DOI: 10.2478/orga-2026-0026

Security Culture as a Foundation for Data Security in Organizations: A Conceptual Framework

Krešimir FILEŠ[1], Gordan AKRAP[2]

[1] University of Maribor, Faculty of Organizational Sciences, Kranj, Slovenia, kresimir.files@gmail.com

[2] Dr. Franjo Tudjman Defense and Security University, Zagreb, Croatia, gordan.akrap@sois-ft.hr

Background/Purpose: Organizations increasingly depend on operating in digital environments, where planning and implementing technical security and protective measures alone is not a sufficient prerequisite for business effectiveness. The aim of this paper is to clarify the concept of security culture and to explain how it emerges and functions in organizations.
Methods: The paper develops a conceptual framework through a theory-driven synthesis of selected literature on organizational culture, socio-technical systems and organizational behavior.
Results: Security culture is defined as a domain-specific pattern of shared assumptions, norms and coordinated practices through which organizational members accept and implement security requirements, establish priorities for action and fulfill security responsibilities. Security culture is distinct from organizational culture, occupational safety culture, compliance culture and security climate.
Conclusion: Security culture does not replace technical security measures and controls; it mediates between formal technical controls and everyday behavior. Five mechanisms through which security culture is enacted are identified, and a three-level (strategic, operational and tactical) framework is proposed, describing distinct functions that must be aligned into a coherent whole. Six propositions for future empirical research are derived from the framework.

Keywords: Security culture, Data security, Organizational culture, Socio-technical systems, Organizational behavior, Cybersecurity, Digital organizations

1 Introduction

1.1 Background and Problem Statement

Planning and implementing technical security and protective measures alone is not a sufficient prerequisite for achieving an efficient working environment in organizations. Security culture is an important organizational factor. As a set of values, ways of thinking and recommendations on security and protection issues, it should indicate clearly and unambiguously to employees why they should adhere to the prescribed rules and procedures and how to build shared responsibility and a sense of belonging to their organization. Security culture must explain why security and protection rules and procedures are established, how they are implemented in individual organizations, how protection mechanisms and systems are built into working practices and how members of the organization are educated about which security behavior is expected, evaluated and practically possible.

The concept of security culture is often used in the literature on cybersecurity and information security management (Alshaikh, 2020; Dornheim & Zarnekow, 2024;

Received: 30th April 2026; Accepted: 19th October 2026

Sutton & Tompson, 2025; Uchendu et al., 2021), but it remains theoretically underdeveloped. Security culture is often interpreted as a general security attitude that covers activities to raise employees' security awareness, the quality of training and the requirement to comply with system rules. Such use creates several problems. The key problem is that the concept of security culture becomes difficult to separate from organizational culture, occupational safety culture and compliance culture.

Organizations increasingly depend on operating in a demanding digital space. Organizations collect, process, transfer, interpret and reuse data and information, both within their own processes and with external stakeholders. Examples from practice show that extensive access to such data can also be held by employees whose formal positions seem routine, but whose approach to and understanding of security and organizational culture can have extremely harmful consequences for the functioning of the system, at both the tactical and the strategic level.

The need to preserve the security, protection and integrity of data is often described in technical terms (technical controls): access control, encryption, monitoring, incident response and network defense. These measures are necessary but insufficient. In organizations, data security is essentially ensured by people who make sure that easily overlooked rules and procedures are followed, who often act under different forms of pressure and who may have personal problems that they do not share with the organization. These factors can significantly affect whether they comply with security rules and treat security as a common responsibility, and not only as a task of the organizational unit that deals primarily with security. For this reason, the concept of security culture requires an organizational, rather than a purely technical, explanation.

The central problem explored in this paper is conceptual in nature. Security culture is often referred to as something that organizations should have. If security culture is just another indicator for achieving positive results, it is difficult to distinguish it from organizational culture, occupational safety culture or compliance culture. It also becomes difficult to explain how security culture is created, how it is maintained and how it shapes behavior in jobs and work environments that are intensively shaped by new, primarily digital, technology.

This paper therefore reconceptualizes security culture as a specific organizational construct. It does not present it as an empirical finding derived from case study research, nor does it treat it as a hypothesis. Instead, the paper develops a conceptual framework based on established theories of organizational culture, socio-technical systems and organizational behavior. This is important because security culture can only be useful for organizational research if its theoretical boundaries, mechanisms and levels of analysis are explicitly defined.

1.2 Aim, Conceptual Questions, and Contribution

The aim of this paper is to clarify the concept of security culture and to explain how it acts as an organizational phenomenon in organizations operating in digital environments, and how organizations can use it indirectly to develop and strengthen their business capabilities. The paper addresses three conceptual questions: (1) How can security culture be grounded in established organizational and socio-technical theories? (2) What makes security culture different from related constructs such as organizational culture, occupational safety culture, compliance culture and security climate? (3) Through which organizational mechanisms does security culture affect security behavior and data security outcomes?

The contribution of this paper is conceptual, not empirical. The paper explains what security culture is, differentiates it from related constructs and proposes a multi-level framework for analyzing how security culture is created and how it functions in digital organizations. It grounds security culture in organizational culture theory and socio-technical systems theory, specifies the boundaries of the construct and separates it from neighboring concepts. It also develops a three-level framework that connects strategic orientation, operational implementation and tactical realization in practice. The framework is intended for conceptual clarification and future empirical research; it does not claim that certain incidents are causally explained by this analysis.

A new framework is needed because existing frameworks of information security culture and cybersecurity culture were developed mainly for description and assessment. Van Niekerk and von Solms (2010) extended Schein's model with information security knowledge, Da Veiga and Eloff (2010) proposed a framework and an assessment instrument, and AlHogail (2015) developed and validated a framework of cultural dimensions, while more recent studies address practices, maturity and the culture-behavior link (Alshaikh, 2020; Dornheim & Zarnekow, 2024; Sutton & Tompson, 2025; Uchendu et al., 2021). These works describe what security culture consists of and how it can be measured, but explain less clearly how culture connects formal controls with everyday behavior and at which organizational levels this happens. This paper adds three elements: explicit boundaries of the construct, five mechanisms of cultural mediation derived from the integration of organizational culture and socio-technical systems theory, and a three-level structure in which misalignment between levels weakens security culture. These elements lead to testable propositions.

The central claim of this paper is that security culture functions as a domain-specific cultural system that pro-

vides organizational meaning for data security and information management. It combines formal rules, technical controls, leadership expectations, responsibilities of different roles and the experience of daily practice. In this sense, security culture is the cornerstone of the security of business processes and data because it creates a framework in which different protection mechanisms are understood and integrated into a coherent whole that employees need to understand, consider reliable, use, review and improve.

Because terminological precision is essential in a conceptual paper, the key terms are used as follows. Information security refers to the protection of the confidentiality, integrity and availability of information in any form, and data security to the protection of organizational data, primarily in digital systems, as the part of information security on which this paper focuses. Security refers to protection against deliberate and accidental threats, while safety refers to the prevention of accidental harm to people and physical assets, as in occupational safety; the paper therefore speaks of secure, not safe, behavior. This paper draws on the research traditions of information security culture and cybersecurity culture, integrating them under the broader conceptual framework of security culture. Security climate refers to shared perceptions of current security priorities and practices, and psychological safety to a shared belief that it is safe to take interpersonal risks, such as reporting an error (Edmondson, 1999).

