The American Journal of Engineering and Technology
ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 180-186

Convergence of Industrial Risk Prevention and Cybersecurity Governance: A Multi-Dimensional Policy Framework for Systemic Resilience and Compliance

Dr. Julian Thorne
Department of Systems Engineering and Public Policy, University of Melbourne, Australia

OPEN ACCESS

SUBMITTED 01 December 2025
ACCEPTED 15 December 2025
PUBLISHED 31 December 2025
VOLUME Vol.07 Issue 12 2025

CITATION

Dr. Julian Thorne. (2025). Convergence of Industrial Risk Prevention and Cybersecurity Governance: A Multi-Dimensional Policy Framework for Systemic Resilience and Compliance. The American Journal of Engineering and Technology, 7(12), 180–186. Retrieved from https://theamericanjournals.com/index.php/tajet/article/view/7514

Abstract: This research article explores the critical intersections between industrial risk prevention and modern cybersecurity governance, arguing that the silos separating physical safety from digital security are increasingly obsolete in the face of systemic global threats. By examining the regulatory evolution following catastrophic industrial events-specifically the Lubrizol factory fire in France-and the surge in complex cybercrimes such as the Salt Typhoon and Medibank hacks, the study identifies a pervasive gap in integrated risk frameworks. The research synthesizes the French "major risk prevention" approach with international IT audit frameworks (ITAF) and strategic cybersecurity compliance models. It utilizes a comparative analysis of risk policy tools in Normandy, Piedmont, and Victoria to demonstrate that current methodologies remain overly hazards-focused rather than vulnerabilities-focused. Furthermore, the study investigates the role of third-party vendor risks and the necessity of multi-factor authentication (MFA) as fundamental pillars of organizational resilience. By proposing a "Strategic Cybersecurity Governance" model, this article provides a roadmap for aligning technological protection with legal compliance. The findings suggest that systemic

resilience requires a shift from reactive post-accident regulation toward proactive, blockchain-enhanced financial privacy and comprehensive auditing strategies. This article contributes a deep theoretical elaboration on the "chronic crisis" of industrial safety and the emerging challenges of cyber-physical integration, providing a publication-ready synthesis for researchers and policymakers.

Keywords: Cybersecurity Governance, Industrial Risk Prevention, Regulatory Compliance, Systemic Resilience, IT Audit Framework, Vulnerability Management.

Introduction

The modern industrial and digital landscape is characterized by an unprecedented level of complexity and interdependence. Historically, the management of major industrial risks and the governance of information technology were treated as distinct academic and professional disciplines. Industrial safety focused on the physical containment of hazardous substances and the prevention of mechanical failures, while cybersecurity was relegated to the protection of data and network integrity. However, the contemporary era of "Industry 4.0" and the pervasive digitization of critical infrastructure have fundamentally blurred these lines. A cyberattack on a chemical plant's control system can now lead to a catastrophic physical release, just as a failure in industrial safety protocols can expose sensitive digital data during emergency response.

The theoretical foundation of this study is rooted in the realization that risk is a multi-dimensional construct that transcends the physical-digital divide. In France, the prevention of major industrial accidents has been governed by a robust regulatory framework that emphasizes the "Seveso" directives, yet the 2019 Lubrizol fire in Rouen exposed significant fragilities in state intervention and environmental monitoring (Sénat, 2020). Simultaneously, the global rise in cybercrimes, particularly in developing nations like Nigeria and through sophisticated state-sponsored actors like Salt Typhoon, underscores the fragility of digital ecosystems (Ibrahim et al., 2024; Jaikaran, 2025). The common thread in these disparate events is the failure of governance-a failure to anticipate vulnerabilities and a tendency to rely on reactive policy tools rather than proactive strategic frameworks.

Despite the wealth of literature on individual aspects of safety and security, there is a profound gap in research that integrates these domains into a unified policy framework. Current risk policy tools, particularly in regions like Normandy and Piedmont, remain stubbornly focused on hazards-the external threats-rather than internal vulnerabilities (Tannous et al., 2025). This hazards-focused approach fails to account for the systemic weaknesses in organizational resilience, such as the absence of basic security measures like multi-factor authentication or the mismanagement of third-party vendor risks (Jasper, 2024; Ilori et al., 2024).

