https://doi.org/10.53656/str2024-1s-7-ent

Research Results
Резултати от научни изследвания

ENTERPRISE SECURITY AS AN ELEMENT OF MARKET COMPETITIVENESS

Dr. Gergana Tsankova, Assist. Prof.
University for National and World Economy

Abstract. The security of the enterprise is crucial for its competitiveness in the modern business climate. It involves the protection of assets, information, personnel, and business processes, including intellectual property. Insufficient protection can lead to the leakage of corporate information and infringement of patent rights, jeopardizing the competitiveness of the company. Focusing on security and implementing appropriate measures are essential for achieving market competitiveness and sustainability for the enterprise. The study pays attention to the complexity of defining suitable security measures for the enterprise, considering the dynamics of the environment, industry characteristics, and market presence. The aim of the research is to propose a competitiveness system focused on security, aiming to improve market position and enhance the sustainability of the enterprise. Proactively addressing threats and implementing mitigation measures are crucial for preventing uncertainty, ensuring the resilience of the enterprise, and preserving and increasing its competitiveness.

Keywords: security; corporate security; competitiveness; information security; physical security

Introduction

Enterprise security is an element of market competitiveness, as in the contemporary business environment, safeguarding the assets, information, personnel, and business processes of the enterprise plays a pivotal role in its successful operation and maintaining a competitive position in the market. In this context, enterprise security also encompasses the protection of intellectual property, such as patents, copyrights, trademarks, and other intellectual resources. Safeguarding these rights is of paramount importance since they represent the innovative and creative aspects of the enterprise, setting it apart from market competitors. Such measures also maintain the integrity of the enterprise and prevent unauthorized access or misuse of sensitive information, which could lead to a loss of competitive advantage and trust from customers.

In the digital era, data security and information systems are becoming increasingly significant. Breaches in information security, such as hacking attacks, data theft, or viruses, can result in financial losses, disruptions in business processes, and damage to the company's reputation. Therefore, enterprises must invest in a corporate security system, including internal security policies and procedures, employee training, systematic testing of various systems, data encryption, network protection, and software solutions for threat detection and prevention.

The research thesis argues that deploying an adequate security system against threats and risks is crucial for the enterprise's market competitiveness. Enhancing enterprise security leads to a reduction in risks related to the loss of key personnel, proprietary technologies, losses from theft, sabotage, internal irregularities, and other unfavorable events. This, in turn, builds trust among customers and partners, strengthens the company's reputation, and increases its competitiveness.

The challenge in this study is related to the complexity of defining adequate security measures against threats and risks to ensure the enterprise's competitiveness in the market. The adequacy of these measures should consider the dynamics of the environment, the industry specifics, and the market presence of the enterprise and its products and services.

Security threats to the enterprise

The concept of „security", and specifically „corporate security", can be broadly and inadequately defined using the term „threat". Corporate security can be understood as a state of absence of dangers and threats to the interests of the corporation. If such threats exist, the corporation possesses the capabilities to avoid or neutralize them (Dimitrov et al. 2021, p. 103).

Threats are events, actions, or their consequences directed at impacting the values, interests, or freedom of corporate behavior and action. They are measured as a product of vulnerability potential and intention to influence. Examples of threats include political, economic, financial, and other constraints and sanctions; the coercive power of monopolies; ordinary and organized criminal activities; financial and tax administrative violations; financial and accounting fraud and abuse; money laundering; terrorism financing, and more (Dimitrov et al. 2021, p. 103).

The functions of corporate security are associated with identifying and effectively managing, at an early stage, all negative trends that could jeopardize the enterprise's goals, sustainability, and long-term market presence. Similar to the national security sector, the corporate security system operates based on monitoring, analysis, and evaluation of identified threats and risk management, thus ensuring the continuity of work processes and coordination of all security and safety-related functions within the enterprise (Krushkov 2020, p. 25).

Security threats are identified as those with direct or indirect effects on goal performance. Security threats are those that would objectively hinder the realization of state, national, or public interest in the context of national security or business interest in a corporate sense. If these threats are not identified in a timely manner and timely action is not taken against their development, uncertainty or disruption of work processes arises, directly affecting the achievement of set goals. After a destructive event occurs, resilience and recovery inevitably require significant efforts, additional resources, and a considerable amount of time, all of which come at a high cost. Depending on the destructive event and the time required for recovery, these costs or impacts on work processes can be catastrophic. Predicting such significant destructive events, eliminating vulnerabilities on time, and creating buffers and measures to comprehensively mitigate the consequences are the tasks of the security structure. The most significant factors here are the professionalism of the security team and time.

