The Eurasia Proceedings of
Educational & Social Sciences (EPESS)
ISSN: 2587-1730

The Eurasia Proceedings of Educational & Social Sciences (EPESS), 2023

Volume 32, Pages 151-157

IConMEB 2023: International Conference on Management Economics and Business

Examining the Strategic Embeddedness of Corporate Security

Reka Saary
Obuda University

Abstract: In comparison with the academic literature on public security, national security, social and economic security, and the challenges of the private security sector, corporate security policies have received little attention in the last decade. This is particularly surprising given that, as in the above-mentioned areas, there is a serious ongoing struggle and competition at the corporate level to meet new security challenges in response to the turbulent environment. The aim of this paper is to examine the strategic embeddedness of corporate security policy and its inherent challenges. The theoretical basis of the study, in line with the above, is provided primarily by the conceptualization of corporate security policy and the presentation of the trends and tendencies in this area. Based on the significant shift in the perception of security in organizations, it is predicted that new challenges and converging risks fundamentally change the security priorities of companies today. The exploration of new aspects of corporate security is done in the form of qualitative research through in-depth interviews with experts. The aim of the research is therefore to analyses the relationship between corporate security policy and strategic planning.

Keywords: Corporate security, Integrated security, Maturity levels

Introduction

Over the last two decades, the perception of security has changed significantly, at the level of society, individuals and companies. Businesses are taking an increasingly complex approach to the issue, integrating preparation and protection against different types of risk. At the same time, the responsibility of companies in shaping individuals' perceptions of security is increasing (Saáry, 2020). It is therefore important to examine how the perception of corporate security policy has changed in recent times and what factors are influencing this process. The research presented in this paper explores the views of industry professionals along the above lines. The aim of the research is to examine how companies' perceptions of security have changed in the recent past, and to what extent security is embedded in strategic planning today. Accordingly, the literature review is presented, followed by a description of the research methodology and results, and a summary of the findings on this topic.

Corporates Security

In reviewing the definitions of corporate security, it can be stated that security is a business requirement; corporate objectives cannot be met without a guarantee of it (Vasvári et al., 2006). The security of a company is a favourable state (acceptable to the organisation, given the threat - security sensitivity), where changes are unlikely but not impossible (Vasvári, 2009). The main focus of corporate security policy is the protection of the most important factor of production: the protection of human life and health, along with the viability of the company (Király & Pataki, 2013).

Corporate security is the applied field of security sciences, with a business-oriented approach aiming to protect people, information and corporate assets within the organisation, and to ensure corporate self-protection.

Corporate security policy enables the organisation to respond to security threats in a controlled and regulated way (Ludbey et al., 2017).

One hundred percent security cannot be obtained, the threat to the company remains until the causes are eliminated or become negligible (Király & Pataki, 2013). Corporate security is acceptable if the threat to the confidentiality, integrity and availability of the resources of the company, i.e. the risks (internal and external), meet the level defined in the security strategy (Vasvári et al., 2006; Buzan et al, 1998). It should be noted that some authors argue that the definition of corporate security cannot be interpreted without taking into account the specificities of the sectors concerned, and therefore propose the formulation of sector-specific definitions instead of a generally adapted definition (Brooks, 2010; Walby & Lippert, 2013).

The common feature of the definitions presented above is that they focus almost exclusively on protecting the company against external threats. Michelberger (2014) highlights a very important aspect of corporate security as his definition does not focus exclusively on the protection of the organisation, but emphasises its role in creating and maintaining the security of its environment. According to the author corporate security is a state in which an enterprise is able to maintain its viability and value-creating processes over long terms. A further criterion for security is that the future of the enterprise is in its own hands, based on its strategic plans, and that the enterprise does not endanger its environment, external and internal stakeholders in its activities.

The Evolution of the Perception of Corporate Security

While the currently prevailing perception does not necessarily reflect the true meaning and importance of corporate security, it has taken many years and significant changes in the way companies approach security to get to this point (Dalton, 2003). The phases in the evolution of the perception of corporate security in the 20th century were as shown in Figure 1. This historical development does not, however, mean that the perceptions of each period are not reflected in today's corporate practices.