This research article seeks to address this gap by synthesizing the lessons learned from post-Lubrizol regulatory evolutions with the strategic imperatives of modern cybersecurity governance. By examining the "Strategic Cybersecurity Governance" model proposed by Nayeem (2025), we can begin to see how risk-based policies can bridge the gap between IT protection and compliance. The introduction of blockchain technology into financial systems also provides a new avenue for balancing data privacy with regulatory mandates, offering a technical solution to a socio-legal problem (Joseph, 2024). The following sections will detail the methodology, analyze the comparative results of risk policy tools, and discuss the future of integrated governance in an increasingly volatile world.

Methodology

The methodology employed in this research is a multi-layered qualitative and comparative analysis designed to capture the complexity of risk governance across different sectors and geographies. The primary approach involves a "systematic review and synthesis" of high-level policy documents, parliamentary inquiry reports, and contemporary cybersecurity research. This allows for the identification of recurring themes, such as the tension between distrust in state services and the mandate for regulatory compliance (Negre, 2021).

To achieve a thorough background on industrial risks, the study utilizes the "French approach to major risk prevention" as a baseline (MEDDE, 2013). This involves analyzing the characteristics, regulations, and prevention strategies outlined in foundational texts on

industrial accidents (Margossian, 2006). The research then moves into a comparative phase, contrasting the risk prevention policy tools used in Normandy (France), Victoria (Australia), and Piedmont (Italy). This specific geographical selection provides a diverse set of governance structures-from highly centralized European models to more decentralized Australian systems-to assess how high-risk sites are managed (Tannous et al., 2024; Tannous et al., 2022).

In the digital domain, the methodology incorporates a "comprehensive audit review" of IT security, focusing on the IT Audit Framework (ITAF) updated by ISACA (2020). The research analyzes the efficacy of various cybersecurity standards and frameworks, such as those provided by IT Governance USA, in the context of real-world hacks (ITGovernance, 2016). The methodology specifically isolates the failure of basic security measures, such as MFA in the Medibank case, to understand the discrepancy between policy existence and policy enforcement (Jasper, 2024).

Theoretical elaboration is achieved by applying a "vulnerability-focused lens" to the collected data. Instead of merely listing types of attacks (hazards), the research categorizes systemic weaknesses such as lack of strategic resilience, third-party mismanagement, and the failure of regulatory oversight during crises (Itani et al., 2024). The study also employs a "pre-mortem" and "post-mortem" analysis of accidents, using the Senate's reports on the Lubrizol fire to evaluate the intervention of state services (Sénat, 2020). By combining these diverse methodological strands, the research creates a publication-ready synthesis that is both theoretically rich and practically relevant.

Evolution of Industrial Risk Policy: From Seveso to Post-Lubrizol

The history of industrial risk policy in Europe, and France in particular, is one of punctuated equilibrium-long periods of stability followed by rapid regulatory change triggered by catastrophe. The "Seveso" directives, named after the 1976 chemical release in Italy, established the standard for high-risk site management. These regulations require operators to identify hazards, implement safety management systems, and prepare internal emergency plans. However, as noted by Margossian (2006), the mere existence of regulation does not guarantee the absence of accidents. The characteristics of major industrial risks-their potential for high impact and low frequency-make them difficult for traditional market mechanisms to manage.

The 2019 Lubrizol factory fire in Rouen marked a turning point in French risk governance. While the accident did not result in immediate fatalities, the environmental, health, and economic consequences were profound, leading to a "crisis of distrust" in state institutions (Negre, 2021). The Senate's inquiry (2020) highlighted significant gaps in the state's ability to monitor the environmental impact of the smoke plume and provide transparent information to the public. This lack of transparency exacerbated public anxiety and led to calls for more stringent oversight.

In response to the Lubrizol fire, the French Ministry of Ecological Transition introduced a series of regulatory evolutions aimed at improving prevention and preparation (Ministry of Ecological Transition, 2020). These changes included stricter requirements for the storage of flammable liquids, increased frequency of inspections, and improved coordination between industrial operators and emergency services. However, a deeper analysis reveals that these changes are often "reactive" rather than "preventive." As Tannous et al. (2022) argue, the chemical and petrochemical industries in France are still "paving the way" toward a truly comprehensive assessment framework. The current tools are designed to manage the "aftermath" rather than fundamentally redesigning the industrial system to reduce vulnerability.

