

Institute of Management  
Faculty of Security, Logistics and Management  
Military University of Technology in Warsaw

Instytut Zarządzania  
Wydział Bezpieczeństwa, Logistyki i Zarządzania  
Wojskowa Akademia Techniczna w Warszawie

ISSN 1896-9380 | eISSN 2719-860X

Modern Management Systems  
Volume 21 (2026)  
No. 1 (January-March)  
pp. 41-52

Nowoczesne Systemy Zarządzania  
Zeszyt 21 (2026)  
nr 1 (styczeń-marzec)  
s. 41-52

---

## Cybersecurity management in organizations as a component of modern management systems: Integrating governance, risk, and continuous improvement

### Zarządzanie cyberbezpieczeństwem w organizacjach jako element nowoczesnych systemów zarządzania: integracja tadu korporacyjnego, ryzyka i ciągłego doskonalenia

Izabela Markiewicz<sup>A-F</sup>

University of Warsaw, Poland

izabela.markiewicz001@gmail.com; ORCID: 0009-0006-4697-2296

DOI: 10.37055/nasz/218590

A – Research concept/Koncepcja badania

B – Data collection/Gromadzenie danych

C – Data analysis/Analiza danych

D – Writing the article/Napisanie artykułu

E – Critical revision/Krytyczne zrecenzowanie

F – Final approval/Zatwierdzenie artykułu

Submission/Nadesłano: 28.01.2026

First review/Pierwsza recenzja: 13.02.2026

Second review/Druga recenzja: 20.02.2026

Acceptance/Zaakceptowano: 20.02.2026

Online publication/Opublikowano online: 28.02.2026

Publication/Opublikowano: 28.02.2026

---

#### Abstract:

##### *Research objectives and hypothesis/research questions*

The primary objective of this study is to identify the key success factors for embedding digital asset protection within the broader framework of corporate governance. The research is founded on the hypothesis that the effectiveness of digital protection is significantly higher in organizations where cybersecurity is managed as a strategic risk rather than a technical cost.

##### *Research methods*

This study is grounded in Systems Theory and the Socio-Technical Systems (STS) perspective, which views cybersecurity as an interaction between technology, people, and organizational hierarchy. The research procedure was executed in three distinct stages: a systematic review of contemporary literature on the subject, a comparative analysis of international security frameworks (specifically ISO/IEC 27001 and NIST), and the subsequent synthesis of an integrated four-layer management model. The methodology relies on qualitative research methods, specifically qualitative content analysis of academic journals and industry standards. The research instruments utilized include standardized data extraction sheets for thematic coding and the Capability Maturity Model Integration (CMMI) framework to evaluate organizational progress. By employing these qualitative tools, the study identifies the intersection points where technical controls become strategic management assets, ensuring that the resulting model is both theoretically sound and practically applicable to modern organizations.

**Main results**

The research concludes that a lack of executive level engagement and „siloeed” IT structures are the primary barriers to effective defense, leading to the development of a four-layer model that integrates governance, end-to-end processes, performance measurement, and maturity-based continuous improvement.

**Implications for theory and practice**

Theoretically, this study shifts the academic focus from infrastructure protection to cybersecurity governance by treating security decisions as fundamental business resource allocations. Practically, it mandates that organizations integrate digital risk into Enterprise Risk Management frameworks, prioritize cyber resilience over simple prevention, and move away from „paper-based” compliance toward a functional security culture.

**Keywords:**

cybersecurity, corporate governance, risk management, organizational maturity, information security management

**Abstrakt:****Cel badań i hipotezy/pytania badawcze**

Głównym celem badania jest identyfikacja kluczowych czynników sukcesu w zakresie wdrażania ochrony zasobów cyfrowych w szerszych ramach ładu korporacyjnego. Badanie opiera się na hipotezie, że skuteczność ochrony cyfrowej jest znacznie wyższa w organizacjach, w których cyberbezpieczeństwo jest traktowane jako ryzyko strategiczne, a nie koszt techniczny.