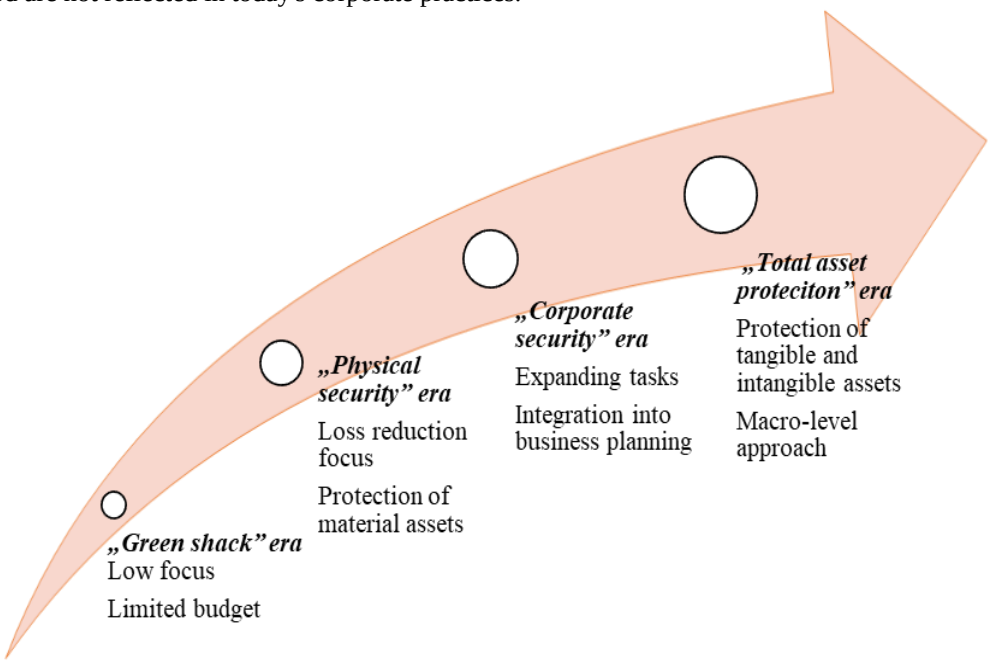

Figure 1. Evolutionary stages in the understanding of corporate security
Source: author's own elaboration based on Dalton (2003)

Looking at the phases of transformation, we see that the third era emerged as the time when the multifaceted approach to security in the enterprise as understood today began to be implemented. An important feature of this era is that business and security interests are converging, and companies are taking a proactive approach to protection (Dalton, 2003). The macro-level approach that characterizes the era of total asset protection, in the view of some authors, foreshadows the evolutionary perspective that will unfold in the 21st century, in which public, governmental institutions will adopt corporate practices and corporate security policy. This culture of strict supervision and control, adopted and infiltrated from the corporate environment, has an impact on the well-being and perceptions of security of members of society (Walby & Lippert, 2013). The authors refer to this trend, which is indeed evident today, as the corporate security creep era.

Convergence and an Integrated Approach to Corporate Security

In the last two decades, the issue of convergence of security areas has become increasingly relevant in the international literature. Convergence of security refers to the harmonisation of traditionally independent areas (islands) of operational risk management in order to achieve a higher level of security in a more cost-effective way. This means an integrated approach to logical, IT, physical, personnel (human) security, business continuity, including disaster recovery and risk management at the level of resources and processes (Tyson, 2007). The growing focus on integrated corporate security is in fact a response to the challenges induced by convergence of risks. However, it is important to distinguish between the concept of an integrated approach, which is manifested at the level of decision-making/management and ideally in the corporate culture, and the concept of an integrated security management system, which can be understood as a functional aspect of the first concept (Papp, 2006). The synergetic effect of combining tools from different areas of security will result in a better, more effective and, last but not least, less expensive overall security system (Kuris, 2010).

The consultancy company Booz Allan Hamilton (2005) has explored what change is needed to create convergent corporate security, based on the views of industry experts. In a multi-phase study, the experts identified nine operational dimensions in three areas (strategic impact: risk management, governance, cost planning; process management: regulation, integration, case studies; and finally, human factor management: leadership style, responsibilities and tasks, and understanding the essence of the business) that play a key role in organisational change.