The comparative analysis of Normandy and Victoria reveals that while Normandy has a highly developed "hazards-focused" toolkit-mapping every possible explosion or leak-it lacks the "vulnerabilities-focused" perspective found in some Australian models (Tannous et al., 2024). In Victoria, there is a greater emphasis on land-use planning and the resilience of the surrounding community, recognizing that risk is not just what happens inside the factory fence but how the factory interacts with the social fabric. This distinction is crucial for developing an integrated policy framework that addresses the systemic nature of modern risk.

Strategic Cybersecurity Governance and the Compliance Imperative

As industrial risks evolved, so too did the digital threats facing organizations. The transition from simple network security to "Strategic Cybersecurity Governance" represents a shift from a technical problem to a leadership mandate. Nayeem (2025) posits that a risk-based policy framework is the only way to ensure IT protection and compliance in an era of constant threat. This model moves away from "one-size-fits-all" security checklists toward a dynamic assessment of an organization's specific risk profile.

A critical component of this governance is the role of auditing and compliance. The IT Audit Framework (ITAF) serves as a structured methodology for evaluating the effectiveness of IT controls and ensuring that they align with business objectives and regulatory requirements (ISACA, 2020). However, the "strategic approach to resilience" advocated by Itani et al. (2024) suggests that compliance should not be the end goal but a baseline for continuous improvement. Compliance-heavy organizations often fall into the trap of "box-ticking," where they satisfy auditors but fail to protect themselves against sophisticated attackers.

The Medibank hack in Australia provides a stark illustration of this "compliance gap." The regulator alleged that the absence of a basic cybersecurity measure-multi-factor authentication-led to the breach (Jasper, 2024). In this case, the organization may have been compliant with high-level standards, but it failed in the fundamental hygiene of cybersecurity. This highlights the necessity of "Vulnerability-Focused Governance," which prioritizes the remediation of internal weaknesses over the pursuit of external compliance certifications.

Furthermore, the surge in cybercrimes in Nigeria and the broader African context underscores the importance of national-level cybersecurity strategies. Ibrahim et al. (2024) identify a lack of skilled personnel and inadequate regulatory frameworks as the primary challenges to sustainable development in the region. Without a robust national policy that mandates basic security standards, organizations are left to navigate the "Wild West" of the digital frontier alone. This national strategy must include a focus on "Third-Party Vendor Risks," as most modern breaches occur through the supply chain. Ilori et al. (2024) emphasize that a comprehensive audit review of vendor security is no longer optional; it is a critical component of institutional survival.

Bridging the Gap: Integrating Safety and Security Frameworks

The core thesis of this research is the need for a converged framework that addresses both industrial safety and cybersecurity. The "Strategic Cybersecurity Governance" model (Nayeem, 2025) provides the template, but it must be expanded to include the "physical" components of industrial risk. This integration is essential because the control systems used in modern factories-Supervisory Control and Data Acquisition (SCADA) systems-are increasingly connected to the internet, making them vulnerable to cyber-physical attacks.

A key challenge in this integration is the different languages and metrics used by safety engineers and security analysts. Safety engineers use tools like Fault Tree Analysis (FTA) to predict mechanical failure, while security analysts use threat modeling to anticipate human-led attacks. A truly integrated policy framework must synchronize these approaches. Tannous et al. (2025) provide a starting point by comparing Normandy and Piedmont, showing how hazard maps can be overlaid with vulnerability assessments. By identifying the "critical nodes" where a digital failure leads to a physical catastrophe, organizations can prioritize their security investments.

The use of blockchain technology offers a promising technical bridge in this integrated landscape. Joseph (2024) explores how blockchain can balance data privacy and compliance in financial systems. This same logic can be applied to industrial safety: using immutable ledgers to record safety inspections, equipment maintenance, and sensor data. This would prevent the "falsification" of safety records and provide an untampered "black box" in the event of an accident. In the post-Lubrizol era, where public distrust in state data is high, a blockchain-based monitoring system could restore credibility to environmental reporting.