**Metody badawcze**

Badanie opiera się na teorii systemów i perspektywie systemów społeczno-technicznych (STS), która postrzega cyberbezpieczeństwo jako interakcję między technologią, ludźmi i hierarchią organizacyjną. Procedura badawcza została przeprowadzona w trzech odrębnych etapach: systematyczny przegląd współczesnej literatury przedmiotu, analiza porównawcza międzynarodowych ram bezpieczeństwa (w szczególności ISO/IEC 27001 i NIST) oraz późniejsza synteza zintegrowanego czterowarstwowego modelu zarządzania. Metodologia opiera się na jakościowych metodach badawczych, a konkretnie na jakościowej analizie treści czasopism naukowych i standardów branżowych. Wykorzystane narzędzia badawcze obejmują standardowe arkusze ekstrakcji danych do kodowania tematycznego oraz ramy zintegrowanego modelu dojrzałości organizacyjnej (*Capability Maturity Model Integration*, CMMI) do oceny postępów organizacyjnych. Dzięki zastosowaniu tych narzędzi jakościowych w badaniu zidentyfikowano punkty przecięcia, w których kontrole techniczne stają się strategicznymi zasobami zarządzania, zapewniając, że powstały model jest zarówno teoretycznie uzasadniony, jak i praktycznie zastosowalny w nowoczesnych organizacjach.

**Główne wyniki**

Badania wykazały, że brak zaangażowania kadry kierowniczej oraz „silosowe” struktury IT stanowią główne przeszkody dla skutecznej ochrony, co doprowadziło do opracowania czteropoziomowego modelu integrującego zarządzanie, kompleksowe procesy, pomiar wydajności oraz ciągłe doskonalenie oparte na dojrzałości.

**Implikacje dla teorii i praktyki**

Teoretycznie badanie to przesuwa akademickie zainteresowanie z ochrony infrastruktury na zarządzanie cyberbezpieczeństwem, traktując decyzje dotyczące bezpieczeństwa jako podstawowe alokacje zasobów biznesowych. W praktyce nakazuje organizacjom integrację ryzyka cyfrowego z ramami zarządzania ryzykiem przedsiębiorstwa (ERM), priorytetowe traktowanie odporności cybernetycznej zamiast prostej prewencji oraz odejście od „papierowej” zgodności na rzecz funkcjonalnej kultury bezpieczeństwa.

**Słowa kluczowe:**

cyberbezpieczeństwo, ład korporacyjny, zarządzanie ryzykiem, dojrzałość organizacyjna, zarządzanie bezpieczeństwem informacji

## **Introduction**

In the digital landscape of 2026, the pervasive nature of cloud technologies and distributed work has transformed cybersecurity from a peripheral IT concern into a cornerstone of modern management systems. This research is justified by the persistent gap between advanced technical safeguards and their lack of integration with strategic business goals, which often results in operational paralysis during cyber incidents. The primary objective of this study is to identify key success factors for embedding digital asset protection within the broader framework of corporate governance. The research strategy addresses whether executive level engagement significantly alters the effectiveness of security protocols and how international standards like ISO/IEC 27001 can bridge the technical managerial divide. It is hypothesized that cybersecurity is fundamentally more effective when managed as a strategic risk rather than a technical cost. This study is constrained by its focus on organizational management structures rather than specific technical algorithms, and its findings are primarily applicable to organizations operating under global digital standards.

### **1. Literature review**

The current state of research, as reflected in databases such as Scopus and Web of Science, demonstrates a significant shift from “infrastructure protection” to “cybersecurity governance”. Key scholars like Von Solms and Van Niekerk (2013) emphasize that in modern systems, security decisions are essentially business decisions regarding resource allocation and risk acceptance. Furthermore, the work of De Haes and Van Grembergen (2009) provides empirical evidence that mature IT governance leads to superior business IT alignment and risk control. From a behavioral perspective, research indexed in ERIH PLUS, such as studies by Siponen (2000) and Bulgurcu, Cavusoglu, Benbasat (2010), highlights the “human factor” as a critical vulnerability that cannot be solved by technology alone, but rather through a robust security culture. An evaluation of this existing body of work reveals that while the theoretical frameworks for governance are well established, many organizations still struggle with “paper-based” compliance. This article contributes to the field by proposing a synthesis that moves beyond formal documentation toward a functional integration of security into daily management processes.

