

Best Practices in Security Convergence: Tales from the Trenches

Michael Whitman
Coles College of Business
Kennesaw State University
Kennesaw, GA, USA
0000-0002-4075-0995

Herbert Mattord
Coles College of Business
Kennesaw State University
Kennesaw, GA, USA
0000-0002-3076-375X

Kathleen Kotwica
Security Executive Council
Marietta, GA, USA
0000-0003-4716-1779

Abstract—Security convergence, the integration of cybersecurity and physical security, has been discussed for over two decades, yet organizations still face challenges in defining and implementing effective strategies. This article explores the evolution of security convergence, highlighting key overlaps between physical and virtual security, especially with the rise of computerized operations in critical infrastructure. Through a 2023 survey and in-depth interviews with security professionals, four best practices are identified: implementing employee risk ratings, utilizing decision matrices, establishing fusion centers, and fostering a supportive organizational culture. These practices enhance collaboration and optimize security operations, demonstrating that effective convergence is not just about structural integration but also strategic coordination and cultural alignment for improved organizational resilience.

Keywords—Security convergence, cybersecurity and physical security integration, enterprise risk management, fusion centers, security governance, workforce risk rating

I. INTRODUCTION

Security convergence is a concept that has been discussed in industry circles for many years. The term describes the integration of cybersecurity and physical security to develop a unified approach to managing security threats in an organization.

The industry's definition of 'convergence' remains a subject of debate. The term is commonly used in various security communities to describe the merger of the management of corporate security and cybersecurity functions within the organization. Challenges to the definition and classification of convergence begin with a lack of a unified approach to physical security and cybersecurity in the governance structure for such business units. Even outside of convergence discussions, there are differences in how organizations assign roles and responsibilities associated with the administration of computer and networking assets. Does the physical loss of a server fall under the purview of the cybersecurity department or the physical security department? Does the assignment of facilities access controls, based on keycards and computerized door locks, fall under physical

security or cybersecurity? Many organizations choose a degree of oversight that could technically be classified as convergence, finding some measure of association or coordination to address these areas of overlap.

Operational activities in both the public and private sectors are found to be computerizing operations and monitoring functions, creating new vulnerabilities that overlap the physical and virtual domains.[1] Supervisory Control and Data Acquisition (SCADA) systems are critical for managing and monitoring industrial processes and infrastructure. SCADA systems gather data in real-time from remote locations to control equipment and conditions, primarily used in industries such as energy, water, and manufacturing, all parts of any nation's critical infrastructure. The earliest references to SCADA systems in literature date back to the 1960s, when these systems were first developed to improve the efficiency and reliability of industrial operations. One of the initial uses of SCADA was for electric power utilities, enabling more efficient grid management and reducing the need for manual monitoring and control. As technology advanced, SCADA systems evolved to incorporate more sophisticated data acquisition and control capabilities, including the integration of PLCs (Programmable Logic Controllers) and improved human-machine interfaces (HMIs). By the 1990s, SCADA systems were recognized as essential components for modern industrial automation, providing critical support for complex operational environments. Significant early works on SCADA include technical reports and papers from industry conferences and early research by key companies and institutions involved in industrial automation and control. [2], [3]

This reference to a 'path to convergence' somehow connotes an optimum state at the end of a series of converging functions that are expected to be superior to other ways of collaborating.[4] Outside the binary state of "nothing to do with each other" and "one team, one role," there is an entire spectrum of degrees of interaction that can occur between a physical security department tasked with the protection of the organization's physical assets and personnel, and the cybersecurity department, tasked with the protection of the organization's information and other virtual assets.