2 Literature Review and Theoretical Background

As this is a conceptual paper, the literature was not reviewed systematically; sources were selected purposively, according to their theoretical relevance, and the selection procedure is documented for transparency (see Section 3.2). The selection focused on four related streams of literature: organizational culture, socio-technical systems, organizational behavior and security compliance, and management and organizational design. Table 1 summarizes the sources consulted, the key terms, the selection logic and the number of retained sources used to build the framework.

The literature review is organized around theoretical traditions. The purpose of this paper is to develop a clearer construct, not to report empirical results. Table 2 summarizes the main theoretical traditions used to build the framework.

The theoretical framework for security culture must explain both the cultural and the security-specific part of the concept. The framework combines organizational culture theory, socio-technical systems theory and behavioral approaches to organizational security, while organizational design informs the levels of analysis. These traditions are complementary. Organizational culture theory explains the shared meanings that guide organizational life. Socio-technical systems theory explains the interaction between technology and social organization.

2.1 Organizational Culture as the Parent Construct

Organizational culture theory provides the parent construct for security culture and represents the primary conceptual anchor and theoretical foundation. Schein (2010) explains culture as a pattern of shared basic assumptions that a group learns as it solves its problems of external adaptation and internal integration. Such an understanding is useful because culture is seen as something more than visible behavior. It includes assumptions that are taken for granted and affect what members of the organization perceive, how they interpret risk and which actions seem legitimate. Pettigrew (1979) similarly emphasizes symbols, language, ideology, beliefs and rituals as elements through which organizational cultures become meaningful.

Trice and Beyer (1993) describe work organizations as cultural communities in which practices, stories and rituals strengthen collective understandings. Weick (1995) adds that members act through sensemaking: they interpret ambiguous events and make them actionable. These perspectives show why security culture should not be defined merely as formal policy or employee awareness. Security culture is created when members repeatedly make sense of security responsibilities and when these interpretations are built into routines, leadership communication and everyday decisions.

Pettigrew (1979) and Trice and Beyer (1993) both emphasize the symbols, practices, rituals and meanings through which organizations produce shared interpretations. This tradition is important because it prevents security culture from being reduced to individual attitudes. Security culture is “cultural” only when security-related meanings are shared, reproduced and built into organizational practices.

Security culture is therefore conceptualized as a domain-specific expression of organizational culture. It refers to the shared assumptions and practices that guide how members of the organization handle data, accept and apply the rules and principles of security responsibility, and coordinate security-related work. Security culture remains connected to the general organizational culture but is narrower in scope because it focuses on data security, digital work, security-relevant behavior and the creation of a secure working environment.

Organizational culture theory also clarifies the role of leadership. Leaders cannot simply declare the existence of security culture. They embed culture through what they pay attention to, how they allocate resources and rewards, how they react to critical incidents and what behavior

they model (Schein, 2010), as well as by defining acceptable trade-offs and by making some interpretations more legitimate than others. Leadership is therefore a cultural mechanism and not just a source of instructions. Security culture becomes visible when leadership commitments are translated into structures, roles, routines and everyday expectations.

Table 1: Literature Selection Procedure for the Conceptual Analysis

Phase	Subphase	Criterion	Procedure
Assembling	Identification	Domain	Security culture and data security in organizations.
	Identification	Source Type	Peer-reviewed articles, scholarly books and selected official, legal or public sources used for context or illustration.
	Acquisition	Sources Consulted	Scopus, Web of Science, ScienceDirect, SpringerLink, Emerald Insight, Taylor & Francis Online, Wiley Online Library and Google Scholar. Official and legal sources were consulted for the NIST framework, the Tyan, Inc. v. Garcia case and public materials on the Manning case.
	Acquisition	Key Terms	"security culture" OR "information security culture" OR "cybersecurity culture" AND "organizational culture" OR "socio-technical systems" OR "security compliance" OR "data security" OR "governance" OR "behavior" (used as guiding terms, not as a systematic search string).
	Acquisition	Time Frame	No lower time limit was applied to foundational theory. Sources specific to information security culture and cybersecurity culture were drawn mainly from the period 2009 to 2025.
Arranging	Screening	Exclusion Criteria	Duplicates, non-English sources, insufficiently relevant or reliable sources, as well as sources that treat security culture only as awareness or training without conceptual contribution, were excluded.
	Organization	Organizational Framework	Four conceptual streams: organizational culture; socio-technical systems; organizational behavior and security compliance; and management and organizational design.
	Final Selection	Number of Sources Retained	The paper cites 38 sources: 29 peer-reviewed journal articles, 5 scholarly books, 1 official governance framework, 1 court decision and 2 public context sources.
Assessing	Evaluation	Method of Analysis	Conceptual synthesis and differentiation of constructs. Sources were retained when they defined the parent construct, clarified the boundaries, explained the mechanisms, supported the multi-level framework or illustrated the application.
	Reporting	Reporting Method	Narrative synthesis supported by tables. Table 1 documents the logic of source selection; the other tables organize theoretical traditions, construct boundaries, framework levels and propositions.

Table 2: Main Theoretical Traditions Used to Develop the Framework

Theoretical tradition	Key contribution	Role in proposed framework
Organizational culture theory	Culture is a pattern of shared assumptions, meanings, symbols and practices that direct interpretation and action.	It positions security culture as a domain-specific cultural subsystem, not as a general orientation towards security.
Socio-technical systems theory	Organizational outcomes depend on the joint design of social arrangements and technical systems.	It explains why security cannot be reduced to technology or employee awareness alone.
Research on organizational behavior and security compliance	Behavior is shaped by intentions, motivation, perceived control, leadership, policy design and social norms.	It explains how security culture becomes visible through routines, decisions and security-relevant actions.
Management and organizational design	Structures distribute authority, responsibilities, coordination and escalation duties.	It links security culture to strategic, operational and tactical levels of organizational functioning.

2.2 Socio-Technical Systems and Digitally Mediated Security Work

Socio-technical systems theory adds a second theoretical foundation. Trist and Bamforth (1951) showed that technical change alters social relations, work roles and responsibilities. Cherns (1976) later formulated the principles of socio-technical design, including the idea that work systems should be designed taking into account both technical and social requirements. Baxter and Sommerville (2011) applied this tradition to systems engineering and argued that technical systems should be understood together with the organizational context in which they operate.

This tradition is directly relevant to data security. Security technologies do not operate in isolation. They are configured, interpreted, bypassed, supervised and maintained by people working within particular structures of authority and responsibility. A password policy is also a social practice that depends on usability, workload, trust, implementation, norms and system expectations. A security monitoring tool changes what is visible and what can be reported, and it helps distribute and attribute responsibilities. This means that technical controls cannot be evaluated independently of the work system in which they are used. Access control, monitoring, authentication, data classification and incident reporting are technical and procedural arrangements, but they also distribute responsibility, shape discretion, change power relations and influence workflow.

Security culture mediates the relationship between technology and work practices. It shapes how employees apply security rules, how they react when these rules conflict with task requirements, and whether they report weaknesses and see security as part of their role or as an external burden imposed by experts. Security culture therefore emerges at the intersection of social and technical arrangements. It shapes the way in which technologies distribute access, the way in which structures distribute responsibility and the way members learn what is expected when security conflicts with speed, practicality or workarounds.

