European Research Studies Journal
Volume XXVII, Issue 4, 2024

pp. 512-523

The Role of Organizational Culture in Managing Organizational Security

Submitted 13/09/24, 1st revision 20/09/24, 2nd revision151/10/24, accepted 30/10/24

Aneta Chrząszcz[1], Marek Tomaszycki[2], Wiesława Załoga[3], Andrzej Sztandera[4]

Abstract:

Purpose: *The aim of the article is to analyse the role of organizational culture in managing organizational security and to examine how this culture influences the effectiveness of security management strategies. In the first part of the article, the authors present the essence of organizational culture concerning security. They then describe security management in contemporary organizations. The main section involves an analysis and comparison of organizational culture and security.*

Design/Methodology/Approach: *An analysis and comparison of organizational culture and security were conducted. The research problem was formulated as: How does organizational culture influence security management within an organization, and which elements of this culture are crucial for effective protection against threats? In line with this research problem, a hypothesis was proposed, suggesting that a strong organizational culture promoting engagement, responsibility, and open communication significantly enhances the effectiveness of security management activities and reduces the number of internal and external incidents. The theoretical research methods included a literature review covering management theories, models of organizational culture, and concepts related to risk and security management. A synthesis method was also employed, combining various theories and models of organizational culture and security management to develop an integrated perspective. This reasoning allowed for the formulation of general conclusions.*

Findings: *Managing security in the context of organizational culture is a complex process that requires further research and analysis to fully understand the dynamics and impact of culture on organizational security. Organizational culture and security strategies must be closely integrated to create a coherent security management system.*

Practical Implications: *Best practices in organizational security arise from the daily application of principles. Employees must understand that their personal actions affect the overall security of the organization. By implementing tools such as two-factor authentication,*

[1]*Faculty of Economics, John Paul II University in Biala Podlaska, Poland,*
ORCID: 0000-0001-9749-274X, aneta.chrzaszcz@op.pl;
[2]*Military University of Land Forces in Wrocław, Poland,*
ORCID: 0000-0001-7952–0954, marek.tomaszycki@awl.edu.pl;
[3]*Military University of Technology, Warsaw, Poland,*
ORCID: 0000-0001-7758-0187, wieslawa.zaloga@wat.edu.pl;
[4]*Warsaw Management University, Poland,*
ORCID: 0009-0008-1101-923X, andrzej.sztandera@interia.pl;

data encryption, and strict access control, companies can significantly reduce the risk of incidents.
Originality value: *A well-formed organizational culture is the foundation upon which effective security management in an organization is built.*

Keywords: *Security, organizational culture, management, organization, risk.*

JEL codes: *M14.*

Paper type: *Research article.*

1. Introduction

Organizational culture plays a crucial role in managing the security of an organization. It encompasses a set of values, norms, beliefs, and practices that shape how employees act and influence how they perceive and fulfil their responsibilities in the context of protecting the company's resources. The authors focus on demonstrating how these invisible mechanisms can either strengthen or weaken the effectiveness of security systems.

Organizational security is not solely about formal procedures, technologies, or infrastructure. It also involves people's attitudes toward threats, their risk awareness, and the ways in which they collaborate to minimize potential dangers. Organizational culture can either support or hinder the implementation of effective security strategies. Organizations that promote open communication, trust, and accountability are more likely to quickly identify and manage threats. In contrast, companies dominated by a fear of punishment, concealment of mistakes, or lack of transparency may struggle to maintain an adequate level of security.

The authors attempt to illustrate that security management is not merely a technical issue but requires understanding and managing elements of organizational culture that can either facilitate or obstruct resource protection. A well-formed organizational culture is the foundation upon which effective security management in an organization is built.

2. The Essence of Organizational Culture in the Context of Security

Organizational culture is an important organizational determinant of the process of organizational creativity (Bratnicka, 2010). One of these factors is the model of organizational culture. This structure enables an understanding of how various elements influence the functioning of a company, particularly in the context of security management, innovation, and operational efficiency. When creating such a

model, it is essential to consider the key components that shape employee behaviours and attitudes and support the implementation of organizational strategies.