While there have been many efforts to describe the optimum placement of both corporate and cybersecurity organizational units, there is no definitive solution.[4], [5], [6] This is reflected in the lack of standardization on the roles and responsibilities of the top cybersecurity/information security executive: "There is no single agreement on the assigned duties or scope of the CISO role, or its most effective organizational reporting structure." [6] The optimization of security operations in larger organizations has often centered on discussions of the relative degree of convergence of corporate security functions and cybersecurity functions.[6]

A. *Why Converge Security?*

When examining the domains of physical security and cybersecurity, there are many points of overlap where at least coordination is crucial. Knowledge of vulnerabilities in physical security is essential in cybersecurity. An adage in cybersecurity, back when it was known as IT security, is that the best firewall won't protect information on a server from a well-placed brick. Physical security trumps logical security. If attackers can lay their hands on a server or client hard drive, they own that information. The threat of theft of information assets has long been a concern for both physical and virtual security professionals. It only makes sense to at least increase the coordination between these two areas, if not unify them.

The field of digital forensics expanded the traditional investigatory activities associated with physical crimes and workplace abuse and misuse. The need to use digital forensics for internal employee investigations and root cause analysis of cyber-attacks further integrates the physical and cyber domains. As physical security becomes increasingly computerized, it extends the physical and virtual overlaps. Automated door locks, digital closed-circuit television (CCTV) systems, employee badges, and card swipes have replaced the traditional steel keys and analog monitoring systems.

B. *The Evolution of Security Convergence*

Security convergence began to gain formal recognition in academic and industry discussions in the early 2000s. By 2005, Hamilton had explored the challenges and perspectives of this concept in the Security Journal. Concurrently, ASIS International, ISACA, and ISSA began advocating for security convergence through the Alliance for Enterprise Security Risk Management.

Research has touched on integrating corporate and cybersecurity, especially in access controls[7], [8], [9] but there's limited focus on merging corporate and cybersecurity operations. Some have proposed a risk analysis model compatible with both ISO 27001 and ISO 31000, addressing both risk types.[10], [11] Similarly, the recommendation of integrating corporate security with IT networks through six essential methods has been described. Beyond physical access, technologies like those in SCADA systems are becoming digital. Some researchers have discussed the transition to 'smart' factories, but they briefly cover security,

offering broad suggestions like central management platforms.[12]

Academic literature on security convergence is sparse, often more discussion-based than analytical. The prevailing view is that as new digital technologies emerge, organizations will likely upgrade their corporate security alongside information security.[13] While many studies address specific industries adopting new technologies, including risk analysis, few formal studies have provided comprehensive guidance on security convergence operations.

Convergence is often seen as inevitable or beneficial, yet the impact on organizations needs more study to identify effective collaboration and optimization methods. Much of the discussion centers on potential issues arising from convergence, suggesting these issues could cause problems if poorly understood. Even resolved issues might negatively affect an organization's risk management and breach prevention capabilities.

Industry professionals' interviews and articles offer valuable insights into security convergence, especially in the early stages of understanding collaborative security environments. These discussions help shape a general understanding of convergence and its future direction. Most commentary suggests that convergence is either necessary or already happening. For instance, Fretty advises creating separate networks and keeping firmware updated[14], while Hodgson highlights the importance of integrators engaging with client IT departments.[8] Kloepple stresses the need for inter-department communication and cross-training to support convergence.[4] However, these perspectives are not empirical, and their effectiveness needs further research.

A 2019 ASIS study highlighted ongoing efforts and challenges in implementing converged security. The ASIS Foundation's "The State of Security Convergence in the United States, Europe, and India" surveyed over 1,000 senior professionals in physical security, cybersecurity, disaster management, and business continuity. It revealed that despite predictions of inevitable security convergence, only 24 percent of respondents had merged their physical and cybersecurity functions. Of those, 96 percent reported positive outcomes, with 72 percent noting improved overall security. Overall, 78 percent believed convergence would strengthen their security function.

II. INITIAL SECURITY CONVERGENCE REQUEST FOR PARTICIPATION

Researchers contacted organizations that are clients of the Security Executive Council. The request sought to conduct interviews of key security personnel regarding the current, desired, and potential states of security convergence across multiple industries, security budgets, and organizational sizes. The request aimed to identify factors influencing collaborative outcomes in security convergence. The request asked these professionals to participate in a detailed interview to gain an understanding of their perspectives and intentions regarding

convergence. Out of 99 invitations sent, 23 security professionals from both sides of the convergence agreed to interviews.