This socio-technical conceptualization prevents the concept from becoming an exclusively moral appeal to employees and instead treats it as part of organizational design. It also explains why security failures cannot automatically be attributed to individual negligence or poor character. A security incident can reflect inadequate role design, conflicting motivations, poorly integrated technology, unclear roles and authority, weak reporting channels or discrepancies between formal policy and everyday work. The analysis of security culture raises the question of how the organizational system makes certain behaviors meaningful, likely or difficult.

2.3 Distinguishing Security Culture from Related Constructs

Security culture overlaps with several established constructs but should not be considered identical to any of them.

Comparing occupational safety culture and security culture is useful because both include risk, routines, leadership and reporting. However, occupational safety culture was developed primarily around the prevention of harm in physical, operational and high-risk work systems. Guldenmund (2000), Cooper (2000) and Reason (1997) show that occupational safety culture focuses on how organizations understand and manage accident risk. Security culture, in contrast, includes confidentiality, integrity, availability, access control, insider risk and adversarial, including competitive, threats. It may include accidental behavior, but it also includes deliberate misuse and contested interpretations of secrecy, disclosure and accountability.

Compliance culture is also related to, but not identical with, security culture. Compliance culture emphasizes adherence to laws, rules, policies and control systems. Interligi (2010) and Weaver et al. (1999) show that compliance depends on formal systems, leadership commitment and an ethical infrastructure. Security culture includes compliance but is broader, because secure behavior requires interpretation, judgment, escalation and adaptation in situations that are not fully defined. Employees can formally adhere to rules and yet use insecure workarounds, or they may have to act securely when the policy is unclear.

Security culture also differs from security climate. Climate usually refers to shared perceptions of current practices, priorities and expectations. Schneider et al. (2013) distinguish climate from deeper cultural assumptions. In this paper, security climate is treated as a more visible and potentially measurable surface expression of security culture. Climate indicators can help in assessing security culture, but they do not capture the whole construct.

Research on information security culture and cybersecurity culture provides the closest domain-specific literature. Da Veiga and Eloff (2010) proposed a framework and an instrument for assessing information security culture, while Van Niekerk and von Solms (2010) emphasized the management perspective. AlHogail (2015) developed and validated an information security culture framework, and Da Veiga et al. (2020) clarified how academia and industry define the construct. More recent studies extend the field by linking cybersecurity culture to behavior, organizational practice and maturity (Alshaikh, 2020; Dornheim & Zarnekow, 2024; Sutton & Tompson, 2025; Uchendu et al., 2021). This paper builds on these definitions and dimensions, but focuses on the mechanisms and organiza-

tional levels through which security culture links controls with behavior. Table 3 presents the conceptual boundaries adopted in this paper.

2.4 Behavioral Foundations of Security Culture

Behavioral approaches explain how individuals and groups enact security culture in practice. Behavioral factors are conceptualized here as individual-level conditions through which culture is enacted. Motivation affects whether employees will invest effort in secure behavior; responsibility affects whether they see data protection as part of their role; satisfaction and perceived support affect whether they identify with organizational goals and whether they are willing to report problems or participate in improvements.

Security culture becomes visible through behavior, but behavior should not be treated as an indicator without theory. Behavioral approaches help explain how culture is translated into action. Ajzen's (1991) theory of planned behavior suggests that action is affected by attitudes, subjective norms and perceived behavioral control. In the security context, this means that employees are more likely to act securely when they believe that secure conduct is important, when colleagues and leaders expect it and when systems make secure behavior feasible.

Security compliance studies extend this view. Herath and Rao (2009) explain policy compliance through protection motivation and deterrence. Hu et al. (2012) show the importance of top management and organizational culture for employees' compliance with security policies. Siponen et al. (2014) and Moody et al. (2018) further stress that adherence to policies depends on motivation, normative beliefs, habits and organizational conditions. A recent review also points out that human factors in cybersecurity require an interdisciplinary approach and cannot be reduced to awareness training (Khadka & Ullah, 2025), while qualitative evidence shows that knowledge of cyber risks is often present, but no one assumes responsibility for secure behavior (Aschwanden et al., 2024).

In this paper, motivation, responsibility and satisfaction are not treated as direct findings resulting from incidents. They are conceptualized as individual-level conditions through which security culture can affect behavior. Deci and Ryan (2000) show that motivation depends partly on autonomy, competence and relatedness. Edmondson (1999) shows that psychological safety supports learning behavior in teams. In security work these conditions are important because members have to report errors, ask questions, challenge insecure practices and accept responsibility for data management decisions.

Security culture therefore operates through collective and individual mechanisms. At the collective level, it establishes shared norms on what is considered responsible behavior towards the organization and its data, and at the individual level it affects whether employees experience security as meaningful, legitimate and feasible. Motivation, responsibility and satisfaction are best understood as bridges between cultural expectations and behaviors carried out in practice.

3 Methods

3.1 Conceptual Research Design

The main contribution of this conceptual paper is to clarify the construct, integrate the literature and develop propositions for future research. Whetten (1989) argues that a theoretical contribution requires attention to what concepts are involved, how they are related, why they are related and under what conditions they apply. Jaakkola (2020) and Gilson and Goldberg (2015) similarly stress that conceptual articles can contribute by distinguishing constructs, organizing fragmented knowledge and proposing new explanatory frameworks. Of the four types of conceptual articles described by Jaakkola (2020), this paper follows the model type, which builds a framework of relationships between constructs and expresses them as testable propositions.

Table 3: Conceptual Boundaries of Security Culture

Construct	Core focus	Boundary in relation to security culture
Organizational culture	Shared assumptions, values, meanings and practices in the organization.	Security culture is a domain-specific subsystem of organizational culture.
Occupational safety culture	Prevention of accidents and harm, often in physical or operational high-risk systems.	Security culture includes digital assets, data, access, adversarial threats and insider risks.
Compliance culture	Adherence to formal rules, laws, policies and control systems.	Security culture includes compliance, but also judgment, escalation, interpretation and informal norms.
Security climate	Current shared perceptions of security priorities and practices.	Security climate is a visible expression of security culture, not the entire construct.

The methodological logic is therefore theory building, not empirical testing. The paper gradually identifies relevant theoretical traditions, compares adjacent constructs, defines security culture and formulates propositions. Such design seeks to respond to the conceptual problem: the need for security culture to be explained as a specific organizational phenomenon, not as a general normative orientation.

3.2 Literature Selection and Analytical Procedure

The literature was selected purposively, on the basis of theoretical relevance, and not through a systematic review protocol. In line with Jaakkola (2020), the selection of theories was guided by their capacity to explain the phenomenon, and a source was retained when it defined the parent construct, clarified construct boundaries, explained a mechanism, supported the multi-level framework or illustrated its application (Table 1). The conceptual analysis uses three groups of sources. The first group consists of foundational organizational and socio-technical theories, including organizational culture, sensemaking, socio-technical design and organizational structure. The second group comprises research on information security culture and cybersecurity behavior. The third group comprises selected sources on governance and security practice that help link the conceptual argument with contemporary work on data security.