Method

In line with the objective presented in the previous section, the empirical research explored the perception of security issues within organizations. The method used was qualitative research, in-depth interviews with corporate security managers. The selection of the participants was based on the idea of including representatives of several economic sectors, taking into consideration that corporate security policies are highly industry-specific. The selection was constrained by the availability and willingness to respond of the participants. The interviewees all held senior positions in the security field, their position in the corporate hierarchy and some characteristics of their organizations are presented in Table 1.

Table 1. Centre the caption above the table.Source: author’s own elaboration

Inter-viewees	Represented industry	Size of security department	Position in the company hierarchy
C1	Food and chemical industry	3	Production Manager's report
C2	Energetics	8	Top manager's report
C3	Electronics	11	Top manager's report
C4	Telecommunications	19	Chief executive's report
C5	Telecommunications	~30	Chief executive's report

According to the selected methodology of the research, the information was collected along an interview guide which, although it may limit the flow of information, helps to avoid possible loss of data due to a complete lack of structure. In this case, a total of five 45-60 minute interviews were conducted. In processing the information a simple content analysis was used.

Results and Discussion

The results of the research will be presented starting with a review of the priorities identified in the literature, including the strategic embeddedness of corporate security policy, the appearance of integration and expert opinions on security as a potential competitive advantage. The aim was to capture the complexity of security in the context of corporate security. Based on industry expert reports and academic research, we see that there has been some recent shift in the perception of security and risk, yet security policy remains primarily an operative management area in corporate practice.

Regarding the perception of corporate security within the organisation, the only consistent view that emerged from the in-depth interviews was that it depends on a number of factors. Without exception, the interviewees perceive that, although there has been some positive shift in the prestige of the field, security managers must

continue to take action to ensure that security policies are accepted. All respondents highlighted the importance of management commitment (which they consider to be highly personality-dependent) and the importance of the security expert's personal persuasiveness.

The recognition of security within the organisation is clearly reflected in the position of the security manager in the organizational hierarchy. This can be confirmed by what one interviewee (C3) said "as the number of levels between top management and the safety executive increases, the effectiveness of the safety organisation decreases." In four of the companies in the research, the head of security was a direct subordinate of the top manager, although there was one company (C5) where this was the result of a change in organisational structure that had taken place just over a year earlier. The reorganisation in their case was not only important from this point of view, but also involved the integration of different areas (facilities, information security, compliance, regulatory data), resulting in a highly complex centre of competence. In the one remaining case, most of security functions, due to their sectoral nature, belong to a significant operational area (supply chain organisation), and operate as a separate island, completely isolated from IT security. Nevertheless, the expert's view is that, also in this case, the management has recognised the increased importance of security and is treating this area as a growing priority.

Heterogeneous opinions were expressed on the extent to which security considerations are incorporated into the strategic planning process. Security is elusive, its absence mostly manifesting itself in different incidents. This is precisely the reason why security organisations often take a reactive approach, as preparedness and proactivity typically involve high costs. It can be stated that for today's business executives, "security is important, but not sufficiently so" (C3) to avoid dealing with this area retrospectively. In the light of the above, it is rather utopian that security is always integrated into the design phases of all processes ("security as design"). However, efforts are being made in this direction, as it has been proven in numerous cases that prevention costs less than mitigation (C5).

Although there was one interviewee (C1) who believes that managers take security aspects into account to a sufficient extent in strategic planning, this seems to be contradicted by the common understanding that emerged among the experts regarding the setting of the security budget. There was therefore a consensus that the budget planning of the security organisation is clearly an operational issue for companies. From this point of view, again, the skills of the security manager, who can justify the expenditure on the basis of a cost/savings - or even revenue - approach, become of paramount importance. "...business is almost always the priority" (C1). At the same time, conscious strategic planning is obviously hampered by a number of factors, such as the issues, items that are difficult to monetise, and the lack of information available in certain situations and risk analysis.

Interviewees also agreed that security is a value, that "security and quality cannot be questioned" (C1), and that security management is therefore a "value-creating process" (C2), a "productive area" (C3), a "driving force" (C4) that brings companies closer to meeting business objectives. Moreover, one company has a "profit centre" (C5) within the security organisation, where security services are sold on the basis of the "security as a service" principle.

