Section 1.1. Essence and Evolution of the Insider Threat Concept in Corporate Systems

Paulina Kolisnichenko[1]

[1]*Ph.D.(Economics), Vice Rector for International Cooperation, WSHIU University, Poznan, Poland, e-mail: paulina.kolisnichenko@wshiu.pl, ORCID: https://orcid.org/0000-0001-6730-1236*

Citation:
Kolisnichenko, P. (2025). Essence and evolution of the insider threat concept in corporate systems. In P. Kolisnichenko (Ed.), *Insider threats and security in corporations.* 274 p. (pp. 9–31). Scientific Center of Innovative Research. https://doi.org/10.36690/ITSC-9-31

This monograph`s chapter is an open access monograph distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC 4.0) license

OPEN ACCESS

Abstract. *In the twenty-first century, the digitalization of corporate systems and the globalization of supply chains have expanded the concept of security beyond traditional cyber defense. Insider threats – actions by employees, contractors, or trusted partners that compromise organizational integrity – have become a multidimensional governance challenge. This monograph explores the evolution, theoretical frameworks, and cross-jurisdictional variations of insider threat management within modern corporations. Its main goal is to provide a comprehensive understanding of how behavioral, engineering, and governance approaches integrate into a unified system of resilience capable of anticipating and mitigating insider risks. The methodology combines a structured literature review, comparative analysis, and synthesis of international standards and case studies. Sources include academic research, cybersecurity frameworks, and national strategies from the United States, European Union, East Asia, Latin America, the United Arab Emirates, and Israel. The analysis systematizes theoretical perspectives into three dominant approaches: the behavioral, focusing on psychosocial precursors and early detection; the engineering, emphasizing technical and data-driven controls; and the governance, framing insider threats as failures of ethics, accountability, and leadership. The results demonstrate that insider threats evolve alongside technological and societal change: from Cold War–era espionage and sabotage to modern socio-technical and hybrid risks. Jurisdictional comparison reveals diverse governance logics – compliance and deterrence in the United States; privacy and ethics in the European Union; collectivist responsibility in East Asia; adaptive compliance in Latin America; centralized oversight in the UAE; and innovation protection in Israel. Despite their differences, all systems converge on a hybrid model that integrates behavioral analytics, AI-based monitoring, and ethical governance. The conclusion emphasizes that the future of insider threat management lies in predictive resilience – the capability to anticipate, contextualize, and ethically manage internal risks. Future research should focus on developing adaptive frameworks that embed insider threat intelligence into ESG reporting, cross-border governance, and AI-driven foresight systems, ensuring that corporate security becomes inseparable from organizational trust and sustainability.*

Keywords: *insider threats; corporate security; governance frameworks; behavioral analytics; cybersecurity management; hybrid threats; organizational resilience; ethical leadership; information protection; global compliance; risk management; digital transformation.*

ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

1. Evolution and Conceptual Broadening. The notion of *insider threat* has undergone a profound conceptual and methodological evolution, reflecting the dynamic changes in corporate governance, information security, and digital transformation. In the 1970s and 1980s, insider threats were primarily associated with deliberate sabotage or espionage conducted by employees or contractors possessing legitimate access to sensitive information (Anderson, 1972; Parker, 1981). This early perspective was grounded in the logic of *technical control* – securing systems through access restriction, surveillance, and legal sanctions. As corporations transitioned toward information-driven economies, the insider threat became understood as a socio-technical and behavioral problem that cannot be addressed solely through technological solutions (Colwill, 2009).

The evolution of the insider threat concept reflects a continuous shift in how organizations and scholars perceive the balance between trust and control in complex systems. This evolution can be divided into four major stages, each corresponding to technological, organizational, and socio-political transformations that redefined the nature of insider risk (Figure 1.1).