The analysis process followed four steps. First, organizational culture was identified as the parent construct and selected the theoretical elements relevant for data security behavior. Second, security culture was compared with organizational culture, occupational safety culture, compliance culture and security climate. Third, the mechanisms that link culture with behavior were derived. A mechanism was retained if it was grounded in at least one of the theoretical traditions in Table 2, linked formal controls with everyday behavior and was conceptually distinct from the other mechanisms; this resulted in five mechanisms (Section 4.2). Fourth, the mechanisms were organized into strategic, operational and tactical levels, and propositions were formulated for future empirical research.

3.3 Use of Analytical Illustrations

Two public incidents are used as illustrative vignettes: the civil dispute Tyan, Inc. v. Garcia and the public case of Chelsea Manning. They were selected for theoretical reasons, as contrasting cases. Both involve insiders with access to sensitive data, the situation in which the relationship between formal position, access and responsibility, central to the framework, becomes visible. They differ in organizational setting and type of threat: a private company and the misuse of proprietary information on the one hand, and a strongly hierarchical military organization and a contested disclosure of classified information on the other. The vignettes therefore illustrate different mechanisms and levels of the framework (Section 4.4). This paper does not draw conclusions about psychological motives, satisfaction or responsibilities as empirical facts beyond what is available in public sources. This restriction is introduced deliberately. Public media reports, court documents and biographical sources are not sufficient to establish with scientific certainty an internal organizational culture or individual motivation. In this paper, the analytical illustrations help readers understand the concepts, while the validity of the framework rests on theoretical integration and future empirical testing.

4 Results: A Conceptual Framework of Security Culture

4.1 Definition and Construct Boundaries

The proposed definition is that security culture is a domain-specific pattern of shared assumptions, norms and coordinated practices through which members of the organization accept and implement security requirements, establish priorities for action and carry out responsibilities in the field of organizational and data security. This definition contains four elements. First, security culture is domain-specific because it refers to data, systems, access, confidentiality, integrity, availability and decisions that are relevant for security. Second, security culture includes shared assumptions, as organizational members develop taken-for-granted beliefs about what constitutes responsible behavior concerning data. Third, security culture includes norms that are implemented in practice, because culture is visible in routine behavior and not only in statements. Fourth, security culture includes coordinated practices, because security requires coordination of roles, technologies and hierarchical levels.

Security culture is distinct from organizational culture, occupational safety culture and compliance culture. Security culture is not only a favorable attitude towards security, because attitudes become organizationally meaningful only when supported by structures, rules, routines, leadership and shared expectations. Security culture is not a substitute for technical security measures and controls. Security culture and technical security measures and controls are interdependent: technical measures and controls structure behavior, and culture shapes the way technical measures and controls are interpreted and implemented in practice.

4.2 Organizational Mechanisms

The central mechanism proposed here is cultural mediation: security culture mediates between formal technical controls and everyday behavior. It does so through giving meaning through leadership, management and coordination, role design and responsibility, motivation and identification, and learning from employee voice and incident response (Figure 1).

The five mechanisms were derived from the theoretical traditions presented in Section 2. Leadership signalling follows from organizational culture theory and its account of how leaders embed culture (Schein, 2010). Structural harmonisation follows from organizational design, which explains how work is divided and coordinated (Mintzberg, 1979). Socio-technical compliance follows from socio-technical systems theory and the principle that technical and social requirements must be designed jointly (Cherns, 1976). Behavioral support follows from research on organizational behavior and security compliance (Ajzen, 1991; Herath & Rao, 2009), and meaning and identity follows from the sensemaking and team learning perspectives (Edmondson, 1999; Weick, 1995). Training and awareness campaigns are not treated as separate mechanisms, because they are instruments through which these five mechanisms operate.

The first mechanism is leadership signalling. Leaders signal whether data security is an actual organizational priority or only a formal requirement. Signals include response planning, resource allocation, role modeling, responses to incidents, attention to employees' concerns and the balance between productivity and security. Leaders influence security culture by embodying the meaning of data security, its importance and how it should be balanced with other organizational priorities. A statement that security is important will have limited strength if employees are rewarded only for speed, output or cost reduction. By contrast, management reactions to near misses, as well as to incidents that have occurred, can show whether the organization treats security as an opportunity to learn or only as a disciplinary problem. Strategic leaders provide an interpretive framework, but middle managers and direct supervisors often determine whether and how this framework will become operational. Therefore, the framework places leadership in a multi-level model instead of attributing security culture to top management only.

The second mechanism is structural harmonisation. The organizational structure distributes authority, responsibilities and coordination. Mintzberg (1979) shows that organizational design serves to divide and coordinate work. In security culture, structural harmonisation means that roles, access rights, reporting lines and escalation procedures are consistent with the security responsibilities assigned to individuals and units. Data security problems often cross functional boundaries: IT may manage infrastructure, the legal function may interpret obligations, HR may manage employee-related processes, business units may be process owners, and employees on the "first line of defense" may control the first point at which data enter the organization or are targeted. Without a shared security culture, these responsibilities can fragment. In technology-intensive environments, security culture functions as a coordination mechanism. It aligns interpretations among structural units, creates a common language of risk and helps employees understand when they need to escalate concerns. Security culture is the way organizations coordinate distributed data and technology decisions. Access rights are not only technical permissions; they are organizational distributions of trust and responsibility. When access is granted without adequate responsibility, training and feedback, organizations create a socio-technical imbalance. This mechanism is particularly important in digital organizations because employees in lower hierarchical positions can have high-impact access to technology. A front-desk worker, patrol officer, analyst, external contractor or support employee can interact with data systems in ways that affect the entire organization. The analysis of security culture therefore calls into question the assumption that organizational importance follows formal rank. It asks how power is distributed through access to data and how it is managed.

The third mechanism is socio-technical compliance. The term refers here to the fit between technical controls and work requirements, not to employees' rule-following. Technology should be usable, proportionate and consistent with workflows. If secure behavior is too slow, unclear or incompatible with work requirements, employees can create informal workarounds. A weak security culture tolerates such workarounds, while a strong one makes them a topic of discussion and correction. Security culture is also achieved through role design. Employees with access to data or systems need clear expectations of what they may and may not do, how exceptions are handled and how responsibilities change when new technologies are introduced.

The fourth mechanism is behavioral support. Security-relevant behavior is shaped by feedback, recognition, learning and consequences. Organizations should support and encourage incident reporting, responsible use of access rights, secure cooperation and learning from near misses. Motivation, responsibility and satisfaction are conceptual variables that help explain why employees internalize or reject security expectations. Motivation refers to the readiness to invest effort in secure behavior, while responsibility refers to the perception that data protection is part of one's role. Satisfaction and perceived support refer to the relationship between employees and the organization, including whether employees identify with organizational goals and whether they feel that secure behavior is acknowledged. These factors may affect security behavior in

several ways. A motivated employee is more likely to take time to check a suspicious request instead of forwarding it automatically. An employee with a strong sense of responsibility is more likely to report a misconfiguration or an incorrect access assignment. A satisfied and supported employee is more likely to express concerns through internal channels. However, these outcomes cannot be assumed. They depend on the surrounding culture, work design, leadership and the technical feasibility of secure conduct.