Those accepting the invitation were asked to classify their current state of security convergence using the following options:

- Option 1: Physical security and Cybersecurity are merged into an organizational unit such as a department or division, and collaborate on all or most programs and administration.
- Option 2: Physical security and Cybersecurity are separate organizational units but formally collaborate and partner on all or most routine operational issues.
- Option 3: Physical security and Cybersecurity are separate organizational units that do not routinely collaborate or partner regularly, but may do so when a situation forces the need.
- Option 4: Some other approach – (please specify).

Each individual who responded to the invitation was also asked to invite their counterparts to participate. Of the 23 ultimately interviewed, only three organizations had representatives from both functions interviewed.

These interviews were recorded and transcribed to allow better analysis and accurate preservation of their responses. After three separate researchers reviewed the transcripts, common themes were identified for examination and discussion.

After the survey phase, 23 security professionals were invited to participate in in-depth interviews, with 21 completing the process. These individuals represented 19 unique organizations and represented five broad industry sectors: Finance & Insurance (6), Healthcare & Pharmaceuticals (5), Energy & Infrastructure (4), Technology & Media (4), and Government & Consulting (4). This distribution reflects the diversity of convergence experiences and security models across industries with varying regulatory environments, asset profiles, and operational complexities. Interviewees included senior leaders from both corporate (physical) security and cybersecurity, with job titles such as Chief Security Officer (CSO), Chief Information Security Officer (CISO), Security Director, and other senior vice president-level positions. Collaboration structures varied considerably: approximately 38% operated under “separate but partnered” models, 24% reported fully converged or combined organizations, and the remaining respondents described ad hoc or evolving arrangements. While a few organizations (3) had representation from both security domains, most insights reflected perspectives from a single security function within each organization.

Among the 23 interview participants, 9 held C-suite roles (e.g., CSO, CISO), 5 were Vice Presidents or Senior Vice Presidents, and 7 were Directors or Heads of Security. This

distribution indicates that all interviewees were within one to two degrees of separation from the CEO, ensuring strategic insight into their organization’s security convergence posture. No junior-level staff or operational roles were included, which helps to ensure the findings reflect high-level planning, policy, and executive oversight in cybersecurity and physical security integration.

All interviews were recorded, transcribed, and analyzed thematically by the research team. This analysis surfaced four recurring best practices seen as essential to successful security convergence.

These four “best practices” were identified as:

1. The use of “employee risk ratings” to identify potential internal threats and employees of interest for training/re-training.
2. The use of “decision matrices” to support security operations and decision making.
3. The implementation of a “fusion center” to provide integration and coordination between physical and cybersecurity groups, regardless of their level of convergence.
4. The impact of organizational culture on all security-related programs, plans, and operations.

Each of these best practices is described in the following sections.

A. *Employee Risk Ratings*

Internal threats pose significant risks to both physical and cybersecurity operations. These threats can arise from malicious insiders, negligent employees, or those inadvertently compromised by external actors. To mitigate such risks, organizations increasingly rely on employee risk ratings, a systematic approach to assessing and managing the potential threat each employee poses to organizational security.[15] These risk ratings can lead to targeted security training, increased monitoring, informed access control decisions, and support for both physical and cybersecurity postures. These matrices can also provide insight into insider security attacks such as data exfiltration and theft.

Central to employee risk ratings is the identification, assessment, and prioritization of risks associated with employee behavior and access to sensitive information. This can be supported through an understanding of the psychological and behavioral traits that may indicate a higher propensity for risky behavior or susceptibility to external threats is crucial in developing effective risk ratings.[16] Data analytics tools providing metrics on employee performance (both physical and virtual) can further support the development of these risk matrices.

Several interviewees mentioned using decision matrices in different roles. One interviewee’s organization uses them in their helpdesk to route incoming requests, another’s

organization uses them to guide security strategic planning, while two other organizations use them to support investigations.