The first and fundamental element of the model is core values, which serve as the backbone of any organization. They express the company's main beliefs about what is important, right, and desirable. These values shape the organization's goals and long-term priorities. Aligning organizational culture with these values can lead to transformations in areas such as:

- internal communication styles (e.g., providing feedback, presence of coaching conversations) and external communication,
- management styles,
- broadly understood work atmosphere (presence of empathy, understanding of emotions, and management of those emotions),
- creating a developmental environment,
- employee competencies, their expansion or tapping into market talents,
- implementing principles of sustainable development and human-centred organization,
- business strategy.
  https://www.impactinternational.com/pl/blog/zarzadzanie-przez-wartosci-jak-budowac-kulture-organizacyjna-poprzez-wartosci.

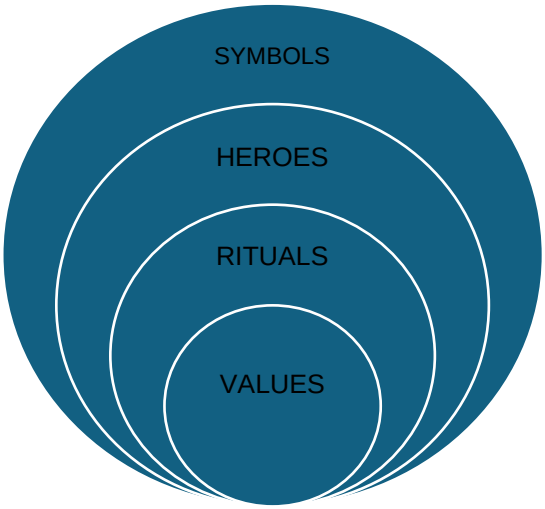
Organizational culture can serve many functions, thereby supporting the achievement of various goals. Below are three fundamental functions (Skalik, 2001):

- An integrative function – the process of forming organizational culture is akin to forming a group; organizational culture acts as a kind of "glue" that holds the institution together.
- A perceptual function – it enables the perception of the environment and understanding the meaning of the reality in which the organization operates.
- An adaptive function – it reduces uncertainty and allows for stabilizing reality by utilizing established response patterns.

Organizational culture has a significant impact on the unity, cohesion, and collaboration of the individuals employed within it, as well as on the overall atmosphere in the workplace (Pawłowski *et al.*, 2019). The key elements that comprise organizational culture are presented in Figure 1.

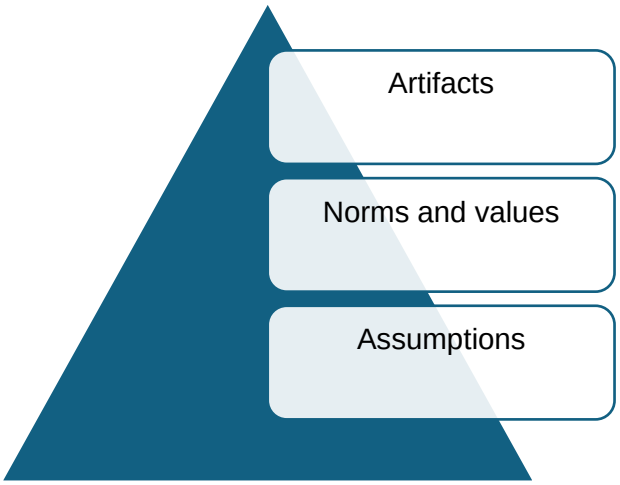
In the context of security management, values such as responsibility, trust, integrity, collaboration, and care for employees are crucial (Serafin, 2015, p. 91). It is based on these values that employees make decisions and carry out their responsibilities, which affects the effectiveness of security systems. Organizational culture can be divided into three levels, which are illustrated in Figure 2.

Figure 1. *Manifestations of culture at different levels of depth*



Source: *Michalski, 2017.*

Figure 2. *Levels of Organisational Culture*



Source: Gitling, 2013.