The fifth mechanism is meaning and identity. Security culture is stronger when employees understand why security is important for the organization, its clients, public trust and their professional identity. This is especially important in organizations where work is digitally mediated, where low-level actions, such as forwarding a file or approving access, can have organizational consequences far beyond the immediate task. The effectiveness of security culture in practice is shown by whether organizations learn from errors, both their own and those of others. Employees are often the first to see insecure workarounds, confusing policies, suspicious messages, excessive access rights or technical controls that do not correspond to the work process. A strong and applicable security culture makes the reporting of such issues legitimate. It reduces the fear that reporting errors will only lead to blame, and it creates routines through which information from incidents is converted into organizational learning. This mechanism distinguishes security culture from an exclusively disciplinary approach. Disciplinary measures may be necessary in cases of misconduct, but a security culture that relies heavily on punishment can suppress reporting and hide systemic weaknesses.

The key organizational question is how to shape practices that make it likely that threats are recognized early, understood and reported, that errors and their negative consequences are corrected, and that the organization learns with the aim of preventing future incidents before the damage arises or escalates.

4.3 Three Levels of Security Culture

The proposed three-level framework translates the theoretical argument into an organizational model. The three levels of security culture are strategic, operational and tactical. They describe different functions that must be harmonised into a coherent whole. The levels follow the distinction between strategic, operational and tactical levels that is established in security studies, where the tactical level refers to the execution of tasks. In terms of organizational design, they correspond to the strategic apex, the middle line and the operating core (Mintzberg, 1979). They are organizational levels and should not be confused with Schein's (2010) levels of cultural depth (artifacts, espoused values and basic assumptions), which can be observed at each of them. Table 4 shows the organizational framework.

At the strategic level, security culture is expressed through mission, values, governance, leadership and resource allocation. This level answers the questions why security is important and what kind of security conduct the organization expects. Strategic security culture is weak when leaders treat security only as an information technology issue or when they require secure behavior but reward only speed, cost reduction or error concealment.

At the operational level, security culture is translated into processes. This level answers the questions how, when and where security expectations are implemented. It includes system design, access management, reporting systems, incident response, risk assessment, onboarding, offboarding and coordination between business and technology functions. The operational level is where many cultural contradictions become visible, as formal security messages must be reconciled with workloads, usability and management priorities.

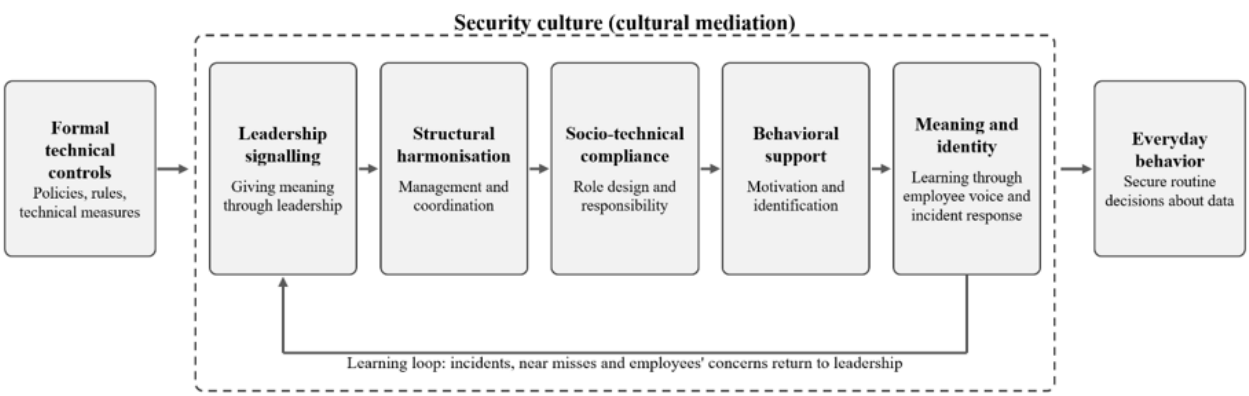


Figure 1: Five Organizational Mechanisms of Security Culture Mediation
Source: Authors

Table 4: Three-Level Security Culture Framework

Strategic level	Direction and legitimacy	Defines the purpose of security, values, priorities, management expectations and acceptable risk. Top leadership carries this level.
Operational level	Translation and coordination	Turns strategy into policies, workflows, training, access processes, monitoring routines and escalation routes. Middle management and security functions carry this level.
Tactical level	Realization and feedback	Performs secure work in everyday tasks: data handling, reporting, use of access, cooperation and local problem solving. Teams and employees carry this level.

Table 5: The Three Levels of Security Culture as Organizational Processes

Level	Organizational roles	Cultural function	Visible processes and analytical questions
Strategic level	Owners, board members, senior executive managers and top-level security management	It defines security as part of organizational identity, risk appetite, mission, values and governance, establishing the assumptions that make security legitimate.	How are security priorities determined? Are resources, incentives and responsibility consistent with security claims? How do leaders respond to incidents and to trade-offs between speed, cost and protection?
Operational level	Mid-level managers, security officers, process owners, HR, legal department, IT and data management functions	It translates strategic meanings into organizational arrangements. It integrates security into workflows, roles, training, access management, monitoring and incident-related processes.	Are policies implemented in daily tasks? Are roles clear? Are technical controls integrated with workflows? Are there feedback channels, escalation routes and learning routines?
Tactical level	Teams, first-line employees, external contractors and users with access to data or systems	It achieves security in everyday work. It produces local norms on login, authentication, data handling, exception handling and workarounds.	Do employees see security as part of their role? Can they report errors or suspicious events? Do peer norms support secure behavior? Are workarounds discussed and corrected instead of being hidden?

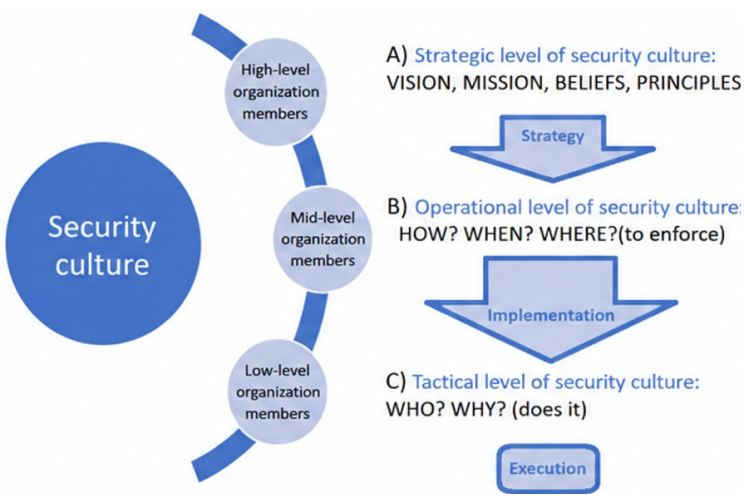


Figure 2: The Three Levels of Security Culture
Source: Authors

At the tactical level, security culture is achieved in everyday behavior. This level answers the questions of who performs security-relevant actions and why these actions make sense to members. It includes routine decisions such as checking requests, protecting credentials, classifying information, reporting anomalies, avoiding unauthorized tools and challenging insecure practices. Tactical security culture is a collective performance within local teams and workflows.