In addition to the above, safety executives, with the exception of one participant, all believe that safety can be a competitive advantage. The comparative advantage manifests itself mainly in the form of guarantees offered to customers and clients, protection, quality assurance linked to standards. According to the interviewees, these certifications distinguish their company from competitors and thus have a direct impact on purchasing decisions. Furthermore, the reputation associated with a reliable partnership implicitly influences the market position of the company.

Summarising the information provided in the interviews, it can be concluded that, according to the views of the security executives, there has not necessarily been a significant change in the perception of security in recent years, although there has been a major shift in the context of digitalisation and globalisation pressures for more than a decade. It can also be seen that the importance and perception of this area within the company is determined less by external trends than by the personality, negotiating power, actions and approach of the security manager. Security aspects are not typically considered in strategic planning. The general consensus among interviewees is that corporate security continues to be viewed primarily as a cost centre by managers, despite the unanimous emphasis among practitioners on the value-added potential of this field. A summary of the experts' opinions is shown in Figure 2.

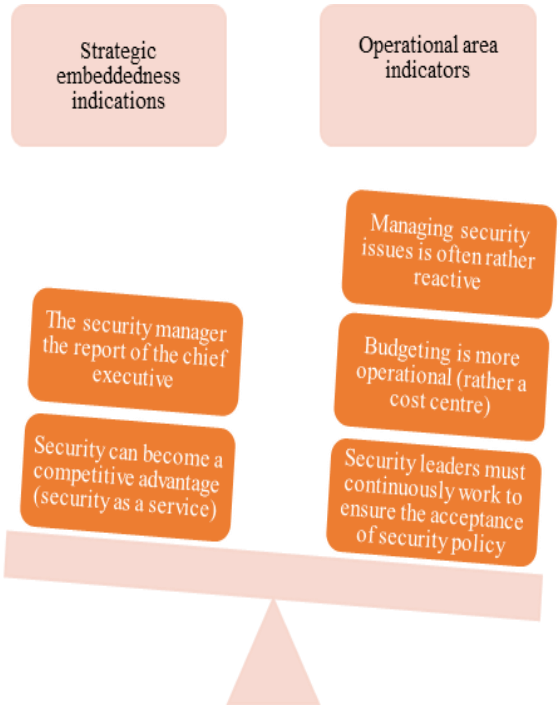

Figure 2. Perception of security within organizations based on expert's opinion
Source: author's own elaboration

However, when interpreting the results, we must take into consideration the fact that for professionals working in this field, familiarity with the field, day-to-day problem solving, active participation in the processes may make it difficult to abstract and to assess the trends underway as an external observer.

Conclusion

The research examined the position of security management within the company, based on the opinions of security managers. Based on literature background a significant shift in the perception of security within the company was predicted based on the fact that new challenges and converging risks are fundamentally changing the security priorities of companies today. International good practice in this area therefore highlights the trend towards the spread of the concept of integrated security and the integration of security issues into strategic decision-making as a direction of development. On the basis of the in-depth interviews with experts, it was found that Hungarian practice in terms of the strategic embedding of corporate security policy typically lags behind international trends and recommendations. As regards the perception of security within the company, although a certain shift can be observed, the positioning of this area is still mainly a function of the competencies of security managers and not based on environmental expectations. For security executives, this is why it is particularly important to make security "visible", which can only be achieved by mapping the right - in the first instance - internal stakeholders and through targeted, effective communication. Involving internal stakeholders is the first step in the change process, as they will later become the first point of contact for a wider range of stakeholders.

Overall, it can be stated that the performance of companies in this area depends to a large extent on the perception of security within the company and the recognition of the security organization. Internal company characteristics therefore have a significant influence on the extent to which security is integrated into strategic planning. Taking all this into account, the maturity or corporate orientation model, as set out in Table 2. emerges.

The guarantees of progress between maturity levels and stages can be provided by appropriate assessment and diagnostics (with targeted methodologies), as well as assistance in the development of strategies and operational tools for each maturity level, which are still being developed.

