FRI-1.414-1-MIP-04

CYBERSECURITY GOVERNANCE: THE CHIEF INFORMATION SECURITY OFFICER'S TECHNICAL AND PSYCHOLOGICAL APPROACHES [4]

Angel Brenishki, PhD Student
Faculty of Natural Sciences and Education
Department Informatics and Information Technologies
University of Ruse "Angel Kanchev"
Email: angel@angel.bg

Abstract: *The scale of an organization plays a decisive role in the efficiency and feasibility of cyber security governance. While security policies may be designed with universal principles, their application in a global enterprise differs substantially from their enforcement in smaller environments. This article explores the challenges arising from the scale itself and um is based on managing cyber security in a multinational organization of 10,000 employees distributed across 40 offices on four continents. The analysis focuses on the interplay between human factors, cultural diversity, policy enforcement, incident response, patch and update management. The study compares the complexity of large-scale environments with that of smaller organizations, highlighting how the volume of people, systems and processes magnifies operational and security risks. The central argument is that effective cyber security governance in global enterprises requires not only technological solutions such as automation, Zero Trust architectures and artificial intelligence, but also strong leadership approach capable of harmonizing cultural differences, managing resistance to change and ensuring that policies are enforced without disrupting core business operations.*

Key words: *Cybersecurity, CISO, Business, Enterprise.*

INTRODUCTION

The larger the organization, the more difficult it becomes for a Chief Information Security Officer (CISO) to establish policies that are both universally applicable and locally enforceable. Human factors amplify this difficulty: employees come from diverse backgrounds, they have varying levels of knowledge, experience and attitudes toward security and the work processes. Some may resist strict policies as an obstacle to productivity, while others may unintentionally bypass rules due to lack of awareness or cultural differences in communication and hierarchy. As a result, the CISO must act not only as a strategist and technologist but also as a mediator and educator (Ciekanowski, M., Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y., & Czech, A., 2024).

Another challenge is the technical governance at a scale. Deploying security patches across thousands of endpoints requires automation pipelines and monitoring tools that are themselves prone to failures. Coordinating updates across heterogeneous infrastructures in multiple time zones risks disrupting business processes if not carefully planned, scheduled, performed and monitored. Incident response is equally complicated: what may appear as a localized breach in one office can quickly escalate across interconnected networks, with massive volumes of logs overwhelming traditional Security Information and Event Management (SIEM) systems. Without advanced approaches such as AI-driven anomaly detection and automated workflows, security teams risk drowning in false positives while real threats remain unnoticed. And if they don't properly manage this time, they may stick in endless manager meetings and waiting for the best time to start acting, until it is too late (Uccello, F., Pawlicki, M., D'Antonio, S., Kozik, R., Choraś, M., 2024).

The aim of this article is to compare the distinct challenges between large-scale and small-scale environments, to analyze the role of human and technical factors in policy enforcement and to propose strategies for effective cyber security governance. By emphasizing the unique difficulties of managing 10,000 employees across 40 offices worldwide, this study highlights the critical importance of scalability, adaptability and cultural sensitivity in modern information security leadership, compared to smaller and more manageable organizations.

[4] Докладът е представен на конференция на Русенския университет на 24 октомври 2025 г. в секция „Математика, информатика и физика" и отразява резултати от работата по проект № 25-ФПНО-04, финансиран от фонд „Научни изследвания" на Русенския университет.

EXPOSITION

Large-scale complexity in cyber security governance

Table 1. Large scale complexity

Section	Topic	Main Challenges	Key Solutions /Strategies
2.1 Human factor and organizational diversity	Managing people and cultural diversity in global cybersecurity	- Human behaviour is the weakest link - Cultural, social, and language differences affect policy acceptance - Misaligned security perceptions	- CISO as strategist and cross-cultural leader - Adapt policies to local contexts - Communicate security goals effectively across regions
2.2 Policy enforcement at scale	Applying consistent security policies globally	- Difficult to enforce policies uniformly - Shadow IT and legacy systems - Balancing global vs. local needs	- Define minimum global baselines (e.g., MFA, encryption) - Allow local flexibility for non-critical areas - Balance rigidity and adaptability
2.3 Patch and update management	Coordinating software updates across a large enterprise	- Time zone conflicts - Legacy systems - Limited network infrastructure	- Use centralized patch management and EDR tools - Employ phased rollouts and fallback plans - Validate and automate updates carefully
2.4 Monitoring and incident detection	Detecting and analyzing security threats globally	- Overwhelming data volumes - False positives - Inconsistent local reporting	- Deploy AI-enhanced SIEM/SOAR systems - Standardize escalation paths and playbooks - Train local teams for consistent reporting
2.5 Incident response at global scale	Coordinating global response efforts	- Time zone and jurisdictional delays - Legal variations (e.g., GDPR deadlines) - Rapid lateral threat movement	- Implement global IR plans with legal input - Use Zero Trust and segmentation - Conduct continuous drills and red team exercises
2.6 Resistance to change and operational continuity	Overcoming resistance to security measures	- Employees see security as slowing productivity - Local business priorities conflict with global rules	- Position security as business enabler - Communicate value of security for trust and growth - Sequence rollouts and compromise when needed

Table 1 outlines the six major operational and human challenges faced by global enterprises in cybersecurity management:

- The human factor (2.1) is the foundation — cultural, social, and communication barriers shape how security is perceived.
- Policy enforcement (2.2) and patch management (2.3) highlight operational and logistical challenges of maintaining consistent security across diverse regions and technologies (Kozik, R., Choraś, M., 2024).
- Monitoring and incident response (2.4–2.5) focus on detecting and reacting to threats effectively on a global scale, balancing automation with skilled human oversight.