The learning loop is key. Security culture is continuously checked and supplemented on the basis of lessons learned. Digital organizations face changing threats, technologies and working arrangements. Feedback from incidents, near misses, employee concerns and audits should return to operational and strategic levels. This is in line with contemporary cybersecurity governance, which highlights continuous risk management, roles and improvement cycles (Pascoe et al., 2024). The loop assumes continuous adaptation of the system, so that structures, processes, rules, norms, decision-making and technology can be improved.

The proposed framework treats security culture as a multi-level organizational phenomenon. The strategic level refers to assumptions, priorities and governance commitments through which senior leaders define what security means for the organization. The operational level refers to the translation of these priorities into policies, workflows, role design, access arrangements, training practices and routine incident response. The tactical level refers to achieving a secure work environment daily through local decisions, peer norms, reporting, secure use of technology and responses to ambiguity. Table 5 further describes the three levels of security culture as organizational processes, and Figure 2 summarizes them.

These levels are analytically distinct but interdependent. Strategic definitions without operational translation remain symbolic. Operational policies without tactical feasibility create workarounds. Tactical awareness without strategic support leaves employees responsible for risks they cannot control. Security culture becomes organizational when these levels are strengthened and integrated instead of contradicting each other; misalignment between them weakens security culture.

The framework also explains how the three levels are related to behavioral factors. Motivation, responsibility and satisfaction are most visible at the tactical level, but they are shaped by strategic and operational conditions. For example, employees can be motivated to protect data when they understand the purpose of technical controls, believe that security is valued and experience secure behavior as feasible within their workload and work environment. Employees can accept responsibility when role expectations, access rights and accountability mechanisms are clear, and they can be more willing to report concerns when experiencing psychological safety and fair treatment. Therefore, behavioral factors are not isolated personality traits; they are produced within organizational systems.

The distinction between security culture and occupational safety culture is particularly important. Research on occupational safety culture shows that organizational accidents often result from systemic patterns, not from isolated errors (Cooper, 2000; Reason, 1997). Security culture can learn from this tradition, but it must cover features that are specific to data security. Security threats may be either deliberate or accidental. Security work often involves intangible digital assets, distributed access, fast data mobility and the behavior of competitors. Unlike many hazards in occupational safety, data security breaches can involve actors who understand technical controls and deliberately exploit them. A framework of security culture therefore requires attention to access rights, trust, monitoring, insider threats, confidentiality and the organizational meaning of data.

The distinction from compliance culture is equally important. Compliance can produce adherence to rules, but secure behavior often requires judgment in ambiguous situations. Employees may encounter requests that appear legitimate but are misleading, workflows that create pressure to circumvent technical controls, and incidents in which rapid reporting is more valuable than strict compliance. Compliance culture asks whether rules are adhered to. Security culture asks how rules, responsibilities, technologies and working practices are understood and coordinated so that secure behavior becomes a normal part of organizational life. Figure 3 shows the framework as a diagram.

4.4 Illustrative Application

The framework can be illustrated by the two public cases introduced in Section 3.3. In the case of Tyan, Inc. v. Garcia (2017), the public court record refers to unauthorized access, manipulation of internal systems and misuse of proprietary information. From the perspective of the security culture framework, the case mainly illustrates the operational level and the mechanisms of structural harmonisation and socio-technical compliance: access rights, supervision, offboarding procedures, role expectations and managerial response need to be harmonised (Propositions P2, P3 and P6). The illustration does not allow direct conclusions about the internal culture of the organization or the psychological state of any actor.

The public case of Chelsea Manning, a junior intelligence analyst in the United States Army, illustrates a different type of question: broad access to classified information within a strongly hierarchical organization and contested interpretations of responsibility and disclosure (Davies, 2022; Ray, 2024). The case mainly illustrates the relationship between the strategic and tactical levels and the mechanisms of leadership signalling and meaning

and identity (Propositions P1, P4 and P5). Through the proposed framework, it can be used to discuss escalation channels, ethical conflict, identity, reporting norms and the relationship between hierarchical authority and data access. The case does not prove a specific security culture; it shows why security culture must include a structure that enables organization members to feel safe when reporting problems, acknowledging errors and taking responsibility, while ensuring the responsible handling of sensitive information. These illustrative examples highlight several issues addressed by the conceptual framework of security culture: the organizational significance of user behavior, the interaction between hierarchy and security in recognizing problems and errors, the limitations of technical controls when separated from actual work practices, and the potential consequences of discrepancies between role responsibilities and organizational authority. They help to specify the types of organizational questions that the framework of security culture asks: Who has access? Who is responsible? What is expected from employees when policy, ethics and hierarchy are in conflict? How do concerns escalate, and how do they de-escalate? How does the organization learn from signals before a harmful incident and what are these signals?

Such material is used sparingly and analytically: it helps to illustrate why security culture is important, but it does not prove that a particular organizational culture has caused an incident.

4.5 Conceptual Propositions

The framework leads to six propositions for future empirical research. They are not empirical hypotheses tested in this paper; they specify relationships between constructs that can be examined in future studies by surveys, interviews, archival data, incident analysis or mixed methods. Each proposition follows from the framework: P1 from leadership signalling at the strategic level, P2 from structural harmonisation as operational translation, P3 from socio-technical compliance, P4 from behavioral support and the conditions for reporting, P5 from meaning and identity and the distinction between culture and climate, and P6 from the alignment of responsibility, authority and access across levels. Table 6 shows the six conceptual propositions.

