ABSTRACT

MANAGING ENTERPRISE SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY SECTOR AND CORPORATE ESPIONAGE

Globalisation and the rapid advancement of technology have profoundly transformed the operational and competitive landscape for contemporary enterprises. These changes have introduced a wide range of risks that threaten organisational stability, performance, and competitive positioning. Among these, corporate espionage emerges as a particularly critical yet frequently underestimated challenge. Defined as the illegal acquisition of confidential information to gain a competitive advantage, corporate espionage encompasses deliberate actions targeting sensitive data such as strategies, technologies, production processes, financial records, and other critical corporate assets. Despite being historically recognised in forms such as industrial and economic espionage, the concept has gained unprecedented prominence in the digital era, where information is a cornerstone of organisational value and operational success.

The increasing reliance on digital technologies and the interconnectedness of global markets have magnified the risks associated with corporate espionage. This phenomenon has become a pressing issue for organisations across all industries, particularly those within the Information and Communication Technology (ICT) sector. Characterised by rapid innovation, high-value intellectual property, and unique technological solutions, ICT enterprises face significant exposure to espionage-related risks. Consequently, corporate espionage represents a multifaceted threat that undermines not only financial stability but also competitive advantage and organisational reputation. This research critically examines corporate espionage within the ICT sector in Poland, offering insights into its prevalence, methods, and consequences while proposing comprehensive countermeasures.

A central argument advanced in this dissertation is the pivotal role of employees in combating corporate espionage. Although advanced technological solutions are essential in securing organisational assets, human factors—such as awareness, education, and engagement—play an equally critical role. Gaps in employee understanding of espionage risks and insufficient knowledge of countermeasures weaken internal security systems, rendering organisations vulnerable to sophisticated attacks. The study highlights the importance of

integrating technical, organisational, and human-centric approaches in designing effective security management strategies.

The primary objective of this research is to develop a security management model tailored to the unique challenges faced by ICT enterprises, with a specific focus on addressing employees' diverse perceptions of espionage-related threats. The study's overarching aim is to enhance data protection and safeguard organisational secrecy in a manner that accounts for both technological and human factors. To achieve this, the following specific objectives were established:

1. **Identification of Security's Role in Corporate Management:** Recognising the strategic importance of security in maintaining organisational stability and achieving business objectives.
2. **Analysis of Challenges in Implementing Information Security Practices:** Exploring the barriers and prerequisites for adopting robust information security measures.
3. **Examination of Espionage Risks in the ICT Sector:** Investigating how corporate espionage influences security management practices in ICT enterprises.
4. **Assessment of Employee Awareness and its Impact on Security Management:** Evaluating the relationship between employee awareness of espionage risks and the effectiveness of security management systems.

This research defines its main problem as understanding the challenges posed by varying employee perceptions of corporate espionage threats in the management of security within ICT enterprises. To address this, a central hypothesis is proposed: effective security management in ICT enterprises must account for differences in employees' threat perceptions to address espionage risks comprehensively. Supporting hypotheses explore the role of rational decision-making, adherence to international standards, countermeasures against espionage techniques, and the integration of employee perspectives into security strategies.

The methodology adopted for this research involves a multifaceted approach, comprising literature reviews, expert interviews, survey-based research, and computational simulations. The study was conducted in five distinct stages:

1. **Literature Review:** An extensive review of existing scholarly and professional literature on corporate espionage, security management, and the ICT sector. This stage involved critical analysis and identification of key themes for further exploration.
2. **Expert Interviews:** Semi-structured interviews with 12 experts in organisational security, focusing on their insights into espionage threats and security practices within the ICT sector.

3. **Survey Research:** A comprehensive survey of 466 respondents across various organisational levels in selected ICT enterprises operating in Poland. The survey assessed perceptions of corporate espionage, response procedures, training practices, and the role of state institutions in addressing these threats.
4. **Model Development:** Based on empirical findings, a security management model was designed, integrating technical, procedural, and human-centric dimensions to address the identified challenges comprehensively.
5. **Computational Simulations:** Simulation-based validation of the proposed model, examining its effectiveness in real-world scenarios and optimising its implementation through iterative testing.

Key findings from the expert interviews and surveys reveal significant gaps in employees' understanding of espionage risks and their ability to respond effectively to incidents. While technical measures such as advanced firewalls, intrusion detection systems, and encryption protocols are widely adopted, the human element remains a critical vulnerability. Inadequate training, low levels of awareness, and inconsistent communication of security policies weaken the overall efficacy of organisational security measures.

The results underscore the importance of regular training, awareness campaigns, and simulated exercises to prepare employees for potential threats. Additionally, organisations must invest in advanced identity and access management systems, conduct periodic security audits, and adopt a proactive approach to policy updates in response to evolving threats. Collaboration with industry partners, technology providers, and governmental agencies is also essential for sharing threat intelligence and coordinating responses to espionage incidents.

The proposed security management model integrates these insights, offering a structured framework for ICT enterprises to enhance their resilience against espionage threats. The model emphasises the following core elements:

- **Educational Initiatives:** Regular training programmes to increase employee awareness of espionage risks and improve their capacity to identify and respond to threats.
- **Technological Solutions:** Deployment of state-of-the-art security infrastructure, including threat detection systems, encryption tools, and access control mechanisms.
- **Policy and Governance:** Development and enforcement of comprehensive security policies, aligned with international standards and best practices.
- **Monitoring and Evaluation:** Implementation of key performance indicators (KPIs) to assess the effectiveness of security measures and identify areas for improvement.

Computational simulations conducted during the research validate the model's effectiveness, demonstrating significant improvements in organisational resilience when its

components are applied holistically. Nine implementation scenarios were tested, each highlighting the importance of adapting the model to the specific needs and risk profiles of individual enterprises. The simulations also reveal the critical role of dynamic adaptation, enabling organisations to respond effectively to emerging threats in the rapidly evolving ICT environment.

This dissertation contributes to the field by presenting a comprehensive and empirically validated framework for managing security in ICT enterprises. It emphasises the need for an interdisciplinary approach, integrating technological, procedural, and human-centric elements to address the complex challenges posed by corporate espionage. The findings have practical implications for policymakers, business leaders, and security professionals, offering actionable insights for enhancing organisational resilience in an increasingly competitive and innovation-driven market.

The research concludes by emphasising the importance of fostering a culture of security within organisations. This involves not only investing in advanced technologies but also prioritising employee education, promoting cross-departmental collaboration, and maintaining alignment with international regulations and standards. Future research directions include exploring the role of artificial intelligence and machine learning in enhancing security management practices and examining the broader implications of corporate espionage in other high-risk sectors.

This study underscores that effective security management is a cornerstone of organisational stability and success in the ICT sector, providing a robust foundation for safeguarding valuable assets and ensuring long-term competitiveness in a rapidly changing global marketplace.