An important element is the norms and rules that serve as unwritten guidelines governing the daily behaviours of employees. These norms can both support adherence to formal procedures and influence attitudes toward security and risk management. In practice, they include safety-related norms, such as reporting incidents and following procedures, as well as norms for collaboration between teams, which can facilitate the exchange of information about potential threats.

Artifacts and symbols represent visible manifestations of organizational culture that are easily recognizable to employees and outsiders alike. Artifacts can be categorized into:

- Cultural – this refers to the language used by members of the organization, as well as the myths and legends that are passed down among employees.
- Behavioural – these pertain to the rituals, ceremonies, customs, and celebrations that characterize the organization.
- Physical – this encompasses everything that is "material," such as technology, the interior design of the company, art, furniture, and employee attire (Szmurło, 2013).

In the context of security, these artifacts may take the form of posters, certificates, or awards given for maintaining safety in the workplace, reminding employees of the company's priorities and reinforcing its values.

Practices and rituals are the daily actions and procedures that support the functioning of the organization. These include regular safety training, risk assessment meetings, and team-building activities aimed at fostering trust among employees. Such rituals significantly influence the atmosphere within the company and the way security-related strategies are implemented.

Communication plays a crucial role in shaping organizational culture, determining how values, norms, and rules are conveyed among employees. It is also vital for effectively managing information related to threats, risks, or incidents. Open and transparent communication enables quick responses to potential issues and creates a foundation for a safety culture. In contemporary management, effective, empathetic communication is perceived as a sine qua non condition for proper ethical relations in any organization.

Employees' attitudes and beliefs are a reflection of the prevailing values and norms within the organization. Organizational culture directly impacts how employees think about safety, perceive their responsibilities, and make decisions in crisis situations. In organizations with a strong safety culture, employees view safety as an integral part of their professional role.

Leadership is a key element that shapes organizational culture. Leaders serve as role models and have a significant influence on how important safety is in the daily operations of companies; therefore, they often become exemplars for other members of the organization (Avery, 2009).

Good leadership fosters a culture where safety is prioritized, and leaders actively engage in initiatives aimed at improving it by providing employees with appropriate resources and support.

The final element of the model is organizational structure, which can influence organizational culture, particularly concerning safety. Hierarchical structures may promote a more formal approach to safety management, while flat structures facilitate faster information flow and greater accountability at every level of the organization. In terms of safety, organizational structure can determine how decentralized decisions regarding this area are made, allowing for quicker responses and increased team accountability. Strategy and structure are essential for business development, but organizational culture is critically important (Machaczka, 2010).

In summary, the model of organizational culture can be divided into eight main areas: values, norms, artifacts, practices, communication, attitudes, leadership, and organizational structure.

These elements interconnect to create a unique identity for the organization and influence its effectiveness, including safety management. For organizational culture to effectively support safety management, it is crucial that values such as responsibility, integrity, and transparency are fully embraced by both leaders and employees at all levels of the organization.

3. Security Management in Contemporary Organizations

Security management in modern organizations is an essential process that encompasses a wide range of activities aimed at protecting resources, data, and ensuring business continuity. In the face of rapidly changing technologies, increasing cyber threats, and legal regulations, organizations must develop comprehensive protection strategies.

Information security is one of the key elements of security management within an organization. Its goal is to protect data from unauthorized access, theft, destruction, or alteration. An example of good practice in this area is the creation and implementation of an information security policy that defines the principles and procedures related to data processing.

Environmental uncertainty positively influences the need for greater innovation, which increases dependence on IT, thereby making the effectiveness of organizational factors more desirable (Chang and Ho, 2006). Access management is also a critical tool for protection, ensuring that only authorized individuals have access to sensitive information.

In addition to protecting digital resources, it is also important to secure physical assets such as buildings, equipment, and documents. This includes controlling access to facilities, surveillance systems (CCTV), and fire safety procedures. Modern alarm systems and integrated building management technologies help minimize the risk of data loss and the loss of physical assets.