However, theoretical resistance to this integration remains. Many argue that the "dynamic" nature of cyber threats makes them incompatible with the "static" nature of industrial safety regulations. Counter-

arguments suggest that industrial processes are not as static as they appear and that "Safety 2.0" models already emphasize adaptability and resilience. The "chronic crisis" described by Merad (cited in Tannous et al., 2022) is precisely the result of trying to manage dynamic, modern risks with static, 20th-century tools. The integration of AI-driven cybersecurity with blockchain-enhanced industrial auditing is not a luxury; it is the necessary evolution of governance.

Results

The results of the comparative analysis demonstrate a clear hierarchy of risk policy tools, ranging from the highly prescriptive to the more strategic and flexible. In Normandy, the "Risk Prevention Plans" (PPRT) are the dominant tool. These are legally binding documents that restrict land use around Seveso sites and mandate physical protective measures. While effective at reducing the consequences of a "standard" accident, they are ill-equipped to handle non-standard events like the Lubrizol fire, where the interaction of different chemical products created unforeseen toxicities.

In Victoria, Australia, the "Safety Case" regime is used. This requires operators to "demonstrate" to the regulator that they have identified all major hazards and implemented effective controls. This is a more flexible, goal-based approach than the French prescriptive model. The analysis shows that the Safety Case regime is better at fostering a "safety culture" within organizations, as it forces leadership to engage with the specifics of their risk profile. However, it requires a highly skilled and well-resourced regulator to verify the claims made by operators-a resource that is not always available (Tannous et al., 2024).

In the cybersecurity domain, the analysis of IT Audit Frameworks across several sectors shows a high degree of "fragmentation." Organizations often juggle multiple standards-ISO 27001, NIST, ITAF-leading to "compliance fatigue." The results indicate that organizations that adopt a "Strategic Cybersecurity Governance" model (Nayeem, 2025) perform significantly better in breach detection and response. This is because the model emphasizes "Resilience" over "Perimeter Defense." Instead of trying to keep everyone out, these organizations assume a breach will occur and focus on minimizing the impact through rapid detection and compartmentalization.

The evaluation of state intervention during the Lubrizol crisis (Sénat, 2020) reveals that the "human factor" is the weakest link in governance. Even with the best policy tools, the failure to communicate effectively during a crisis led to a breakdown in public trust. This result is echoed in the Medibank hack, where the regulator's scathing assessment focused on the failure of leadership to enforce basic security hygiene (Jasper, 2024). These findings suggest that the most effective risk policy tool is not a document or a piece of software, but a culture of "accountability and transparency."

Discussion

The discussion centers on the theoretical implications of the "chronic crisis" in risk prevention. Merad (cited in Tannous et al., 2025) suggests that society is in a state of permanent crisis because our governance structures are fundamentally misaligned with the nature of modern risk. We treat accidents as "anomalies" to be investigated and regulated, rather than as "inherent properties" of complex systems. This "hazards-focused" worldview ignores the reality that our vulnerabilities are systemic and interconnected.

A major theme in the discussion is the role of "distrust" in modern risk governance. Negre (2021) points out that in the aftermath of the Lubrizol fire, the public did not just distrust the industrial operator; they distrusted the state itself. This distrust is a significant barrier to effective policy implementation. If the public does not believe the data provided by the state, they will not comply with evacuation orders or health recommendations. This theoretical insight suggests that "transparency" must be a core pillar of any integrated risk framework.

Furthermore, the surge in cybercrimes like the Salt Typhoon hack of telecommunications companies (Jaikaran, 2025) shows that the "attack surface" is now the entire nation. When telecommunications systems are compromised, the federal response must be strategic rather than tactical. This leads to a discussion of "Sovereign Cybersecurity," where the state's role is not just to regulate private industry but to actively defend the national digital infrastructure. The Nigeria case study (Ibrahim et al., 2024) illustrates the

consequences of failing to achieve this sovereignty.

The future scope of this research lies in the development of "Algorithmic Governance." As AI and machine learning are increasingly used to monitor both industrial processes and digital networks, the governance of the algorithms themselves becomes paramount. Who is responsible when an AI system fails to detect a gas leak or misses a cyber intrusion? The integration of "Blockchain-Based Auditing" (Joseph, 2024) could provide the accountability needed for algorithmic governance, but it requires a new set of international standards and ethical frameworks.