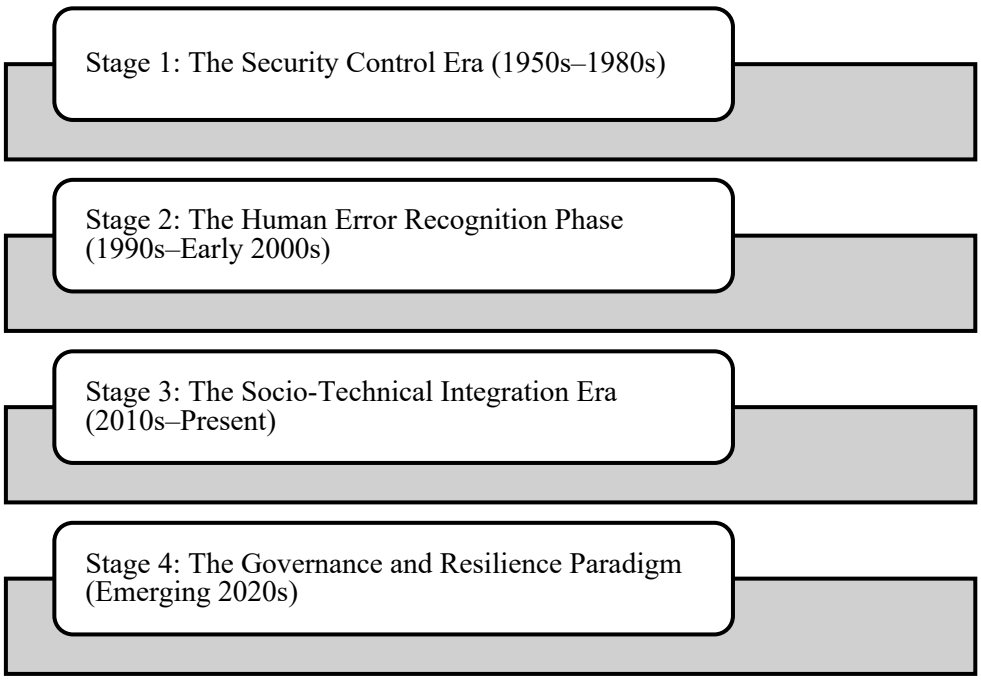


Figure 1.1. The Four Major Stages of Insider Threat Concept Evolution

Source: systematized by the author

Stage 1: The Security Control Era (1950s–1980s). In the earliest phase, insider threats were conceptualized narrowly as acts of deliberate espionage or sabotage by employees with privileged access to classified or proprietary

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

information. This perspective emerged in the context of the Cold War, when industrial espionage and information leaks were viewed primarily through a national security lens. Early works by Anderson (1972) and Parker (1981) framed the insider as a *malicious actor* motivated by ideology, revenge, or personal gain.

Organizations at this time operated in closed environments where information was centralized and physical security dominated. Security management was procedural and hierarchical – focused on limiting access through clearance systems and monitoring employee loyalty. The "trust but verify" principle guided corporate and government policy, assuming that loyalty could be assessed and controlled through background checks and supervision. This stage thus represented a compliance-oriented and punitive paradigm, where insider activity was treated as deviance to be detected and punished rather than as a systemic risk to be managed.

Stage 2: The Human Error Recognition Phase (1990s–Early 2000s). The diffusion of information technologies and the rise of digital enterprises in the 1990s transformed the insider threat landscape. As organizations digitized workflows, human error and negligence became dominant causes of security incidents. Scholars such as Colwill (2009) and Shaw and Fischer (2005) emphasized that unintentional insiders – those who inadvertently disclosed data or failed to follow security protocols – posed risks equal to or greater than malicious actors.

This stage marked a paradigm shift from intent to impact, recognizing that damage could occur regardless of motive. Security frameworks began integrating *human factors engineering*, emphasizing user training, ergonomic system design, and awareness campaigns. Behavioral science also entered the discourse, exploring how stress, cognitive overload, and unclear communication contributed to security lapses. Corporations began investing in internal education programs and incident response teams that combined technical and psychological expertise.

Stage 3: The Socio-Technical Integration Era (2010s–Present). The early 2010s witnessed an unprecedented convergence of digitalization, globalization, and remote connectivity. Insider threats were no longer confined to physical spaces or individual actions; they became systemic and networked, operating within complex socio-technical ecosystems. The CERT Insider Threat Center at Carnegie Mellon University (Cappelli et al., 2012) and the NIST (2021) frameworks formalized a comprehensive definition encompassing *malicious, negligent, and unintentional* insider actions.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

This stage introduced hybrid threats, where insiders collaborated with or were manipulated by external actors through social engineering, financial coercion, or ideological radicalization. The boundary between "insider" and "outsider" became porous, requiring integrated detection mechanisms across departments. Organizations started to adopt *User and Entity Behavior Analytics (UEBA)*, *Security Information and Event Management (SIEM)* systems, and *machine learning algorithms* to identify deviations from normative behavior.