## 2. Research methodology

This study is grounded in Systems Theory and the Socio-Technical Systems (STS) perspective, which views cybersecurity as an interaction between technology, people, and organizational hierarchy. The research procedure was executed in three distinct stages: a systematic review of contemporary literature, a comparative analysis of international security frameworks (specifically ISO/IEC 27001 and NIST), and the subsequent synthesis of an integrated four-layer management model. The methodology relies on qualitative research methods, specifically qualitative content analysis of academic journals and industry standards. The research instruments utilized include standardized data extraction sheets for thematic coding and the Capability Maturity Model Integration (CMMI) framework to evaluate organizational progress. By employing these qualitative tools, the study identifies the intersection points where technical controls become strategic management assets, ensuring that the resulting model is both theoretically sound and practically applicable to modern organizations.

## 3. Cybersecurity as a managerial domain: From “IT problems” to business risk

Historically, information security was often situated within IT departments and defined primarily as the protection of infrastructure. With the growing scale of threats and their consequences, a shift in perspective has occurred: cybersecurity is becoming a component of risk management and corporate governance (Von Solms, Van Niekerk, 2013). This means that security decisions are business decisions (resource allocation, risk acceptance, investment prioritization); cyber risk has a strategic, financial, legal, and reputational dimension; and responsibility for the level of risk cannot be delegated exclusively to technical specialists. From the perspective of management sciences, three dimensions are particularly significant:

- Governance and accountability: clear definition and empowerment of roles (the board, process owners, CISO), policies, risk appetite, as well as oversight and reporting mechanisms (Weill, Ross, 2004; De Haes, Van Grembergen, 2009);
- Behavior and security culture: even the best technical solutions will fail in an organization that is unable to shape employee behavior and minimize human error (Siponen, 2000; Bulgurcu, Cavusoglu, Benbasat, 2010);
- Processes and continuous improvement: cybersecurity constitutes a system of cyclical activities requiring measurement, learning from incidents, and adaptation to technological and business changes.

#### **4. Frameworks and standards in systemic cybersecurity management**

Contemporary approaches to cybersecurity management are grounded in established standards and frameworks that function as a “common language” bridging business, technical, and audit perspectives. In organizational practice, reliance on a single methodology is uncommon; instead, organizations typically adopt hybrid approaches that combine multiple, complementary frameworks. The backbone of such an architecture is most often an Information Security Management System (ISMS) aligned with ISO/IEC 27001. Through the application of the PDCA cycle and systematic risk management, the ISMS enables the development of a coherent and internally consistent hierarchy of policies, roles, and control mechanisms. This foundational structure is further complemented by functional frameworks, which significantly enhance communication and the structuring of concrete operational activities across the entire incident management lifecycle. However, the effectiveness of these mechanisms is contingent upon strong IT governance and corporate oversight. Such governance ensures that cybersecurity considerations are embedded in strategic decision-making, project portfolio management, and compliance assurance processes, rather than treated as isolated technical concerns. The literature consistently emphasizes that the selection of a standard alone does not substitute for active and informed management, but merely provides a formalized structure within which such management can occur. As argued by Dhillon and Backhouse (2001), the ultimate effectiveness of cybersecurity management systems depends on organizational maturity, the capability to accurately assess and measure risk, and the quality of the prevailing security culture. Consequently, the primary challenge lies in integrating formal requirements with day-to-day practices in a manner that avoids the proliferation of parallel, purely “paper-based” systems, and instead supports substantive business decision-making and the reinforcement of desired employee behaviors.