Conclusion

In conclusion, this research has demonstrated that the silos between industrial safety and cybersecurity governance are a major source of systemic vulnerability. The lessons from the Lubrizol fire and high-profile cyber breaches like Medibank and Salt Typhoon all point toward a single conclusion: our current risk policy tools are too reactive and too focused on external hazards. To achieve true resilience, we must transition toward a "Strategic Cybersecurity Governance" model that integrates both physical and digital risks into a unified, vulnerability-focused policy framework.

The "French approach" to major risks, while robust in its prescriptive requirements, must be augmented with the flexibility and leadership focus of the "Safety Case" and "Strategic Governance" models found in other jurisdictions. This requires a shift in organizational culture-from "box-ticking" compliance to a culture of accountability, transparency, and continuous resilience. The use of emerging technologies like blockchain and AI offers the technical means to achieve this, but only if they are implemented within a sound socio-legal framework that prioritizes public trust.

Ultimately, the goal of this integrated governance is not just the prevention of accidents or the stopping of hacks, but the preservation of our societal stability and the protection of our sustainable development goals. As the physical and digital worlds continue to converge, the "chronic crisis" of risk will only deepen unless we redefine what it means to be "secure." The roadmap provided by Nayeem (2025), Tannous (2024), and Joseph (2024) offers a path forward-a path that leads toward a future where our most complex systems are governed by our most sophisticated and integrated policies.

References

1. Ibrahim, Y. A., Ishaya, A. O., Yusuf, M., Nancy, I., Bijik, H. A., & Aiyedogbon, S. F. (2024). Cybersecurity and Cybercrimes in Nigeria: An Overview of Challenges and Prospects. 2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG).

2. Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. World Journal of Advanced Research and Reviews.

3. ISACA. (2020). ISACA Updates IT Audit Framework (ITAF).

4. Itani, D., Itani, R., Eltweri, A. A., Faccia, A., & Wanganoo, L. (2024). Enhancing Cybersecurity Through Compliance and Auditing: A Strategic Approach to Resilience. 2024 2nd International Conference on Cyber Resilience (ICCR).

5. ITGovernance. (2016). Cybersecurity Standards and Frameworks | IT Governance USA.

6. Jaikaran, C. (2025). Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications. Congress.gov.

7. Jasper, C. (2024). The absence of a basic cybersecurity measure led to the Medibank hack, regulator alleges. ABC News.

8. Joseph, S. A. (2024). Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems. Journal of Engineering Research and Reports.

9. Margossian, N. (2006). Risques et accidents industriels majeurs: Caractéristiques, réglementation, prévention. Dunod.

10. Ministère de l'Écologie, du Développement Durable et de l'Énergie (MEDDE). (2013). La démarche française de prévention des risques majeurs.

11. Ministry of Ecological Transition. (2020). Les évolutions réglementaires post-lubrizol sur la prévention et la préparation à la gestion des accidents, en un coup d'œil.

12. Mohammed Nayeem (2025). Strategic Cybersecurity Governance: A Risk-Based Policy Framework for IT Protection and Compliance. In Proceedings of the International Conference on Artificial Intelligence and Cybersecurity (ICAIC 2025).

13. Negre, E. (2021). Crisis management and distrust: study of an industrial accident in France. Proceedings of the 54th Hawaii International Conference on System Sciences.

14. Sénat. (2020). Évaluer l'intervention des services de l'État dans la gestion des conséquences environnementales, sanitaires et économiques de l'incendie de l'usine Lubrizol à Rouen. Tome I: Rapport & Tome II: Auditions.

15. Tannous, S., Merad, M., & Hayes, J. (2022). Major accidents and risk prevention policies in the chemical and petrochemical industry in France: Paving the way towards an assessment framework. Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022).

16. Tannous, S., Merad, M., & Hayes, J. (2024). A comparative analysis of risk prevention policy tools and governance structures in Normandy (France) and Victoria (Australia): assessing policies for high-risk sites. Int. J. Disaster Risk Reduct.

17. Tannous, S., Castro Rodriguez, D. J., Merad, M., & Demichela, M. (2025). Risk policy tools for high-risk industrial sites in Normandy (France) and Piedmont (Italy): more hazards-focused than vulnerabilities-focused. J. Risk Res.