At the same time, ethical considerations gained prominence. Surveillance-based approaches risked eroding employee trust, raising questions about privacy, proportionality, and data protection – especially under the European Union's General Data Protection Regulation (GDPR). Hence, the socio-technical era emphasized balance: protecting the organization while preserving ethical standards and employee autonomy.

Stage 4: The Governance and Resilience Paradigm (Emerging 2020s). In the post-pandemic and hybrid-work context, the insider threat is increasingly perceived as a governance challenge intertwined with organizational culture, leadership ethics, and strategic resilience. Corporations now operate within globally distributed teams, cloud infrastructures, and inter-organizational networks where access rights are fluid and accountability is diffused. This shift has transformed insider risk management into a *strategic component* of corporate governance and enterprise risk management (ERM).

The governance paradigm integrates behavioral analytics, technical surveillance, and ethical leadership into a holistic framework. Organizations adopt *zero-trust architectures* – a principle assuming no implicit trust even within the corporate perimeter – and emphasize continuous verification, accountability, and data transparency (ISO/IEC, 2022). In parallel, insider threat programs are embedded within ESG (Environmental, Social, Governance) structures, linking ethical corporate behavior with digital responsibility and stakeholder trust (Greitzer et al., 2021).

The future trajectory of insider threat management lies in predictive resilience: the ability to anticipate insider risk through data-driven foresight, early intervention, and corporate empathy. The insider is thus reconceived not solely as a risk factor but as an integral part of a living organizational system where security, trust, and ethics must coexist dynamically.

The historical trajectory of insider threat studies reveals a deepening understanding of the phenomenon's multi-layered nature. The focus has expanded from individual intent to systemic vulnerability, and from reactive punishment to proactive governance. Each stage introduced new conceptual

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

tools: psychological models, human-factor engineering, analytics-based monitoring, and strategic resilience frameworks.

Table 1.1. Evolution of the Insider Threat Concept in Corporate Systems

Stage	Historical Period	Dominant Perspective	Core Features	Representative Sources
1. Security Control Era	1950s–1980s	Insider as malicious actor	Focus on espionage and sabotage; hierarchical control; punishment	Anderson (1972); Parker (1981)
2. Human Error Recognition	1990s–2000s	Insider as negligent or unaware	Emphasis on human factors, training, and procedural design	Colwill (2009); Shaw & Fischer (2005)
3. Socio-Technical Integration	2010s–Present	Insider as part of complex socio-technical systems	Hybrid threats; UEBA and AI-driven monitoring; privacy dilemmas	Cappelli et al. (2012); Greitzer & Frincke (2010); NIST (2021)
4. Governance and Resilience Paradigm	2020s onward	Insider risk as governance challenge	Zero-trust architecture; ESG integration; predictive resilience	ENISA (2023); ISO/IEC (2022); Nurse (2022)

Source: systematized by the author

In contemporary corporate systems, insider threats are no longer confined to isolated actors or singular incidents. They represent *emergent properties* of complex organizations where governance gaps, technological interdependencies, and human factors intersect. Addressing these threats therefore requires not only technical sophistication but also ethical foresight, cross-disciplinary collaboration, and a culture of shared responsibility. The insider threat, in its modern interpretation, is ultimately a mirror of the corporation's internal coherence, moral integrity, and adaptive capacity in an era of digital interdependence.

2. Theoretical Approaches to Insider Threats. The literature identifies three complementary but distinct theoretical approaches: behavioral, engineering, and governance. Each provides insight into different mechanisms through which insider risks materialize and propagate within organizations.

The Behavioral Approach. The behavioral approach examines insider threats through the lens of psychology, criminology, and organizational behavior. It posits that insider misconduct is rarely spontaneous; rather, it develops progressively along identifiable behavioral and emotional trajectories. Early behavioral models, such as Shaw and Fischer's (2005)

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

Critical Path Model, demonstrated that insiders often experience a combination of personal grievances, perceived injustice, and rationalization before committing a harmful act. This model builds upon criminological theories like *strain theory* and *social learning theory*, suggesting that environmental stressors – workplace conflict, career stagnation, or moral disengagement – can erode employee loyalty and foster deviant behavior.

Behavioral research emphasizes that insider actions are embedded within social contexts. Studies by Greitzer and Frincke (2010) reveal that observable precursors, such as withdrawal, declining performance, or vocalized dissatisfaction, often precede security breaches. Similarly, emotional distress, burnout, or financial pressure can act as catalysts, especially when organizational communication is weak. This approach underscores the necessity of early detection through behavioral monitoring, psychological support programs, and employee well-being initiatives.