External threats to enterprise security

Among the main external threats are: regional or national macroeconomic or social instability; incidental changes in regulatory requirements directly or indirectly affecting enterprise operations; mergers and acquisitions among competitors; consolidation of business and market share among competitors; emergence of new competitors or new products in the existing market; development and access to new technologies by competitors in the existing market; patent-protected inventions and utility models created by competitors in the existing market, and others (Krushkov 2020, p. 26).

External threats arise from the external environment for the corporation. Various subjects can be sources of such threats. External threats are most commonly associated with the actions of competitors. Customers, suppliers, the government in the form of administration, and other structures can also be considered as threats. Natural and social phenomena are another type of external threats. The most recent example of such a threat is the COVID-19 pandemic, which, in turn, triggers other processes – economic, political, and social – that unfold at the national, regional, or global level, impacting the corporate world (Dimitrov et al. 2021, p. 106).

One of the main sources of external threats to corporate interests comes from natural phenomena that often possess a force beyond human control. Their impact can be direct or indirect, depending on the nature of the business and the characteristics of the location where the event is considered. Although their occurrence may be predicted and well-known from experience at a certain point, their manifestation can be surprising, exceeding predictions and rendering the taken impact measures inapplicable.

Internal threats to enterprise security

Internal threats to corporate security are of a diverse nature. In certain cases, the negative consequences of these threats can be extremely serious, as they may go unnoticed or underestimated for an extended period. Additionally, they can easily be disguised. Another characteristic of internal threats is that, when detected in a timely manner, the corporation can react directly (for example, if it is found that an employee is leaking information, they can be dismissed and held accountable, or if a conflict arises due to poor communication between units, it can be resolved through mediation by management, improving communication). Such a possibility is lacking in the case of external threats.

Among the main internal threats are: unclear or incorrectly formulated goals, lack of centralization and/or organizational responsibility in decision-making; underestimation of planning, lack of specific deadlines and/or unclear responsibilities; non-implementation or non-updating of the plan due to changes in the external environment; turnover in key positions; increase in production, technological, or trade defects; inability to prevent incidents that may affect corporate reputation; unspecified and unprotected intellectual property; undefined and unprotected corporate information representing trade secrets; lack of respect for creative work as a developmental factor; ineffective corporate security system; poor leadership, and others.

The personnel engaged in various tasks remain one of the main sources of threats to corporations, regardless of the nature of their activities. This element can be seen as a sustainable source of threats, mainly focusing on behavioral aspects. Threats related to personnel are more often intentional and to a lesser extent accidental.

Building a competitiveness system from the perspective of enterprise security

Building a competitiveness system from a security perspective is a complex approach that involves various factors and strategies implemented by the enterprise to achieve and maintain its competitiveness in the market. This system involves analyzing internal and external factors that influence the enterprise's competitiveness. The enterprise must analyze the external environment, including economic, social, political, and technological factors that may impact its competitiveness. This analysis helps understand market trends and identify opportunities and threats.

Internal factors include resources, capacity, personnel, operations management, and innovations, as mentioned earlier. External factors encompass market competition, customer needs and preferences, economic environment, legal and regulatory factors, among others. The enterprise needs to analyze its internal resources, including human resources, finances, technologies, and operational

processes. This helps identify the strengths and weaknesses of the enterprise and develop strategies to build a competitive advantage.

The competitiveness system also involves developing strategies to achieve a competitive advantage. This includes defining the target market niche, differentiating products or services, optimal brand positioning, utilizing marketing and advertising strategies, developing innovations, etc. The enterprise needs to formulate strategies to position its products or services in the market, considering target audiences, differentiation from competitors, pricing policies, and implementing marketing and advertising strategies.

An essential part of the competitiveness system is continuous improvement and adaptation to changing market conditions. The enterprise must be flexible and responsive, monitor industry trends and innovations, and take measures for adaptation and improvement.

All these factors and strategies interact and complement each other within the competitiveness system. The goal is to achieve long-term competitive advantage and successfully position the enterprise in the market by meeting customer needs and preferences, reducing costs, improving quality, and implementing innovations.

The competitiveness system from the perspective of enterprise security includes measures and strategies aimed at protecting and preserving its security and integrity. This system aims to prevent potential losses, damages, or vulnerabilities that could harm the enterprise's competitiveness. The main aspects and factors that are part of the competitiveness system from a security perspective include information security, physical security, risk management, and protection of intellectual property.

Information security

Information security is an integral part of the enterprise's corporate competitiveness system. It pertains to the protection of the information that the enterprise operates, including data, systems, networks, and communications.

