 2023, vol. 3, no. 1, pp. 1–12. DOI: https://doi.org/10.33422/eje.v3i1.275 (accessed May 21, 2025).

12. Lazazzara A., Ricciardi F., Za S. Exploring Digital Ecosystems: Organizational and Human Challenges. Springer, 2020, 472 p. DOI: https://doi.org/10.1007/978-3-030-23665-6 (accessed August 15, 2025).

13. Mayhuasca J., Sotelo S. Quantum Technologies for Digital Transformation and Informatica Security. *International Journal of Engineering Sciences*, 2022, vol. 15, no. 2. DOI: https://doi.org/10.36224/ijes.150201 (accessed August 21, 2025).

14. Meeran Y. A., Shyry S. P. Resilient Detection of Cyber Attacks in Industrial Devices. *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 11–13 April 2023. 2023. DOI: https://doi.org/10.1109/icoei56765.2023.10125932 (accessed July 21, 2025).

15. Raimundo R. J., Rosário A. T. Cybersecurity in the Internet of Things in Industrial Management. *Applied Sciences*, 2022, vol. 12, no. 3, p. 1598. DOI: https://doi.org/10.3390/app12031598 (accessed July 11, 2025).

16. Rosemann M., vom Brocke J. The Six Core Elements of Business Process Management. *Handbook on Business Process Management 1*, Berlin, Heidelberg, 2014, pp. 105–122. DOI: https://doi.org/10.1007/978-3-642-45100-3_5 (accessed August 25, 2025).

17. Saarikko T., Westergren U. H., Blomquist T. Digital transformation: Five recommendations for the digitally conscious firm. *Business Horizons*, 2020, vol. 63, no. 6, pp. 825–839. DOI: https://doi.org/10.1016/j.bushor.2020.07.005 (accessed June 11, 2025).

18. Saeed S. et al. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, 2023, vol. 23, no. 15, p. 6666. DOI: https://doi.org/10.3390/s23156666 (accessed June 11, 2025).

19. Sandhu K. Advancing Cybersecurity for Digital Transformation: Opportunities and Challenges. IGI Global, 2021. DOI: https://doi.org/10.4018/978-1-7998-6975-7.ch001 (accessed August 24, 2025).

20. Shveda N. et al. Digital transformation as an imperative for innovative development of business processes under martial law (Ukrainian experience). *Economics of Development*, 2024, vol. 23, no. 2, pp. 69–79. DOI: https://doi.org/10.57111/econ/2.2024.69 (accessed July 24, 2025).

21. Suharto. Challenges and Opportunities of Digital Transformation in Strategy Management. *International Journal of Science and Society*, 2024, vol. 6, no. 1, pp. 620–630. DOI: https://doi.org/10.54783/ijsoc.v6i1.1050 (accessed June 24, 2025).

22. Sundaram K. T. Digital Transformation with AI/ML & Cybersecurity. *International Journal of Computer Science and Mobile Computing*, 2022, vol. 11, no. 11, pp. 1–3. DOI: https://doi.org/10.47760/ijcsmc.2022.v11i11.001 (accessed July 11, 2025).

23. Trung N. D., Huy D. T. N., Le T.-H. IoTs, Machine Learning (ML), AI and Digital Transformation Affects Various Industries – Principles and Cybersecurity Risks Solutions. *Webology*, 2021, vol. 18, Special Issue 04, pp. 501–513. DOI: https://doi.org/10.14704/web/v18si04/web18144 (accessed June 23, 2025).

24. Yu X. The Impact of Digital Transformation on Manufacturing Firm Performance. *Frontiers in Business, Economics and Management*, 2023, vol. 11, no. 1, pp. 117–121. DOI: https://doi.org/10.54097/fbem.v11i1.11825 (accessed July 21, 2025).