Contemporary developments in this field incorporate machine learning and natural language processing to identify patterns of sentiment, abnormal communication, and social network changes among employees. However, scholars caution against reducing behavioral analysis to mere surveillance. Effective behavioral management must balance predictive insight with privacy and ethical responsibility, integrating psychological safety and trust into corporate governance (Nurse, 2022).

The Engineering Approach. The engineering approach conceptualizes insider threats as *systemic vulnerabilities* arising from inadequate control of access, identity, and information flows. This perspective treats insiders not solely as human actors but as entities interacting with complex digital infrastructures. The approach originates from information assurance frameworks that aim to ensure *confidentiality, integrity, and availability* through layered defense mechanisms (Liu et al., 2018).

Central to this paradigm are *User and Entity Behavior Analytics (UEBA)* systems, which employ statistical modeling and machine learning to detect deviations from established behavioral baselines. For example, unusual data transfers, after-hours access, or anomalous login patterns may indicate potential insider compromise. Data Loss Prevention (DLP) systems, identity governance tools, and continuous authentication protocols further enhance this architecture.

This approach aligns with international standards such as ISO/IEC 27001:2022 and NIST SP 800-53, both of which prescribe continuous risk assessment, privilege minimization, and audit logging. In advanced applications, engineering models integrate artificial intelligence to correlate

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

technical anomalies with behavioral indicators, producing composite risk scores for each user.

While the engineering approach offers scalability and precision, critics argue that its technical focus may overlook contextual and cultural dimensions of insider behavior. Excessive reliance on automated analytics can generate false positives, leading to employee distrust or privacy infringements. Therefore, modern practice recommends a *socio-technical synthesis* – combining engineering controls with behavioral interpretation and ethical oversight.

The Governance Approach. The governance approach expands the discussion beyond technical systems and individual psychology to the institutional level of corporate integrity, ethics, and leadership. It views insider threats as manifestations of governance failure – specifically, the breakdown of accountability, transparency, and ethical culture within organizations (Hunker & Probst, 2011). This approach aligns with corporate governance theories emphasizing stewardship, stakeholder engagement, and internal control frameworks such as COSO ERM.

From a governance standpoint, insider risks are not only operational hazards but strategic vulnerabilities affecting reputation, shareholder value, and legal compliance. Weak internal audit mechanisms, insufficient segregation of duties, and lack of ethical training can foster environments conducive to insider misconduct. Boards of directors play a crucial role in setting the "tone at the top," ensuring that ethical values are embedded in performance evaluation and risk management systems (Cappelli et al., 2012).

Governance-oriented insider threat programs integrate ethical leadership, whistleblowing policies, and employee empowerment mechanisms. By fostering psychological safety, organizations encourage early reporting of misconduct and reduce the temptation for retaliation or collusion. This approach is particularly effective in multinational corporations, where decentralized structures require strong ethical alignment across diverse cultural settings.

However, the governance approach faces implementation challenges. Ethical cultures cannot be imposed mechanically; they require consistent reinforcement through leadership modeling, transparent communication, and fair treatment. Furthermore, balancing surveillance and trust remains a delicate governance dilemma – overcontrol can erode morale, while undercontrol can expose the enterprise to severe financial and reputational losses.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

Table 1.2. Comparative Overview of the Three Approaches

Approach	Core Focus	Primary Tools and Methods	Institutional Level	Advantages	Limitations
Behavioral	Human motives, psychosocial and cognitive factors	Psychological profiling, sentiment analysis, HR data integration	Individual and interpersonal	Early detection of stress and discontent; supports prevention	Privacy and ethical concerns; subjective interpretation
Engineering	Technical and system-level vulnerabilities	UEBA, DLP, access control, machine learning, audit trails	Technological and operational	High scalability, real-time detection, quantifiable results	Ignores human context; potential false positives
Governance	Ethical culture, leadership accountability, institutional integrity	Whistleblowing systems, ethics codes, internal audit, compliance reporting	Strategic and organizational	Aligns ethics, risk management, and strategy; strengthens trust	Difficult to measure; dependent on leadership quality

Source: systematized by the author

In modern corporations, the most effective insider threat management strategies combine these three approaches into a *multi-layered defense model*. Behavioral analysis identifies psychological and social precursors; engineering mechanisms detect anomalous digital activity; and governance ensures ethical oversight and accountability. This integration is consistent with the principles of *defense-in-depth*, where organizational, technical, and human layers jointly mitigate risk (NIST, 2021).