- Resistance to change (2.6) emphasizes the importance of leadership, communication, and viewing cybersecurity as a facilitator of business continuity rather than a burden (Nascimento Heim, T., 2023).

Small-scale complexity in cyber security governance

Table 2. Small scale complexity

Section	Topic	Main Challenges	Key Solutions /Strategies
3.1 Limited resources and expertise	Lack of dedicated security staff and budget	- No CISO or SOC - IT staff lack cyber expertise - Misconception that general IT = security - High risk from basic errors (e.g., exposed RDP, weak passwords)	- Recognize distinction between IT and cybersecurity - Provide targeted training - Outsource or share security services - Prioritize essential protections
3.2 Simplified infrastructures and reduced complexity	Smaller scale and simpler systems	- Limited systems but easier management - Informal governance replaces policy	- Easier policy enforcement - Manual patching possible - Leverage personal trust and direct communication for compliance
3.3 Vulnerability to single points of failure	Overreliance on few individuals or single servers	- One person holds critical knowledge - Lack of redundancy or backups - Human absence = operational risk	- Document procedures - Build redundancy and backup systems - Cross-train staff to reduce knowledge silos
3.4 Absence of formalized policies and procedures	Weak or non-existent governance structures	- Informal/unwritten rules - Shared accounts, reused passwords - Reactive rather than proactive responses	- Develop simple but formalized security policies - Implement basic identity management - Encourage proactive risk assessment
3.5 Balancing security with business priorities	Security seen as secondary to growth	- Budget and attention go to sales, not security - Reactive investment after incidents	- Integrate security into business strategy - Show value of security for trust and resilience - Treat security as business enabler, not obstacle
3.6 Opportunities for agility	Small organizations can adapt quickly	- Fewer bureaucratic constraints - Less legacy infrastructure	- Rapid adoption of modern frameworks - Use agility to innovate and strengthen posture - Build efficient, scalable defences quickly

Table 2 summarizes how small organizations experience cybersecurity governance differently from large enterprises:

They struggle mainly with resource scarcity, lack of expertise, and informal governance (3.1, 3.4). Their simplicity and agility (3.2, 3.6) provide advantages — fewer systems, direct communication, and faster adaptation to new technologies. The main vulnerabilities arise from overreliance on individuals (3.3) and security deprioritization (3.5) in favour of short-term business goals. When small organizations combine their agility with basic formalization, redundancy, and proactive planning, they can achieve a surprisingly resilient cybersecurity posture despite limited resources (Johannsen, A., Kant, D., Creutzburg R., 2020) (Chidukwani, A., Zander S., Koutsakis P., 2022).