One of the key aspects of information security is safeguarding the enterprise's confidential information. This involves measures to prevent unauthorized access to information, such as using secure passwords and authentication, access control, data encryption, and other protection techniques. The goal is to prevent potential losses or disclosure of sensitive information that could harm the enterprise's competitiveness.

Information security also includes protection against malicious software, such as viruses, trojans, ransomware, and other types of malware. The enterprise should implement appropriate antivirus and anti-malware solutions, update its systems with the latest patches, and conduct systematic security checks and analyses to detect and prevent potential threats.

Corporate competitiveness systems should also include measures to protect data during technical issues or natural disasters. This may involve data and system backups, building disaster recovery systems, and other measures to ensure business operations' continuity.

Data and information protection: The enterprise must build secure systems for data storage and processing. This may include using secure servers, secure network connections, and protected databases. The systems should be configured to limit data access only to authorized users.

Encrypting information is a crucial aspect of data and information protection. The enterprise should use encryption when transferring and storing data to prevent unauthorized access or data transfer.

The enterprise must establish and enforce data protection policies. This involves defining rules and procedures for data management, establishing passwords and access control to systems and information. Policies should be clear, implemented, regularly reviewed, and updated.

Employee training is essential for data and information protection. Staff should be trained in data security, understand the risks, and apply the correct data protection practices. This may include training on strong passwords, the importance of regularly updating software, and awareness of phishing attacks and other forms of social engineering attacks.

Continuous training and awareness of employees regarding information security are also crucial. The enterprise must provide training and regular updates to staff to ensure they understand the importance of information security and are familiar with best practices for information protection. This includes training on data security, the enterprise's policies and procedures, the use of secure passwords, recognizing social engineering, preventing phishing attacks, and other forms of cyber attacks.

The enterprise must provide clear and clearly communicated policies and procedures for information security. This includes defining rules and corresponding sanctions for violations, protecting the privacy of customer and employee data, regular security checks and audits, as well as incident response and recovery.

Continuous monitoring and updating of information security systems and technologies are also crucial. The enterprise must monitor for new threats and vulnerabilities, update and patch software products, use secure network configurations and traffic filtering, and implement measures for monitoring and conducting security analyses.

Ensuring compliance with regulatory requirements for information security, such as GDPR (General Data Protection Regulation), PCI DSS (Payment Card Data Security Standards), and other regulatory frameworks, is essential. This involves building processes and controls that meet regulatory requirements, ensuring the legality and integrity of the enterprise's information.

The competitiveness system from the perspective of enterprise security must be comprehensive and continuously improved to ensure that data and information are well-protected from external threats and internal security breaches.

Physical security

Physical security is of paramount importance for the competitiveness of an enterprise, protecting physical assets from various threats. Measures include video surveillance and activity recording, access restriction through barriers, cards, and biometric systems, secured signaling systems for warning and access control. The physical protection of equipment is carried out through the use of safes, grilles, cash boxes, and locking devices, ensuring the integrity and security of essential inventory. These measures work in conjunction with the technical and information aspects of the enterprise's overall security system.

Physical security integrates with technical and information protection measures for the enterprise. The technical infrastructure includes installed systems such as alarms, motion detectors, and video surveillance. Integrated systems allow centralized management and interaction with the enterprise's information systems. Employee training focuses on familiarizing them with physical security policies and procedures, the use of technical systems, and response to threats. Physical design of facilities involves the use of durable materials, appropriate planning of video surveillance, and lighting. Regular checks and analyses are conducted to assess the effectiveness and improvement of physical security systems.

Risk management

Risk management is a crucial aspect of the enterprise's competitiveness system. The goal of risk management is to identify potential threats and risks that may affect the competitiveness of the enterprise and take appropriate measures to reduce or manage these risks.

The first step in risk management is conducting a risk analysis. This involves identifying potential threats and risks related to the competitiveness of the enterprise. These risks may be associated with the market environment, technological developments, financial factors, legislation, and other aspects.

After identifying the risks, the enterprise needs to develop and implement appropriate measures to reduce or manage these risks. This may include creating business continuity plans that outline actions and procedures to maintain the continuous operation of the enterprise in crisis situations or unexpected events.

Additionally, the enterprise should ensure backup systems and capacities are available to be used in case of necessity or damage to the primary systems. This may involve having backup servers, data copies, and disaster recovery systems.

Developing crisis plans is also an essential part of risk management. These plans outline the actions that should be taken in the event of a crisis to minimize damages and restore the normal operation of the enterprise.

All these risk management measures aim to ensure the security of the enterprise and guarantee the continuity of its competitiveness. As part of the competitiveness system, risk management helps prevent potential losses and maintain the stability and success of the enterprise in the competitive environment.