Cybersecurity plays an increasingly important role in organizational security management, especially in light of the rise in cyberattacks. Companies employ advanced protection systems such as firewalls, antivirus software, and intrusion detection and prevention systems. Regular vulnerability management through software and system updates is also crucial to protect against new threats. Organizations implementing technologies and systems used by others are more attractive targets for cyberattacks and are also exposed to a higher degree of vulnerability (Kshetri, 2021). Employee training in cybersecurity is equally important to raise awareness about potential threats.

Risk management is the foundation for protecting organizations against potential threats (Hopkin, 2018). This process involves identifying, assessing, and developing strategies to minimize risk. Increasingly, organizations are using automated risk analysis tools that allow for quicker identification of threats and better management of operational risks.

Business Continuity Planning (BCP) is also a key element of organizational security. Well-designed contingency plans enable organizations to quickly return to full operational capacity after a crisis such as a technological failure, natural disaster, or cyberattack (Wróblewski, 2021). Activities in this area include creating data backups, developing emergency scenarios, and regularly testing procedures to practically assess the effectiveness of these plans.

Security management is also associated with compliance with legal regulations such as the EU General Data Protection Regulation (GDPR). Organizations must meet legal requirements regarding personal data protection and information security, which necessitates regular audits and updates to internal procedures. Adhering to standards such as ISO/IEC 27001 allows companies to maintain a high level of security and minimize legal risks.

Modern organizations also face new challenges such as remote work and the use of cloud solutions. Working outside the office, often on employees' personal devices, creates new data protection threats. Organizations must employ tools such as virtual private networks (VPNs) and encryption technologies to ensure secure connections to corporate systems.

The development of cloud computing also necessitates appropriate safeguards regarding the protection of data stored and processed in cloud infrastructures. It is important for organizations to use certified cloud service providers and implement data protection policies that comply with regulations.

Modern technologies must be adapted for use by organizations. Their structure, operation methods, and environmental conditions in which they operate are critical (Ciekanowski *et al.*, 2024).

Security management within an organization is a process that encompasses both technological and human aspects. In today's world, where threats evolve and new challenges arise, organizations must continuously adjust their protection strategies. Understanding key areas such as cybersecurity, risk management, business continuity, and regulatory compliance enables companies to operate effectively even in the face of potential threats.

4. Organizational Culture and Security

The role of organizational culture in management is primarily considered in relation to the extent of its prevalence and entrenchment (discussing strong and weak organizational cultures) and the functions it serves within an organization (Wojtowicz, 2004).

In security management, organizational culture plays a crucial role. It encompasses a set of values, norms, principles, and behavioural patterns that shape how members of the organization approach their responsibilities and collaborate with one another. When organizational culture is appropriately shaped with a focus on security, it supports preventive actions, encourages adherence to protective policies, and increases awareness of threats among employees. Below, we outline how organizational culture influences the security of an organization.

A safety-promoting organizational culture encourages all employees to be aware of the risks associated with security breaches, both physical and digital. In such a culture, every employee understands that they have an impact on the organization's security. Responsibility does not rest solely with IT departments or risk management teams but with every team member.

For example, this includes adhering to procedures related to personal data protection and responding appropriately to suspicious situations. The table below presents the key elements of organizational culture concerning security.

Table 1. *Key elements of organisational culture in the scope of security*

Element	Description
1. Awareness of threats and responsibility	Promoting awareness of threats and responsibility for security at all levels of the organization, including every employee.
2. The significance of leaders and communication	Leaders as role models for adhering to safety principles; open communication about threats and preventive measures.
3. Safe behaviour as a norm	Adhering to safety procedures becomes an organizational standard, which minimizes the risk of accidental breaches.
4. Participation in decision-making processes	Involving employees in decision-making processes related to security, which increases their engagement and accountability.

5. Training and development	Regular training on threats and incident response exercises enhances employees' skills.
6. Encouraging to report incidents	Creating an environment where employees can report potential breaches and security incidents without fear.
7. Minimizing internal threats	Safety culture reduces the risk of internal threats through employee education and adherence to guidelines.
8. Building trust and resilience	Organizations with a strong safety culture build trust among customers and business partners and are more resilient to threats.
9. Examples of security in practice	Daily implementation of security tools and principles, such as two-factor authentication and data encryption, reduces the risk of incidents.