#### **5. Results of the synthesis: A model for integrating cybersecurity into modern management systems**

The outcome of the conceptual synthesis is a four-layer model designed to embed cybersecurity within the organization’s overall management system. The model explicitly supports integration with other management systems, thereby reducing fragmentation and mitigating conflicts of priorities.

### **5.1. Layer I – governance, accountability, and decision-making**

The governance layer addresses fundamental questions concerning decision rights, accountability, acceptable levels of risk, and the mechanisms through which top management oversees cybersecurity. In practice, this layer encompasses:

- The establishment of clear risk ownership, extending beyond IT functions to business lines;
- The definition of risk appetite and tolerance thresholds;
- The allocation of roles and responsibilities (board of directors, risk committee, CISO, process owners, internal audit);
- Oversight mechanisms, including periodic reporting, risk reviews, incident reviews, and the approval of investment plans.

Empirical studies indicate that mature IT governance is positively correlated with improved business performance and more effective risk control (De Haes, Van Grembergen, 2009). From a cybersecurity perspective, it is critical that security-related decisions are embedded in standard management processes, such as strategic planning, budgeting, procurement, and supplier management.

### **5.2. Layer II – end-to-end cybersecurity processes**

The process layer encompasses the full lifecycle of cybersecurity activities and can be described using a functional perspective (identify–protect–detect–respond–recover). To be managerially effective, these processes must be explicitly linked to business processes and assigned process ownership. Exemplary end-to-end processes include:

- Asset management and information classification: identifying what needs to be protected and why;
- Cyber risk management: risk identification, analysis, assessment, and treatment, integrated with enterprise risk management (ERM);
- Vulnerability and configuration management: standardization, patching, and change control;
- Identity and access management (IAM): least privilege, segmentation, and identity controls;
- Monitoring and detection: capabilities for early identification of security events;
- Incident response: defined procedures, roles, exercises, and crisis communication;
- Recovery and resilience: backups, recovery planning, and testing.

The literature highlights that organizations often overinvest in “protection” while underinvesting in “detection” and “response,” which significantly increases the actual cost of incidents (Anderson, Moore, 2006). From a management system perspective, ensuring the internal consistency of these processes and their cyclical effectiveness assessment is essential.

### **5.3. Layer III – measurement, reporting, and control (KPIs and KRIs)**

Modern management systems require metrics that enable control, accountability, and informed decision-making. In the cybersecurity domain, measurement should focus not only on incident counts, but on organizational capabilities and residual risk levels. The proposed categories of metrics include:

- Key Risk Indicators (KRIs): risk-oriented measures such as the proportion of critical vulnerabilities not remediated within defined timeframes, supplier risk exposure levels, or access policy violation rates;
- Key Performance Indicators (KPIs): performance measures including mean time to detect (MTTD) and mean time to respond (MTTR), the percentage of systems covered by monitoring, and the proportion of employees who have completed security training;
- Resilience indicators: results of recovery tests, recovery time objectives (RTO) and recovery point objectives (RPO) for critical services, and the effectiveness of tabletop exercises.

The selection of KPIs and KRIs should be derived from the organization’s defined risk appetite and closely aligned with its overarching strategic objectives. Overly technical metrics hinder executive decision-making, while overly aggregated indicators fail to support process improvement. Research on information security behavior suggests that the effectiveness of security programs increases when objectives are clear, measurable, and linked to managerial accountability (Bulgurcu, Cavusoglu, Benbasat, 2010).

### **5.4. Layer IV – maturity, organizational learning, and continuous improvement**

Continuous improvement constitutes a core principle of modern management systems. In the context of cybersecurity, this entails:

- Periodic reviews of risk levels and control effectiveness;
- Post-incident reviews and systematic implementation of lessons learned;
- Regular testing, including response exercises and recovery tests;
- Capability development through training, phishing simulations, and security awareness programs.