An employee risk rating could include variables that quantify potential risk areas, such as:

Creating an "employee risk rating" matrix in the computing and cybersecurity fields involves assessing various factors that could contribute to an individual's risk of causing a security breach or being a target for attacks. Here are key variables that could be included:

5. Access Level - Employees with higher access levels (e.g., system administrators, IT staff) pose a greater risk if their accounts are compromised.
6. Job Role - Certain roles (e.g., developers, financial officers) may have more exposure to sensitive data.
7. Security Training and Awareness - Employees with inadequate training are more likely to fall for phishing attacks and other social engineering tactics.
8. Behavioral Indicators - Behavioral anomalies can signal potential insider threats or negligence.
9. Historical Security Incidents - Previous incidents may indicate a higher risk of future breaches.
10. Technical Proficiency - Employees with lower technical proficiency might be more prone to errors that could lead to security vulnerabilities.
11. Device Usage Patterns - Remote work and use of personal devices can increase exposure to security risks.
12. Compliance with Security Policies - A history of non-compliance can indicate the potential for future misuse.
13. Network Activity - Individuals with unusual network activity (time and duration of usage, quantity of data transferred) can indicate potential threats.
14. Personal Factors - Personal circumstances such as financial stress, job dissatisfaction, or other pressures can increase susceptibility to malicious activities.

Incorporating these variables into an employee risk rating matrix allows organizations to assess and mitigate potential threats more effectively. Each variable contributes to a holistic view of an employee's risk profile, enabling tailored interventions and enhanced security measures.

Employee risk ratings can be a critical component of an effective security operation, offering a proactive approach to identifying and mitigating internal threats. By leveraging risk management theories, behavioral science, and data analytics, organizations can develop robust risk rating systems that enhance their security posture. However, it is essential to

balance security measures with ethical considerations, ensuring that privacy, accuracy, and transparency are upheld. Future research should focus on refining risk assessment models and exploring the integration of emerging technologies, such as AI and blockchain, to further enhance the efficacy of employee risk ratings.

B. Decision Matrices

Another best practice that emerged from the interviews is the use of security-based decision matrices, which provide a structured approach to evaluating and prioritizing various security activities. Interviewees indicated that these can be used in various tasks, ranging from help desk support to incident response.

A decision matrix, also known as a Pugh matrix or a decision grid, is a tool for evaluating and prioritizing multiple options against predefined criteria. The method involves assigning weights to each criterion based on its relative importance and scoring each option against these criteria. The aggregated scores facilitate a comparative analysis, enabling decision-makers to identify the most viable solutions.

In the context of cybersecurity, decision matrices incorporate developments from several areas, including Multi-Criteria Decision Analysis (MCDA), which provides the mathematical and systematic basis for decision matrices. MCDA methods, such as the Analytic Hierarchy Process (AHP) and Simple Multi-Attribute Rating Technique (SMART), offer robust mechanisms for weighting criteria and scoring alternatives.[17] Risk management and utility theory aid in understanding how decision matrices can be used to maximize the overall utility or benefit derived from different security measures.[18]

Decision matrices can be employed in cybersecurity operations, including threat assessment, incident response, and strategic planning.[19] In threat assessments, decision matrices enable security teams to systematically evaluate threats based on criteria such as likelihood, impact, detectability, and the availability of countermeasures. For instance, a decision matrix can help prioritize threats that require immediate attention over those that pose less risk.[19]

During incident response, decision matrices assist in determining the most effective actions. By evaluating response options against criteria like speed of implementation, resource requirements, and potential disruption, teams can make informed decisions quickly. Decision matrices can also support long-term planning by comparing different security strategies or technologies. This involves assessing options against criteria such as cost, scalability, effectiveness, and alignment with organizational goals.

When implemented in the help desk, decision matrices can be used to quickly route incoming user requests for assistance to the proper department. This will support the delineation of issues between traditional user technical support requests

and potential indicators of attacks. With regards to convergence, these matrices can assist in routing support requests to the appropriate individuals or groups responsible for supporting the requested area. This can include group distributions to ensure that both physical and cybersecurity teams receive the same information, to allow each to provide their perspective on the potential attack or issue.