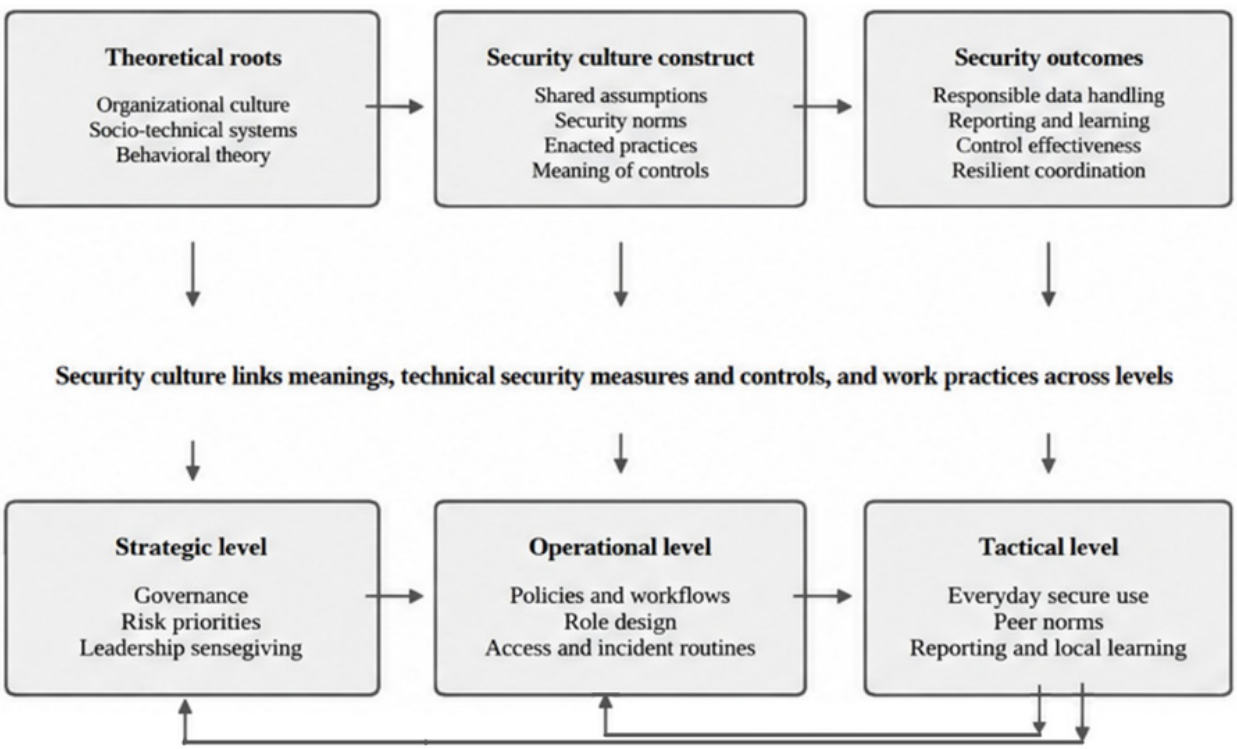


Figure 3: Security Culture as a Socio-Technical and Multi-Level Organizational Construct
Source: Authors

Table 6: Conceptual Propositions for Future Empirical Research

Proposition	Proposed relationship	Possible Empirical Indicators
P1	The more consistently senior leaders link data security to organizational purpose, governance and resource allocation, the stronger the security culture.	Communication from management, budgetary decisions, participation of executive management, visible response to incidents.
P2	Operational translation, achieved through structural harmonisation, mediates the relationship between strategic security priorities and employees' secure behavior.	Policy clarity, training relevance, access processes, escalation routines, mid-level management involvement.
P3	Socio-technical compliance (the fit between technical controls and daily workflows) is positively related to secure conduct, through higher perceived behavioral control.	Usability of technical controls, compatibility with workload, frequency of workarounds, perceived behavioral control.
P4	Psychological safety is positively related to the timely reporting of errors, anomalies and near misses; behavioral support strengthens this relationship.	Reporting rates, quality of narratives on incidents, willingness of employees to challenge insecure practices, perceived feedback and recognition.
P5	Shared meaning of data security is positively related to security climate, and security climate partially mediates the relationship between security culture and secure behavior.	Surveys of perceptions, perceived norms and local team priorities; climate consistency; observed routines.
P6	The greater the inconsistency between formal security responsibility and actual authority, access rights, training and technical design, the weaker the security culture.	Ambiguity of roles and access rights, unclear data ownership, delayed revocation of access at exit, conflicting performance objectives.

5 Discussion

5.1 Theoretical Contribution

The main theoretical contribution is to reposition security culture within specific organizational structures and to examine how it relates to problems of coordination, governance, hierarchy and decision-making. While existing frameworks mainly describe the dimensions and maturity of security culture, this framework explains how culture works, through five mechanisms of cultural mediation at three organizational levels. The security culture framework goes beyond the normative claim that organizations should address security only at a superficial procedural level. It explains security culture as a pattern of shared assumptions, norms that are implemented in practice and coordinated practices that link leadership, structure, technology and behavior. In this sense, security culture is an organizational (pre)condition that affects whether and how technical controls will be interpreted, used and improved in practice.

The paper contributes to clarifying conceptual boundaries. Security culture is linked to organizational culture because it is embedded in broader assumptions and values. It is linked to occupational safety culture because both deal with risk and learning, although with different types of risk. It is linked to compliance culture because both involve rules and responsibility. However, security culture is different because it also refers to digitally mediated data practices, access rights, confidentiality, integrity, availability, and competitive (market), internal and accidental threats.

In addition, the three-level framework contributes to organizational analysis by connecting security culture with coordination, governance, hierarchy and decision-making. It shows that security culture cannot be attributed only to technical experts or to individual employees. It requires strategic legitimacy, operational translation and tactical enactment in practice. It becomes relevant for organizational processes such as role design, management communication, (de)escalation, learning and cross-functional coordination as well as strategic and crisis communication.

For practitioners, the framework implies that interventions in security culture should not be limited to campaigns that call for caution. Organizations should examine whether security responsibilities are clear, whether technical controls are appropriate to workflows, whether employees can report errors without fear, whether managers support secure behavior under operational pressure and whether responses to incidents result in learning and not just blame. In practice, the objective is not a general moral commitment to security, but the integration of secure decisions into the daily routines and practices of organizations.

5.2 Organizational and Managerial Implications

For managers, this framework suggests that security culture should be designed, maintained and developed, and not only promoted through awareness-raising campaigns. Training is useful, but it is not enough if secure behavior conflicts with workload, incentives or the design of technical systems. Managers should therefore examine whether employees have the authority, time, tools and psychological safety necessary for secure operation.

The framework also suggests that security responsibilities should be visible at every organizational level. At the strategic level, leaders need to define why data security is important and how it relates to organizational purpose and trust. At the operational level, middle managers and security professionals need to translate this focus into clear routines and usable systems. At the tactical level, teams should be able to report problems, question insecure practices and learn from mistakes without fear that any disclosure will be treated as grounds for blame.

A practical implication is that organizations should assess security culture through multiple sources. Surveys can measure perceptions, but they need to be complemented by interviews, process reviews, incident narratives, access rights audits, training evaluations and analysis of near misses. This is necessary because security culture includes deep assumptions as well as visible routines.

5.3 Limitations and Future Research

This paper is conceptual and does not provide empirical evidence that the proposed relationships are valid in specific organizations. The illustrative examples are based on public sources and cannot support claims about internal culture, individual motives or the causal mechanisms behind security breaches. Because the literature was selected purposively rather than systematically, some relevant contributions may not have been included. The propositions therefore require empirical testing, and several research strategies are possible.

A survey could cover shared assumptions, role clarity, leadership signals, perceived support, psychological safety, responsibility and perceived consistency between technical controls and workflows. A qualitative case study could examine how the meaning of security is produced at the strategic, operational and tactical levels. Interviews, observations, internal documents, incident reports and process maps would allow researchers to trace how policies become practices. Quantitative analysis could test whether strategic leadership, operational translation and tactical enactment predict security climate and security behavior. Comparative research could examine organizations with similar technical controls but different cultural patterns, to determine how security culture affects reporting, workarounds and the use of technical controls. Such studies could also examine whether security culture works differently in public agencies, military organizations, private businesses, health care and education. It would also be useful to study how security culture changes after incidents, technology implementation, interventions or changes in leadership.

Future empirical work should also avoid treating behavioral factors as self-evident indicators. Motivation, responsibility and satisfaction should be modeled theoretically and measured in relation to role expectations, perceived control, support, justice and psychological safety. This would allow researchers to examine whether these factors mediate the relationship between organizational culture and secure behavior. Future research could also use case studies, but only if case selection, data sources and analytical procedures are clearly specified. Cases should be selected for theoretical reasons, such as variation in hierarchy, digital access, security management or incident response. Future research should also develop stronger measurement instruments. Existing approaches provide useful starting points, but they should be linked to clear theoretical dimensions such as leadership signalling, socio-technical compliance, psychological safety, reporting norms and the alignment of roles and access rights.