Moreover, the corporate landscape increasingly features *hybrid insider threats* – situations in which internal actors collaborate with external adversaries or are manipulated through financial incentives, coercion, or ideological motives. Such hybridization blurs the traditional boundary between insider and outsider, demanding cross-functional coordination between cybersecurity, HR, and compliance divisions.

The convergence of digital transformation, remote work, and global supply chains has made insider threats both more probable and more difficult to detect. As a result, insider threat programs now form an integral component of enterprise risk management, directly influencing corporate reputation, investor confidence, and regulatory compliance. In this sense, managing insider threats is not merely a matter of technical security but a reflection of an organization's ethical maturity and strategic resilience.

3. Insider Threats in Corporate Environments Across Jurisdictions. In the twenty-first century, globalization and digital

https://doi.org/10.36690/ITSC
ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

interdependence have redefined the boundaries of corporate security. As businesses expand across continents, insider threats have become a universal yet context-specific challenge that manifests differently across legal systems, governance traditions, and cultural norms. The complexity of managing insider risks now extends beyond technological controls, requiring an understanding of the social structures, labor relations, and institutional ethics within each jurisdiction.

The manifestation of insider threats and the strategies for their mitigation differ markedly among jurisdictions, reflecting distinctive regulatory architectures, governance models, and cultural perceptions of power, trust, and confidentiality. A comparative analysis of key global regions – the United States, the European Union, East Asia, Brazil and Latin America, the United Arab Emirates, and Israel – demonstrates how regulatory philosophies and organizational cultures shape the architecture of insider threat management programs.

The analysis demonstrates how cultural constructs – such as individual responsibility, collective loyalty, or hierarchical discipline – intersect with legal frameworks for privacy, data protection, and cybersecurity, ultimately shaping distinct national paradigms of corporate resilience.

The United States. In the United States, insider threat management has evolved within a strong compliance and national security tradition. Federal directives, particularly those emerging from the Department of Defense (DoD), the National Insider Threat Task Force (NITTF), and NIST's Special Publications, define standardized protocols for identifying, reporting, and mitigating insider risks (NIST, 2021). These frameworks are mandatory for defense contractors, critical infrastructure operators, and government-affiliated corporations, where insider threats are viewed as potential breaches of national security and economic competitiveness.

U.S. corporations typically employ *centralized Insider Threat Programs (ITPs)* that integrate behavioral, digital, and forensic analytics. Advanced User and Entity Behavior Analytics (UEBA) systems analyze activity logs, network traffic, and communication metadata to flag anomalies. The corporate governance model emphasizes accountability, documentation, and auditability – core principles of the Sarbanes–Oxley Act and other compliance regimes. Consequently, American companies tend to prioritize *early detection and deterrence* over rehabilitation or prevention through education.

However, this approach has been critiqued for its invasive nature and potential tension with employee privacy rights. Research indicates that continuous monitoring and punitive enforcement may erode organizational

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

trust, creating adversarial relationships between employees and management (Greitzer et al., 2021). In response, modern U.S. corporations, particularly in the tech sector, increasingly integrate well-being programs and ethical communication frameworks alongside technical surveillance, aiming to achieve a balanced, human-centered approach to insider risk mitigation.

The European Union. The European Union (EU) adopts a markedly different philosophy grounded in human rights, data protection, and participatory governance. The regulatory foundation lies in the General Data Protection Regulation (GDPR), NIS2 Directive, and ENISA (European Union Agency for Cybersecurity) guidelines, which collectively promote privacy, transparency, and proportionality in security practices (ENISA, 2023). In this model, insider threat management is treated as part of broader corporate risk governance and organizational ethics, rather than solely as a cybersecurity problem.

European corporations focus on prevention through awareness, engagement, and ethical culture-building. Insider threat programs must adhere to privacy-by-design principles, ensuring that data collection for monitoring is both minimal and justified. ENISA encourages the establishment of "*insider threat councils*," which include representatives from HR, legal, IT, and labor unions, reflecting the EU's social dialogue tradition. This collaborative governance structure positions insider threat mitigation within the framework of trust and cooperation, emphasizing restorative rather than punitive approaches.