System maturity may be assessed using a multi-level model, ranging from ad hoc activities to fully managed and optimized processes. This perspective is particularly relevant in large and multinational organizations, where individual business units exhibit varying levels of capability. In such contexts, the central security function must effectively manage the organization's overall "maturity portfolio" to ensure consistent risk posture across the group.

Table 1. Conceptual framework for integrating cybersecurity into modern management systems

Layer	Focus & objective	Key components & activities	Strategic alignment & evidence
Layer I: Governance & Accountability	Defining decision rights and the organization's high-level security posture.	<ul style="list-style-type: none"> <li>- Risk ownership (Business lines);</li> <li>- Definition of risk appetite/tolerance;</li> <li>- Role allocation (Board, CISO, Audit);</li> <li>- Oversight &amp; investment approval.</li> </ul>	Links security to strategic planning and budgeting. Mature governance correlates with improved business performance (De Haes, Van Grembergen, 2009).
Layer II: End-to-End Processes	Managing the full lifecycle of security activities integrated with business processes.	<ul style="list-style-type: none"> <li>- ERM-integrated risk management;</li> <li>- Vulnerability &amp; config management;</li> <li>- Detection, Response &amp; Recovery.</li> </ul>	Shifts focus from pure "protection" to "detection/response" to reduce incident costs (Anderson, Moore, 2006).
Layer III: Measurement & Reporting	Utilizing metrics (KPIs/KRIs) to enable control and informed decision-making.	<ul style="list-style-type: none"> <li>- KPIs: MTTD, MTTR, training completion rates;</li> <li>- Resilience: RTO/RPO, recovery test results.</li> </ul>	Effectiveness increases when metrics are clear, measurable, and linked to managerial accountability (Bulgurcu, Cavusoglu, Benbasat, 2010).
Layer IV: Maturity & Improvement	Driving organizational learning and consistent risk posture across the group.	<ul style="list-style-type: none"> <li>- Phishing simulations &amp; awareness;</li> <li>- Capability development;</li> <li>- Management of "maturity portfolios".</li> </ul>	Ensures the system is not static; emphasizes the PDCA (Plan-Do-Check-Act) cycle and manages variance in multinational units.

Source: own elaboration

## **6. Practical implementation implications: Avoiding “paper-based” security**

### **6.1. Integration with ERM and business decision-making**

Cybersecurity acquires genuine managerial relevance when digital risk is fully incorporated into the framework of Enterprise Risk Management (ERM). This process primarily requires the establishment of a clear risk ownership structure, a rigorous assessment of the impact of cyber incidents on strategic objectives, and the adequate budgeting of mitigation activities. From a practical perspective, it is essential to develop an organization-wide risk taxonomy, apply consistent assessment criteria, and closely align cybersecurity procedures with business continuity planning.

### **6.2. People and culture as an “attack vector”**

Incident root-cause analyses consistently indicate that human error, improper habits, and information overload constitute the most frequent sources of security incidents. The literature (Siponen, 2000) highlights the limited effectiveness of security systems based solely on restrictive policies and sanctions. Instead, a holistic approach is advocated, combining role-tailored education with the design of secure processes in accordance with the principle of security by design. Equally important is ensuring the usability of technical mechanisms such as multi-factor authentication and password managers which, when reinforced by positive social norms, enables the durable embedding of security within organizational culture.

### **6.3. Supplier and supply chain risk management**

In an era of globalization and service decentralization, oversight of risks generated by software vendors, cloud service providers, and system integrators has become a critical challenge. An effective management system in this domain should be based on a multi-tier classification of suppliers according to their criticality to business processes, complemented by precise contractual provisions governing security-related SLAs, incident reporting obligations, and audit rights. These measures should be reinforced by periodic risk assessments and assurance testing, as well as the development of exit plans in the event that a supplier no longer meets established trust requirements.