Decision matrices can serve as valuable tools in security operations, providing a structured and systematic method for evaluating and prioritizing security activities and issues. Their effectiveness hinges on the careful selection of criteria, accurate weighting and scoring, and continuous adaptation to the dynamic cybersecurity landscape.

C. The Fusion Center

The convergence of physical and cybersecurity threats necessitates a holistic approach to security management. Fusion centers, designed to integrate data from diverse sources and facilitate coordinated responses, can play a crucial role in this integrated approach. The fusion center doesn't have to be a joint security operating center (SOC), it can be a virtual network of employees that work together on related tasks, to ensure that information is effectively communicated between the physical and cybersecurity personnel as well as management. These professionals are typically supported by data analytics tools to collect and aggregate information from throughout the organization to inform their activities and operations.

Fusion centers can support a range of activities aimed at enhancing security operations through the integration of physical and cybersecurity functions, including threat intelligence integration, incident response coordination, resource optimization, and policy and strategy development. [20]

1. Threat Intelligence Integration - Fusion centers collect, analyze, and disseminate threat intelligence from both physical and cyber domains. This integrated intelligence helps identify complex threats that span multiple vectors, such as cyber-physical attacks on critical infrastructure.
2. Incident Response Coordination - In the event of a security incident, fusion centers serve as the hub for coordinating responses. By providing real-time situational awareness and facilitating communication between physical security and cybersecurity teams, fusion centers ensure a unified and effective response.
3. Resource Optimization - Fusion centers enable better resource allocation by providing a comprehensive view of the security landscape. This helps prioritize resources based on the most significant risks and vulnerabilities.
4. Policy and Strategy Development - Fusion centers contribute to the development of integrated security

policies and strategies. By leveraging insights from both physical and cybersecurity perspectives, organizations can craft more robust and adaptive security frameworks. [21]

Fusion centers can offer several advantages in strengthening security operations, regardless of the level of convergence:

1. Enhanced Situational Awareness - By integrating data from various sources, fusion centers provide a comprehensive view of the threat landscape, enabling better situational awareness and proactive threat identification.
2. Improved Coordination - Fusion centers facilitate seamless communication and collaboration between physical security and cybersecurity teams, reducing response times and improving incident management.
3. Holistic Risk Management - The integrated approach of fusion centers allows for a more comprehensive risk assessment and mitigation strategy, addressing both physical and cyber threats in a coordinated manner. [22]

However, there are challenges and considerations in fusion centers:

1. Data Integration: Integrating diverse data sources from physical and cybersecurity domains can be technically complex and require significant resources. Ensuring data compatibility and interoperability is crucial.
2. Privacy and Security: The centralized nature of fusion centers necessitates robust security measures to protect sensitive data and ensure compliance with privacy regulations.
3. Organizational Culture: Effective fusion centers require a culture of collaboration and trust across different security disciplines. Overcoming organizational silos and fostering a unified security mindset can be challenging, as discussed in the next best practice. [22]

One interviewee indicated that his organization uses their fusion center to manage organizational investigations. This includes internal investigations (e.g., theft or misconduct) and cybersecurity incident response investigations involving digital forensics. They discovered that each group (physical and cybersecurity) brought a different perspective to the inquiry. Having them all review each incident and provide insight sped up investigations and improved overall efficiency.

Fusion centers represent a critical evolution in the coordination and integration of physical and cybersecurity operations. By leveraging principles of systems theory, information sharing, and risk management, fusion centers enhance situational awareness, improve incident response, and support holistic risk management.

D. The Impact of Organizational Culture on Security

Organizational culture plays a pivotal role in shaping security operations and strategies, especially how the organization views physical and cybersecurity. It influences how employees develop, implement, and adhere to security policies. In the context of the convergence of physical and cybersecurity, organizational culture becomes even more critical as it must support integrated approaches and collaboration across traditionally siloed departments.

Edgar Schein defines organizational culture as “a pattern of shared basic assumptions learned by a group as it solves its problems of external adaptation and internal integration.”[23] These assumptions and beliefs drive behavior and decision-making within the organization.

