OPEN ACCESS

World Journal of Economics, Business and Management
ISSN (Online): 3049-2181 | Vol. 2, No. 4, April, 2025
Website: https://wasrpublication.com/index.php/wjebm

Security and Risk Management: A Comprehensive Review

Amirul Hussain Mojumder*

Independent Researcher.

Received: 14/02/2025 | Accepted: 02/04/2025 | Published: 27/04/2025

Abstract: Security and risk management have become crucial disciplines in safeguarding organizations against diverse threats, ranging from cyberattacks and data breaches to physical security risks and geopolitical uncertainties. Effective risk management involves identifying, assessing, and mitigating risks that could compromise the confidentiality, integrity, and availability of assets. This review article synthesizes existing literature, global standards, and best practices in security and risk management, focusing on methodologies, frameworks, challenges, and future directions. The study highlights the importance of integrating technological, organizational, and human factors in developing holistic risk management strategies.

Keywords: Security management, risk assessment, cybersecurity, ISO 31000, risk mitigation, threat analysis, enterprise risk management, resilience.

1. Introduction

In an increasingly interconnected and digitized world, organizations face unprecedented security challenges. Cybercrime, ransomware attacks, supply chain vulnerabilities, natural disasters, and insider threats are growing concerns. Traditional security measures are insufficient without systematic risk management approaches. Security and risk management provide structured frameworks for identifying vulnerabilities, evaluating risks, and implementing protective controls.

This review consolidates current knowledge on security and risk management, examining theoretical foundations, global practices, challenges, and emerging trends.

2. Concept of Security and Risk Management

Security management involves protecting physical and digital assets, while risk management focuses on identifying and minimizing potential threats to organizational objectives. Together, they form a comprehensive approach to resilience.

Key Elements:

- **Risk Identification**: Recognizing internal and external threats.
- **Risk Analysis**: Evaluating likelihood and impact.
- **Risk Mitigation**: Implementing preventive, detective, and corrective controls.
- **Continuous Monitoring**: Regular audits and adaptive security measures.

3. Frameworks and Standards

Several global frameworks guide security and risk management:

- **ISO 31000**: Provides principles for risk management applicable across industries.
- **NIST Cybersecurity Framework (CSF)**: Focuses on protecting information systems.
- **COBIT**: Governance framework for enterprise IT security and risk.
- **ISO/IEC 27001**: Standard for information security management systems (ISMS).
- **Enterprise Risk Management (ERM)**: Integrates security into overall corporate strategy.

4. Security and Risk Management Methodologies

1. **Quantitative Risk Assessment** – Uses statistical models and cost-benefit analysis.
2. **Qualitative Risk Assessment** – Uses expert judgment, risk matrices, and scenarios.
3. **Threat Modeling** – Identifying potential attack vectors in systems and processes.
4. **Business Continuity Planning (BCP)** – Preparing for disruptions and recovery.
5. **Incident Response** – Structured response to security incidents.

5. Challenges in Security and Risk Management

- **Evolving Threat Landscape**: Cybercriminals use AI-driven attacks, making defenses complex.
- **Human Factor Risks**: Insider threats, employee negligence, and lack of awareness.

Corresponding Author:

Amirul Hussain Mojumder

Email: dr.amirulh13@gmail.com.

- **Compliance Pressure**: Organizations must meet regulatory standards (GDPR, HIPAA).
- **Resource Limitations**: Small organizations struggle with cost and expertise.
- **Global Interdependencies**: Supply chain disruptions amplify risks.

6. Emerging Trends

- **Artificial Intelligence and Machine Learning** in risk detection and response.
- **Zero-Trust Security Models** replacing perimeter-based defense.
- **Cloud Security and Compliance** with hybrid/multi-cloud environments.
- **Cyber-Physical Security Integration** in IoT and smart infrastructure.
- **Risk-Based Decision-Making** using real-time analytics.

7. Conclusion

Security and risk management are essential for ensuring organizational resilience in a volatile and uncertain environment. Effective strategies must integrate global standards, leverage technology, and address human factors. Future research should explore adaptive, AI-driven risk management systems, cross-border cybersecurity cooperation, and sustainable frameworks that balance cost with resilience.

References

1. ISO (2018). *ISO 31000: Risk Management – Guidelines*. International Organization for Standardization.
2. NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology.
3. Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage Learning.
4. Hubbard, D. W. (2020). *The Failure of Risk Management: Why It's Broken and How to Fix It*. Wiley.
5. Hopkin, P. (2018). *Fundamentals of Risk Management*. Kogan Page.