Table 2. Centre the caption above the table. Source: author's own elaboration

Corporate orientations/ Level of maturity	Focus of security policy	Target groups
Invisible security	Problem solving Reactive behaviour Support for operations	Not applicable
Visible security	Proactive Ad hoc coordination of areas Ensuring operations	Employees (internal stakeholders)
Total, "holistic" security	Integrated (comprehensive security) Strategic embeddedness	External and internal stakeholders

Along with the above conclusions, it would also be important to highlight the limitations of the research. While qualitative research methodologies do not allow for generalizable findings, they do support a deeper understanding of phenomena. In this respect, therefore, in-depth interviews with experts, although a good choice for the discussion of the issue of security responsibility, are only suitable for declaring generally accepted results with reservations due to the small sample size. It is important to emphasise, however, that due to the specificity of the topic and the relatively small population of security policy practitioners/interviewees, the conclusions drawn from the results of the five in-depth interviews can be generally valid. This belief is partly confirmed by the qualitative predominance of the theoretical grounding in the field, which is also evident in related studies, and by the fact that already from the fourth interview onwards, theoretical saturation was noticeable.

The issue of security within the company is an increasingly important, though less researched, area. As has been seen, corporate security executives are taking steps to improve the perception of this area, but it is also important to broaden the scope of academic research on this topic.

Scientific Ethics Declaration

The author declares that the scientific ethical and legal responsibility of this article published in EPESS journal belongs to the author.

Acknowledgements or Notes

* This article was presented as an oral presentation at the International Conference on Management Economics and Business (www.iconmeb.net) held in Antalya/Turkey on November 16-19, 2023

References

Booz, A. (2005). *Convergence of enterprise security organizations Alexandria, VA: The alliance for enterprise security risk management* Retrieved from https://www.semanticscholar.org/paper/Convergence-of-Enterprise-Security-Organizations-Hamilton/

Brooks, D. (2010). What is security: Definition through knowledge categorization? *Security Journal, 23*, 225–239.

Buzan, B., Waever, O., & Wilde, J. (1998). *Security: A new framework for analysis (Boulder Colo.).* London: Lynne Rienner Publishers.

Dalton, D. R. (2003). *Rethinking corporate security in the post-9/11 era: Issues and strategies for today's global business community*. Gulf Professional Publishing.

Király, L., & Pataki, J. (2013). Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz. *Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata 23*(1), 173-187.

Kuris, Z. (2010). A biztonságtechnika tudományszak tárgya és eredményei. *Hadmérnok, 5*(1), 39-49.

Ludbey, C. R., Brooks, D. J., & Coole, M. P. (2018). Corporate security: Identifying and understanding the levels of security work in an organisation. *Asian Journal of Criminology, 13*, 109-128.

Michelberger, P. (2014). *Információbiztonság és uzleti bizalom.* (Doctoral dissertation*).* Habilitációs tézisfüzet, Óbudai Egyetem

Papp, A. (2006). Biztonsági megoldások integrációja Robothadviselés 6. *Tudományos Szakmai Konferencia* Retrieved from http://hadmernok. hu

Saáry, R. (2020). *A vállalati biztonságpolitika a stakeholder elmélet és a felelősségvállalás tükrében* In: A. Csiszárik-Kocsir & J. Varga (Eds.) *Vállalkozásfejlesztés a XXI. században X./1.: A szervezetek reakciója és válaszai a jelen kor uzleti kihívásaira* (pp.336-354). Budapest, Magyarország: Óbudai Egyetem

Tyson, D. (2011). *Security convergence: Managing enterprise security risk*. Elsevier

Vasvári, Gy (2009). *A társadalmi és szervezeti (vállalati) biztonsági kultúra*. Budapest: Ad Librum Kiadó.

Vasvári, Gy., Lengyel, Cs., Valádi, Z. (2006). *Vállalati biztonság keretrendszere, Vagyonbiztonság, Uzembiztonság, Informatikai Biztonság Ajánlás 6.0 változat*. Budapest: Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest

Walby, K., & Lippert, R. (2013). The new keys to the city: Uploading corporate security and threat discourse into Canadian municipal governments. *Crime Law and Social Change, 58* (4), 437-455.

Author Information

Réka Saary
Óbuda University, Keleti Faculty of Business and Management
H-1084 Budapest, Tavaszmező str. 15-17.
Hungary
Contact e-mail: *saary.reka@kgk.uni-obuda.hu*

To cite this article:

Saary, R. (2023). Examining the strategic embeddedness of corporate security. *The Eurasia Proceedings of Educational & Social Sciences (EPESS), 32,* 151-157.