The Competing Values Framework (CVF) identifies four types of organizational culture—clan, adhocracy, market, and hierarchy—each influencing security operations differently. For example, a hierarchical culture might emphasize formal policies and procedures, while an adhocracy might prioritize flexibility and innovation. A culture that values security will prioritize robust policies, while one focused on operational efficiency might downplay security measures. A study by Ashenden and Sasse found that security policies often fail when they conflict with the prevailing organizational culture and employees' day-to-day realities.[24]

The convergence of physical and cybersecurity requires a unified approach heavily influenced by organizational culture. A culture that promotes collaboration and cross-departmental communication is essential for integrating physical and cybersecurity. Von Solms and Van Niekerk argue that an integrated approach to security requires breaking down silos and fostering a culture of cooperation between physical and cybersecurity teams.[25]

Several interviewees indicated that organizational culture dramatically affected their degree of convergence, not all of it positively. In one case, the departure of an executive champion completely reversed the organization's progress toward complete security convergence. The myopic perspective of their successor exacerbated the loss of executive-level background in both physical and cybersecurity.

Leadership and Governance: Leadership plays a crucial role in shaping a culture that supports the convergence of physical and cybersecurity. Effective governance structures, driven by a cohesive leadership team, are necessary to align security strategies across domains. Boss and others suggest that strong leadership commitment to security can drive cultural change and facilitate integration.[26]

An organizational culture that emphasizes shared values and common goals across physical and cybersecurity domains can enhance overall security posture. When teams understand and appreciate the interdependence of physical and cybersecurity, they are more likely to collaborate and support integrated security efforts.

Organizational culture is a fundamental determinant of the effectiveness of security operations and plans. It shapes policy development, employee behavior, and the success of training programs. In the context of the convergence of physical and cybersecurity, a supportive culture is essential for fostering collaboration, ensuring leadership commitment, and aligning shared values. Future research should focus on developing frameworks for cultural assessment and intervention in security contexts and exploring best practices for cultural integration in diverse organizational environments.

III. SUMMARY AND CONCLUSIONS

While these best practices were explored in the context of security convergence, and the number of respondents is quite modest, we believe there is value in these observations for any organization with a security function. Regardless of an organization's current or planned security convergence, using these tools can improve communication and operational efficiency for security professionals within and between departments and with organizational management.

Additional research is needed to determine the impact these best practices have on these organizations over time. Furthermore, the costs and perceived benefits should be identified to provide additional information for organizations considering adopting these practices.

REFERENCES

- [1] M. A. Khan, A. Amir, and K. V. Vuda, “Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure,” *Sensors*, vol. 23, no. 8, p. 4060, 2023, doi: 10.3390/s23084060.
- [2] L. Schneller, C. N. Porter, and A. Wakefield, “Implementing Converged Security Risk Management: Drivers, Barriers, and Facilitators,” *Security Journal*, vol. 36, pp. 333–349, 2023, doi: 10.1057/s41284-022-00341-6.
- [3] D. Burgoyne, “On the road to security convergence,” *Consulting-Specifying Engineer*, Nov. 28, 2021. Available: csemag.com.
- [4] S. Kloepple, “Converging Physical Security and Cybersecurity: As buildings become more digitized, it's time for improved communication between the two,” *Buildings*, vol. 113, no. 8, p. 32, Sep. 2019.
- [5] J. P. Coombes, “Factors that influence the placement of the chief information security officer in oil and natural gas organizations,” Ph.D. dissertation, Marymount Univ., Arlington, VA, USA, 2021. Available: ProQuest Dissertations Publishing, Accession No. 28862238.
- [6] D. Ritchey, “The changing role of the CISO,” *Security Magazine*, pp. 16–18, Feb. 2020. Available: securitymagazine.com.
- [7] T. McCreight and D. Leece, “Physical Security and IT Convergence: Managing the Cyber-Related Risks,” *Journal of Business Continuity & Emergency Planning*, vol. 10, no. 1, pp. 18–30, 2016.
- [8] K. Hodgson, “Profiting from Physical/Logical Convergence: SDM talks to four experienced integrators about the future of convergence...,” *Security Distributing & Marketing*, vol. 44, no. 9, Sep. 2014.
- [9] C. M. Lee and H. Chang, “A study on security strategy in ICT convergence environment,” *The Journal of Supercomputing*, vol. 70, pp. 211–223, 2014.
- [10] K. Peciña, R. Estremera, A. Bilbao, and E. Bilbao, “Physical and Logical Security Management Organization Model Based on ISO 31000 and ISO 27001,” in *Proc. Carnahan Conf. on Security Technology (CCST)*, Barcelona, Spain, 2011, pp. 1–5, doi: 10.1109/CCST.2011.6095894.