Source: *Own elaboration.*

In an organizational culture centred around safety, leaders play a critical role by setting an example and shaping employee attitudes. Leaders should not only adhere to safety rules themselves but also actively promote these rules in daily operations. Communication is also key—open dialogue about risks and preventive measures enhances awareness within the organization and builds trust.

In a robust organizational culture that prioritizes safety, adherence to data protection protocols and security procedures becomes a social norm. This means employees instinctively follow security guidelines, such as regularly changing passwords, encrypting confidential data, or exercising caution when interacting with suspicious information sources (e.g., phishing emails).

A strong culture fosters better (or optimal) ways of thinking, feeling, and responding, which can assist managers in making decisions and organizing the organization's activities. A successful organization should cultivate strong cultures that attract, retain, and reward individuals for performing their roles and achieving objectives (Sun, 2008). This makes the organization less susceptible to accidental security breaches.

In a safety-first organizational culture, employees are involved in decision-making processes regarding the protection of data and resources. This not only increases their sense of responsibility for security but also helps them recognize how their actions contribute to the protection of the entire organization. Fostering a collaborative culture in this regard strengthens employee engagement and loyalty.

A crucial element of a safety culture is regular training, which helps employees identify threats and respond to them appropriately. Organizations that emphasize continuous improvement in security elevate the competency levels of their employees, leading to a reduction in human errors, which are often the source of security breaches.

Regular exercises, such as security incident simulations, raise awareness and enhance crisis management skills. An organizational culture that supports safety encourages openness in reporting potential breaches. Employees are encouraged to promptly report incidents without fear of repercussions if the error was unintentional. Properly responding to incidents and learning from them is critical to building organizational resilience.

5. Minimizing Internal Threats

One of the biggest challenges in security is internal threats—employee actions that may expose the organization to risks. A well-developed safety culture helps minimize such risks because employees are aware of the consequences of their actions and comply with established procedures. Examples of internal threats include unintentional mistakes, such as clicking on a suspicious link, or deliberate actions, such as leaking confidential information externally.

A safety-oriented organizational culture builds trust not only within the organization but also in relationships with customers and business partners. Organizations that prioritize data protection become more credible, which can attract new customers and partners, particularly in regulated industries where compliance with security regulations is critical. Furthermore, such companies are more resilient to threats because their employees are better prepared to act in crisis situations.

Best security practices in organizations arise from the consistent application of rules. Employees must understand that their personal actions impact the overall security of the organization. By implementing tools such as two-factor authentication, data encryption, or stringent access controls, companies can effectively reduce the risk of incidents.

Organizational culture has a direct impact on the level of security within an organization. By promoting appropriate values, attitudes, and behaviours, organizations can strengthen their defences against both external and internal threats. Leaders play a crucial role in shaping the security culture, and employees must be regularly educated on best protection practices. With a coherent approach to security management in the context of organizational culture, companies can effectively mitigate risk and build trust.

6. Conclusion

Organizational culture plays a pivotal role in managing an organization’s security, as it directly influences employee attitudes, behaviours, and engagement in protecting against threats. In the face of a rapidly changing business environment and the increasing number of both physical and digital threats, organizations must place particular emphasis on cultivating a culture that promotes safety.

Organizational culture influences employees' daily decisions and actions, and by adhering to prevailing norms and values, they can help reduce the number of incidents by increasing awareness and responsibility for collective security. Moreover, the role of leaders in this process is invaluable—their attitudes and commitment to fostering a positive security culture impact employee trust and willingness to follow procedures.

Internal communication is equally important in building an effective security culture. Efficient information exchange, clear communication of policies, and open communication channels between management and employees contribute to an effective response to any threats. At the same time, the organization must be adaptable to changes, which are an inherent part of modern business. A flexible organizational culture allows for better responses to new challenges, such as changes in legal regulations, the development of new technologies, or cybersecurity threats.