Data and information protection, including the use of secure systems and data encryption, provide protection against potential intruders and unauthorized access to sensitive information. This helps maintain the confidentiality of the enterprise's data and avoid the possibility of theft or loss of crucial information.

Identifying and managing potential risks associated with the competitiveness of the enterprise provides an opportunity for prevention and preparation for possible crisis situations or unexpected events. Business continuity plans and crisis plans provide frameworks and actions to be taken during crisis situations to ensure minimal impact and swift recovery of normal enterprise operations.

The risk management system from the perspective of enterprise security helps create a secure and reliable foundation for its competitiveness by ensuring the protection of valuable assets, preventing losses and disruptions, and ensuring continuity in business operations. This contributes to building trust among customers and partners, which is a crucial aspect of the enterprise's competitiveness.

Intellectual property protection

The enterprise must take measures to protect its intellectual rights by registering ownership and monitoring for infringements. This prevents illegal copies and unauthorized use of intellectual property, maintaining the uniqueness and competitive advantage of the enterprise and safeguarding it from unfair competition.

Intellectual property protection provides legal protection and ownership rights over innovations, enabling legal actions against violators. This allows the enterprise to extract economic value by licensing or selling its innovations to other market participants. Intellectual property protection also helps the enterprise safeguard its reputation and brand. Protected innovations and products ensure better quality and consistent delivery, preventing the emergence of counterfeit versions that could harm the company's reputation. This kind of protection contributes to customers' perception of quality and uniqueness, building more trust in the brand.

Intellectual property protection is a key element for competitiveness and the long-term sustainability of the enterprise. It creates conditions for innovation and

development, which are crucial for the long-term success of the enterprise.

Conclusion

The establishment, implementation, and effective management of a competitiveness system focused on security will enhance the market position and increase the resilience of the enterprise. The primary objective is to ensure a high level of protection for all operational processes. To achieve a high level of security, it is necessary to select an effective security system model that is suitable for the specific environment and aligns with the capabilities of the organization.

Another primary goal is to safeguard the assets of the organization, including physical assets such as buildings and equipment, informational assets like data and systems, as well as the human resources of the enterprise. Implementing appropriate security measures helps prevent losses and damages to these assets.

Such a system will help prevent incidents and breaches, such as theft, break-ins, sabotage, and violations of information security. This leads to a lower risk of business interruption, data loss, and negative consequences for the organization.

Ensuring the safety of operational processes and the people carrying out tasks is crucial for the successful management of any organization. Every management structure should build and maintain an integrated security system. This system is responsible for creating an environment that is secure, predictable, and resilient to achieve the goals of the enterprise.

The functions and responsibilities of security professionals are carried out through an integrated security system. The effective functioning of this system can be jeopardized by various factors, including an inappropriate response to the environment and potential threats, a lack of integration between planning, monitoring, detection, and response processes, insufficient control over the execution of security tasks, or outdated organizational and technical technologies. Therefore, systematic testing plays a vital role in security management by ensuring a high level of protection.

Enterprise security also influences its reputation and trust among clients and partners. Demonstrating commitment to security and adhering to high standards helps build trust and confidence in the organization, improving its image and competitiveness.

An appropriate security system helps the organization identify and manage potential security risks. This includes assessing and minimizing risks, developing contingency plans, and ensuring a prompt response to incidents.

REFERENCES

DIMITROV, D. and et al. 2021., *Corporate Security.* Sofia: Publishing Complex UNWE.

KRUSHKOV, N., 2020. *Security Leadership Creativity*. Sofia: Publishing Complex-UNWE.

MUELLER, D. C., 1986. *Profit in the long run*. Cambridge, MA: Cambridge University Press. PORTER, M., 1985. *Competitive advantage: creating and sustaining superior performance*. New York: The Free Press.

NENOV, T., 2008. *Management of Competitiveness and Growth*. Varna: „Science and Economics", Economic University.

SHTEREV, N., 2012., Quantitative Functional Assessment of the Competitiveness of Business Organizations. *Economic and Social Alternatives Journal*, Issue 3, UNWE.

VELEV, M., 2004. *Assessment and Analysis of Corporate Competitiveness*. Sofia: Softtrade.

VLADIMIROVA, Y., 2005. *Competition and Competitiveness of Companies in Trade*. Gabrovo: Vasil Aprilov.

✉ **Dr. Gergana Tsankova, Assist. Prof.**
Intellectual Property and Technological Transfer Department
Business Faculty
University of National and World Economy
Studentski district
19, December 8th St.
1700 Sofia, Bulgaria
E-mail: g.tsankova@unwe.bg