6 Conclusion

Security culture is often cited as a solution to data security problems. It is usable and useful only when it is theoretically grounded and has clearly established boundaries. This paper argues that security culture should be understood as a domain-specific pattern of shared assumptions, norms implemented in practice and coordinated practices through which members of organizations accept and implement security requirements, establish priorities for action and carry out responsibilities in the field of organizational and data security.

Security culture differs from organizational culture, occupational safety culture, compliance culture, security climate and security awareness, although it is connected with each of them. It works through five mechanisms at the strategic, operational and tactical levels, linking leadership, governance, role design, technical controls, motivation, responsibility, satisfaction and learning. The framework developed in this paper explains security culture through organizational culture theory, socio-technical systems theory and behavioral approaches to security, and translates this explanation into six propositions for empirical research.

The wider implication is that data security is an organizational capability. Technical measures and controls remain key, but their effectiveness depends on wheth-

er people understand them, trust them, use them, report problems with them and improve them. A strong security culture does not replace technology. It makes technology organizationally useful, behaviorally meaningful and continuously improving.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567-575. https://doi.org/10.1016/j.chb.2015.03.054

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Aschwanden, R., Messner, C., Höchli, B., & Holenweger, G. (2024). Employee behavior: The psychological gateway for cyberattacks. *Organizational Cybersecurity Journal: Practice, Process and People, 4*(1), 32-50. https://doi.org/10.1108/OCJ-02-2023-0004

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers, 23*(1), 4-17. https://doi.org/10.1016/j.intcom.2010.07.003

Cherns, A. (1976). The principles of sociotechnical design. *Human Relations, 29*(8), 783-792. https://doi.org/10.1177/001872677602900806

Cooper, M. D. (2000). Towards a model of safety culture. *Safety Science, 36*(2), 111-136. https://doi.org/10.1016/S0925-7535(00)00035-7

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture: Perspectives from academia and industry. *Computers & Security, 92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207. https://doi.org/10.1016/j.cose.2009.09.002

Davies, D. (2022, October 17). Chelsea Manning shared secrets with WikiLeaks. Now she is telling her own story. *NPR*. https://www.npr.org/2022/10/17/1129416671/chelsea-manning-wikileaks-memoir-readme

Deci, E. L., & Ryan, R. M. (2000). The "what" and "why" of goal pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry, 11*(4), 227-268. https://doi.org/10.1207/S15327965PLI1104_01

Dornheim, P., & Zarnekow, R. (2024). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information & Computer Security, 32*(2), 179-196. https://doi.org/10.1108/ICS-07-2023-0116

Edmondson, A. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly, 44*(2), 350-383. https://doi.org/10.2307/2666999

Gilson, L. L., & Goldberg, C. B. (2015). Editors' comment: So, what is a conceptual paper? *Group & Organization Management, 40*(2), 127-130. https://doi.org/10.1177/1059601115576425

Guldenmund, F. W. (2000). The nature of safety culture: A review of theory and research. *Safety Science, 34*(1-3), 215-257. https://doi.org/10.1016/S0925-7535(00)00014-X

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Interligi, L. (2010). Compliance culture: A conceptual framework. *Journal of Management & Organization, 16*(2), 235-249. https://doi.org/10.5172/jmo.16.2.235

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review, 10*(1-2), 18-26. https://doi.org/10.1007/s13162-020-00161-0

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security, 24*(3), Article 119. https://doi.org/10.1007/s10207-025-01032-0

Mintzberg, H. (1979). *The structuring of organizations: A synthesis of the research*. Prentice-Hall.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285-311. https://doi.org/10.25300/MISQ/2018/13853

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Pettigrew, A. M. (1979). On studying organizational cultures. *Administrative Science Quarterly, 24*(4), 570-581. https://doi.org/10.2307/2392363

Ray, M. (2024). *Chelsea Manning*. Encyclopaedia Britannica. https://www.britannica.com/biography/Chelsea-Manning

Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.

Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). Jossey-Bass.

Schneider, B., Ehrhart, M. G., & Macey, W. H. (2013). Organizational climate and culture. *Annual Review of Psychology, 64*, 361-388. https://doi.org/10.1146/annurev-psych-113011-143809

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. https://doi.org/10.1016/j.im.2013.08.006

Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security, 148*, 104110. https://doi.org/10.1016/j.cose.2024.104110

Trice, H. M., & Beyer, J. M. (1993). *The cultures of work organizations*. Prentice Hall.

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the Longwall method of coal-getting. *Human Relations, 4*(1), 3-38. https://doi.org/10.1177/001872675100400101

Tyan, Inc. v. Garcia, Case No. CV 15-05443-MWF (JPRx) (C.D. Cal. May 2, 2017). https://casetext.com/case/tyan-inc-v-garcia

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Van Niekerk, J., & von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486. https://doi.org/10.1016/j.cose.2009.10.005

Weaver, G. R., Treviño, L. K., & Cochran, P. L. (1999). Corporate ethics programs as control systems: Influences of executive commitment and environmental factors. *Academy of Management Journal, 42*(1), 41-57. https://doi.org/10.2307/256873

Weick, K. E. (1995). *Sensemaking in organizations*. Sage.

Whetten, D. A. (1989). What constitutes a theoretical contribution? *Academy of Management Review, 14*(4), 490-495. https://doi.org/10.5465/amr.1989.4308371

Krešimir Fileš, MBA, MHRES. is a doctoral candidate at the Faculty of Organizational Sciences, University of Maribor, Slovenia. He holds a Bachelor's degree in Economics (2017) and an MBA in Marketing (2019) from Zagreb School of Economics and Management, Croatia, as well as a Master's degree in Human Resources and Educational Systems (2021) from the University of Maribor. His research interests include security culture, data security, organizational behavior, and human resource management in digital organizations. He is the author of "Incentivizing Low-level Organization Members by Increasing their Behaviour Factors is Crucial for an Innovative and Secure Up-to-date Workforce," published in National Security and the Future (23(3), 2022).

Gordan Akrap, PhD graduated from the Faculty of Electrical Engineering and Computing, University of Zagreb, in 1994 and received his PhD in Information and Communication Sciences from the University of Zagreb in 2011. His doctoral dissertation was entitled "Informational Strategies and Operations in Public Knowledge Shaping." He actively participated in the Croatian Homeland War and subsequently pursued a career in Croatia's diplomatic and security structures, completing various professional training programmes, including the Diplomatic Academy. His research interests include national and regional security, intelligence, and the history of the Homeland War. He has authored several books and published numerous papers in academic journals and conference proceedings. He serves as Vice-Rector of the "Dr. Franjo Tuđman" Defence and Security University in Zagreb and as Editor-in-Chief of National Security and the Future, a journal published in Croatia.

Appendix A: Originality and conflict-of-interest statement

We hereby certify that this manuscript, titled Security Culture as a Foundation for Data Security in Organizations: A Conceptual Framework, is an original piece of work and has not been published previously, nor is it currently under consideration for publication elsewhere. We confirm that this work is free from plagiarism and that all authors have contributed significantly to the research and have approved the final manuscript for submission.

The authors declare no potential conflicts of interest with respect to the research, authorship and/or publication of this article.