- [11] K. Peciña, A. Bilbao, and E. Bilbao, "Physical and Logical Security Risk Analysis Model," in Proc. Carnahan Conf. on Security Technology (CCST), Barcelona, Spain, 2011, pp. 1–7, doi: 10.1109/CCST.2011.6095895.
- [12] P. A. Okeme, A. D. Skakun, and A. R. Muzalevskii, "Transformation of Factory to Smart Factory," in Proc. IEEE Conf. Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg and Moscow, Russia, 2021, pp. 1499–1503, doi: 10.1109/ElConRus51938.2021.9396278.
- [13] L. C. Gajary *et al.*, "Convergence Research as a 'System-of-Systems': A Framework and Research Agenda," *Minerva: A Review of Science, Learning & Policy*, vol. 62, no. 2, pp. 253–286, 2024, doi: 10.1007/s11024-023-09503-1.
- [14] P. Fretty, "IT/OT Convergence is Here, But Are You SECURE?," *Industry Week*, vol. 269, no. 2, p. 20, Mar. 2020.
- [15] D. Capelli, A. P. Moore, R. F. Trzeciak, and T. J. Shimeall, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Boston, MA, USA: Addison-Wesley Professional, 2016.
- [16] F. L. Greitzer, L. J. Kangas, C. F. Noonan, C. L. Brown, and T. A. Ferryman, "Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats," in Proc. 45th Hawaii Int. Conf. System Sciences (HICSS), Maui, HI, USA, 2012, pp. 2392–2401, doi: 10.1109/HICSS.2012.309.
- [17] S. Alhawari, L. Karadsheh, A. Nehari Talet, and E. Mansour, "Knowledge-Based Risk Management Framework for IT Projects," *International Journal of Information Management*, vol. 32, pp. 50–65, 2012.
- [18] M. Jouini, L. Ben Arfa Rabai, "Security Risk Management Metric for Cloud Computing Systems," *International Journal of Organizational and Collective Intelligence (IJOICI)*, vol. 4, no. 3, pp. 1–21, 2014.
- [19] A. Shamel-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of Information Security Risk Assessment (ISRA)," *Computers & Security*, vol. 57, pp. 14–30, 2016.
- [20] D. L. Carter and J. G. Carter, "The intelligence fusion process for state, local, and tribal law enforcement," *Criminal Justice and Behavior*, vol. 36, no. 12, pp. 1323–1339, 2009, doi: 10.1177/0093854809345674.
- [21] A. Sofaer and S. Goodman, "Cybersecurity and national policy," *Georgetown Journal of International Affairs*, vol. 11, no. 2, pp. 5–12, 2010.
- [22] M. Hentea, "Improving Security for SCADA Control Systems," *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 7, pp. 95–108, 2012.
- [23] E. H. Schein, *Organizational Culture and Leadership*, 4th ed. San Francisco, CA, USA: Jossey-Bass, 2010.
- [24] D. Ashenden and M. A. Sasse, "CISOs and organisational culture: Their own worst enemy?," *Computers & Security*, vol. 39, pp. 396–405, 2013.
- [25] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97–102, 2013.
- [26] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss, "If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security," *European Journal of Information Systems*, vol. 18, no. 2, pp. 151–164, 2009.