#### **6.4. From “protection” to cyber resilience**

Contemporary management paradigms are evolving from attempts to achieve complete prevention toward the development of cyber resilience, understood as the capability to effectively detect, respond to, and recover from incidents. Implementing this approach requires directing investments toward advanced monitoring and telemetry, strengthening incident response team capabilities, and conducting regular simulation exercises. Equally important are the technical foundations of continuity such as network segmentation and robust backup systems supported by professionally designed crisis communication mechanisms that help mitigate reputational damage following an incident.

### **7. Discussion: Global dimension and future directions**

The global nature of cyber threats compels organizations to operate within complex and heterogeneous regulatory, cultural, and technological contexts. In practice, this is reflected in the need to harmonize minimum security standards across legal jurisdictions and to rigorously manage data flows in response to divergent privacy requirements. A significant challenge remains the mitigation of disparities in operational maturity across organizational units and suppliers, while simultaneously adapting to the growing importance of industry standards, certifications, and customer-specific security requirements.

Looking ahead, at least three dominant trends can be identified in the evolution of cybersecurity management. The first concerns the increasing convergence of cybersecurity with operational risk management, resulting in greater emphasis on scenario-based risk analysis and business continuity assurance. The second trend involves the automation and orchestration of security processes through advanced tools that enhance the scalability of detection and incident response, albeit accompanied by inherent risks associated with automation failures. The third key trend is the integration of security directly into the digital service development and delivery lifecycle commonly referred to as the DevSecOps paradigm which enables the relocation of selected governance controls into development processes, ensuring protection from the design stage onward.

## **Conclusions**

The primary objective of this study, which sought to identify the key success factors for embedding digital asset protection within the framework of corporate governance, has been achieved through the synthesis of the proposed four-layer

management model. Based on the conducted research and the comparative analysis of international standards, the findings allow for the positive verification of the research hypothesis, confirming that the effectiveness of digital protection is significantly higher in organizations where cybersecurity is managed as a strategic risk rather than a technical cost. The study demonstrates that when cybersecurity is elevated to a governance-level priority, it ceases to be a collection of reactive measures and becomes a proactive component of organizational resilience. The verification of this hypothesis reveals that the durable embedding of security within management structures specifically through the clear definition of risk ownership and direct reporting to executive boards is the most critical factor for success. Furthermore, the research concludes that cybersecurity must be understood as a socio-technical system where technology serves as a necessary but insufficient condition for effectiveness. A coherent management system must therefore be founded on precisely defined KPIs and KRIs that support strategic decision-making and enable continuous adaptation to the global threat landscape. This shift in perspective from a siloed IT concern to an integrated business process allows organizations to move beyond mere prevention toward a state of true cyber resilience. The primary limitation of this study lies in its conceptual nature, meaning the proposed model requires further empirical validation across diverse operational profiles. Consequently, future research should focus on the development of industry-specific metric sets and longitudinal analyses to determine the exact correlation between cybersecurity maturity, organizational culture, and ultimate business performance.

---

#### REFERENCES

- [1] ANDERSON, R., MOORE, T., 2006. The economics of information security, *Science*, No. 314 (5799), pp. 610-613.
- [2] BULGURCU, B., CAVUSOGLU, H., BENBASAT, I., 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly*, No. 34 (3), pp. 523-548.
- [3] DE HAES, S., VAN GREMBERGEN, W., 2009. An exploratory study into IT governance implementations and its impact on business/IT align, *Computers & Security*, No. 31 (1), pp. 83-95.
- [4] DHILLON, G., BACKHOUSE, J., 2001. Current directions in IS security research: Towards socio-organizational perspectives, *Information Systems Journal*, No. 11 (2), pp. 127-153.
- [5] SIPONEN, M., 2000. A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, No. 8 (1), pp. 31-41.
- [6] VON SOLMS, R., VAN NIEKERK, J., 2013. From information security to cyber security, *Computers & Security*, No. 38, pp. 97-102.
- [7] WEILL, P., ROSS, J.W., 2004. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Brighton: Harvard Business School Press..