Comparative analysis: large-scale vs. small-scale environments

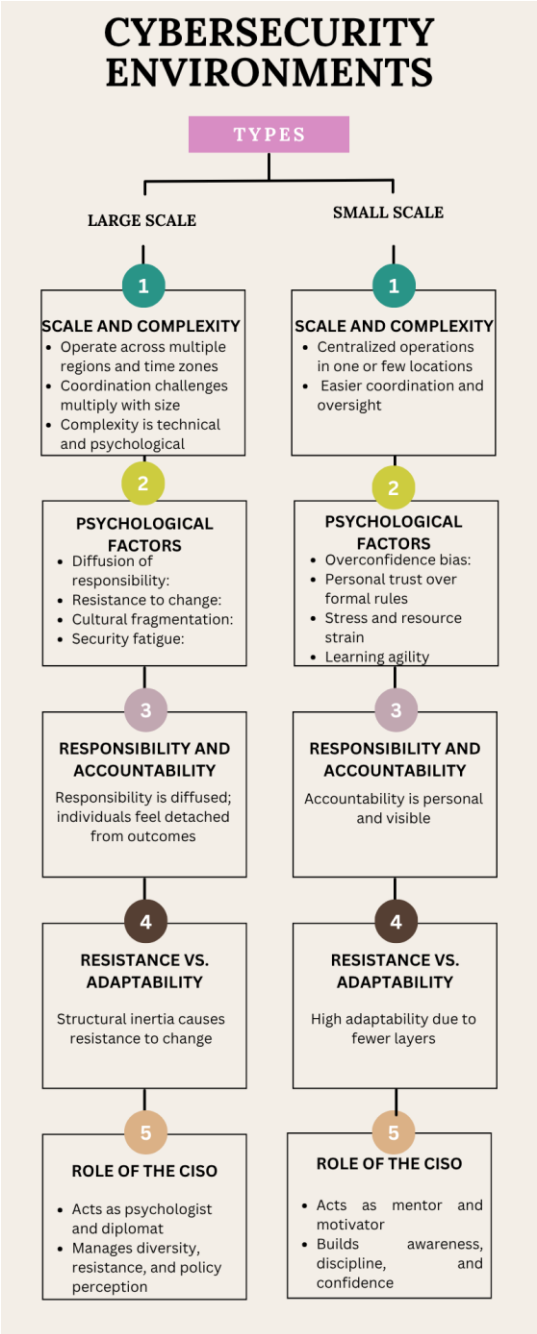

Fig. 1. Comparative analysis: large-scale vs. small-scale environments

Fig. 1 shows comparative analyses of large and small environments of five criteria:

- Scale and complexity.
- Psychological factors.

- Responsibility and accountability.
- Resistance and adaptability.
- Role of CISO.

Cyber security governance extends beyond technical measures, encompassing the management of people, processes, and leadership to foster organizational resilience. Large enterprises struggle with scale, cultural fragmentation, and resistance to change, while small organizations face resource constraints, overreliance on trust, and lack of formal policies. Effective governance integrates technical, organizational, interpersonal, and psychological factors, positioning the CISO as both strategist and leader.

Security culture thrives when employees see protection as a shared duty rather than an imposed rule. Leadership must model compliance and reinforce positive behaviour through recognition and fairness, turning security into a collective value rather than a checklist.

Human relationships can both strengthen and weaken security. Governance should harness them positively - through peer influence or security champions - to encourage compliance and bridge gaps between central policy and local practice.

Clear, positively framed, and well-timed communication determines whether policies succeed or fail. Poor messaging can transform good technical measures into crises, while transparent communication and preparation ensure smooth adoption and trust, especially during incidents.

Executives often underestimate how small technical changes can cause major organizational disruptions. The CISO must translate technical interdependencies into business terms, promoting careful testing, phased rollouts, and contingency planning to prevent cascading failures.

Security must protect without hindering operations. A balanced approach—using gradual enforcement, context-aware flexibility, automation, and feedback—embodies the principle of "secure by design, usable by default" (Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V., 2023).

Cyber work strains staff through fatigue and burnout. Supportive practices such as duty rotation, non-punitive reporting, and recognition improve morale and vigilance. Large organizations can learn agility from small ones, while smaller firms can adopt discipline from larger counterparts.

CONCLUSION

The enhanced governance strategies presented in the paper highlight a holistic model for success. Building a culture of shared responsibility, leveraging interpersonal relations constructively, ensuring professional communication, translating technical risks into business terms for management, balancing enforcement with continuity, supporting staff psychologically and integrating lessons from both large and small organizations are all essential elements of the effective governance. Together, they demonstrate that security cannot be reduced to technology alone: it is the result of aligning people, processes and leadership behaviors toward a common goal.

Ultimately, cyber security governance is a real test of leadership. The effective CISO must be a diplomat, strategist, psychologist, mediator and educator, capable of anticipating ripple effects, harmonizing cultural differences and guiding both executives and frontline staff toward secure practices without paralyzing productivity. By uniting technical competence with psychological insight and management awareness, organizations of every size can transform security from a source of friction into a foundation of trust, resilience and sustainable growth in the interconnected digital world.

REFERENCES

Ciekanowski, M., Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y., & Czech, A. (2024). Chief information security officer: a vital component of organizational information security management. European Research Studies Journal, 27(2), 35-46.

Uccello, F., Pawlicki, M., D'Antonio, S., Kozik, R., Choraś, M. (2024). Towards Hybrid NIDS: Combining Rule-Based SIEM with AI-Based Intrusion Detectors. Daimi, K., Al Sadoon, A. (eds) Proceedings of the Second International Conference on Advances in Computing Research (ACR'24). ACR 2024. Lecture Notes in Networks and Systems, vol 956. Springer, Cham.

Stoleriu, R., Petre I., Pop F. (2025). Cybersecurity governance in large-scale infrastructures, Romanian Journal of Information Technology and Automatic Control, Vol. 35, No. 1, 51-66.

Nascimento Heim, T. (2023). Global governance and regulation of cybersecurity: Towards coherence or fragmentation? [PhD Thesis - Research UT, graduation UT, University of Twente]. University of Twente.

Johannsen, A., Kant, D., Creutzburg R. (2020). Measuring IT security, compliance and data governance within small and medium-sized IT enterprises. Proc. IS&T Int'l. Symp. on Electronic Imaging: Mobile Devices and Multimedia: Technologies, Algorithms & Applications,

252-1 - 252-11, https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-252

Chidukwani, A., Zander S., Koutsakis P. (2022), A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. in IEEE Access, vol. 10, pp. 85701-85719.

Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. Risk Analysis, 43, 2082-2098.