A key element of effective security management is the engagement of the entire organization. It is not sufficient for security responsibility to rest solely on formal regulations—every employee, at every level, must feel responsible for the organization's safety. Therefore, it is essential that the security culture is actively promoted and supported by leaders.

In summary, organizational culture and security strategy must be closely integrated, forming a cohesive security management system. Without a strong, supportive organizational culture, even the best security strategies may prove ineffective. A crucial element in this process is also the continuous training of employees, ensuring they remain updated on current threats and ways to avoid them. Moreover, organizational culture must evolve in response to emerging threats, requiring flexibility and the ability to adapt to new conditions.

Managing security within the context of organizational culture is a complex process that requires further in-depth research. In particular, attention should be paid to the impact of new technologies, such as artificial intelligence or automation, on security culture in organizations. These technologies may introduce new challenges, forcing organizations to transform their approaches to security management.

Another significant area requiring further analysis is the cultural diversity in approaches to security. International organizations must consider cultural differences, raising questions about whether there are universal principles of security management or if each organization must tailor its actions to the specifics of local markets.

Additionally, the relationship between security culture and innovation is an intriguing area for future study. Contemporary organizations must find a way to balance the need for innovation with maintaining a high level of security. A critical

question remains how a security culture can support, rather than hinder, innovation within an organization.

In conclusion, managing security in the context of organizational culture is a complex process that requires further research and analysis to fully understand the dynamics and influence of culture on organizational security.

References:

Avery, G.C. 2009. Przywództwo w organizacji. PWE, Warszawa.

Bratnicka, K. 2010. Kultura organizacyjna i twórczość w przedsiębiorczych organizacjach – model koncepcyjny. Przegląd organizacji, nr 11, 850.

Ciekanowski, M., Żurawski, S., Pauliuchuk, Y., Ciekanowski, Z., Marciniak, S. 2024. Strategies for Effective Cybersecurity Management in Organizations. European Research Studies Journal, Volume XXVII, Issue 1.

Ernest Chang, S., Ho, C.B. 2006. Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, Vol. 106, No. 3.

Hopkin, P. 2018. Fundamentals of risk management: understanding, evaluating and implementing effective risk management. Kogan Page Limited.

Gitling, M. 2013. Człowiek w organizacji: ludzie, struktury, organizacje. Diffin, Warszawa.

Kshetri, N. 2021. Cybersecurity management: An organizational and strategic approach. University of Toronto Press, Toronto Buffalo London.

Skalik, J. 2001. Organizacja i zarządzanie. Wyższa Szkoła Zarządzania i Finansów we Wrocławiu, nr 124, Wrocław.

Pawłowski, M., Kułakowska, A., Piątkowski, Z. 2019. Kultura organizacyjna w organizacji. Postępy techniki przetwórstwa spożywczego, nr. 1.

Serafin, K. 2015. Kultura organizacyjna jako element wspierający realizację strategii przedsiębiorstwa. Studia Ekonomiczne Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach, nr. 222.

Sun, S. 2008. Organizational Culture and Its Themes. International Journal of Business and Management, vol. 3, no. 12.

Szmurło, A. 2013. Kultura organizacyjna jako czynnik wpływający na funkcjonowanie przedsiębiorstwa. Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie, nr. 99.

Machaczka, M. 2010. Kultura organizacji w zarządzaniu wiedzą. Ekonomiczne Problemy Usług, nr. 57.

Wojtowicz, A. 2004. Kultura organizacyjna a proces zarządzania strategicznego. Zeszyty Naukowe Małopolskie Wyższej Szkoły Ekonomicznej w Tarnowie, nr. 6.

Wróblewski, R. 2021. Zarządzanie ryzykiem w przedsiębiorstwie. Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie, no. 17.

Zarządzanie przez wartości. Jak budować kulturę organizacyjną poprzez wartości. https://www.impactinternational.com/pl/blog/zarzadzanie-przez-wartosci-jak-budowac-kulture-organizacyjna-poprzez-wartosci.