In practice, European corporations invest in employee education, digital literacy, and psychological safety mechanisms. For instance, multinational firms headquartered in Germany or the Netherlands routinely implement *ethics hotlines*, anonymous reporting systems, and internal mediation platforms. These tools enable early identification of grievances or misconduct without stigmatization. The EU's distinctive contribution lies in its commitment to privacy-preserving analytics, where AI and behavior-monitoring tools are subject to algorithmic transparency and human oversight.

East Asia. In East Asian corporate systems – particularly in Japan, South Korea, China, and Singapore – the insider threat paradigm is deeply influenced by cultural values such as loyalty, hierarchy, collective harmony, and social obligation. Corporations tend to rely on internal cohesion and personal accountability rather than on automated surveillance or punitive controls (Kim & Park, 2020). The Japanese concept of *wa* (harmony) and the Korean principle of *jeong*(emotional loyalty) shape organizational cultures

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

where insiders often identify closely with the company's mission and leadership.

This cultural embeddedness provides both advantages and vulnerabilities. High levels of employee commitment reduce the likelihood of deliberate sabotage; however, excessive deference to authority can discourage the reporting of unethical or negligent behavior. As a result, insider incidents in East Asia are frequently underreported or resolved internally, outside formal legal channels. In China, corporate security systems are evolving rapidly in response to national cybersecurity laws emphasizing data sovereignty and government oversight. Chinese corporations increasingly deploy AI-enabled monitoring, yet such systems remain closely aligned with state regulations rather than independent corporate governance standards.

East Asian corporations thus operate within a hybrid model that combines cultural control mechanisms with emerging technological surveillance. Companies in Japan and South Korea have begun adopting Western-style compliance frameworks but often adapt them to local contexts by prioritizing moral education, corporate loyalty programs, and lifetime employment incentives as preventive measures. The most advanced models – seen in Singapore – integrate behavioral analytics with leadership ethics programs, striking a balance between traditional collectivism and modern governance efficiency.

Despite these differences, the globalization of digital commerce and transnational regulation is fostering convergence among jurisdictions. U.S. compliance frameworks are gradually integrating ethical and human-centric elements, while EU corporations are adopting technical controls to manage rising cyber-physical integration. East Asian models, meanwhile, are transitioning from cultural reliance to *codified security governance*, influenced by ISO/IEC 27001 adoption and cross-border trade requirements.

A key unifying trend is the rise of zero-trust architecture and data governance frameworks that emphasize continual verification and cross-functional oversight. The global movement toward ESG-based governance further aligns insider threat management with corporate responsibility, sustainability, and transparency. Consequently, corporations worldwide are converging toward a hybrid model – combining U.S. technical rigor, European ethical governance, and East Asian collectivist coherence – to achieve balanced, resilient, and adaptive insider threat management in the digital age.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

Table 1.3. Comparative Framework of Insider Threat Management by Jurisdiction of United States, European Union and East Asia

Dimension	United States	European Union	East Asia (Japan, South Korea, China, Singapore)
Regulatory Orientation	Compliance- and surveillance-driven (DoD, NIST, NITTF)	Rights-based and privacy-oriented (GDPR, ENISA, NIS2)	State-regulated or culturally mediated (National Cybersecurity Laws)
Cultural Foundation	Individual responsibility, competition, deterrence	Collective trust, transparency, ethical governance	Hierarchy, loyalty, group harmony
Institutional Mechanisms	Centralized Insider Threat Programs; technical monitoring	Cross-departmental councils; privacy-preserving analytics	Internal mediation; loyalty programs; limited disclosure
Primary Focus	Detection, investigation, and accountability	Prevention, education, and ethical culture	Moral responsibility and internal discipline
Advantages	High detection capability, strong legal structure	High trust and compliance with human rights	Deep employee loyalty and low malicious intent
Challenges	Privacy risks, potential over-surveillance	High cost of compliance, slower response times	Underreporting, limited transparency, state dependency

Source: systematized by the author

Brazil and Latin America. Latin American corporations operate in environments marked by regulatory fragmentation, uneven enforcement capacity, and pronounced exposure to fraud and corruption risks. Brazil sets a regional reference point due to the General Data Protection Law (Lei Geral de Proteção de Dados, LGPD) and the Marco Civil da Internet, which together have elevated corporate attention to data governance, privacy, and accountability. Insider threat programs in Brazil increasingly connect cybersecurity monitoring with compliance, internal audit, and integrity functions that were catalyzed by anti-corruption reforms and high-profile enforcement actions. In practice, companies in finance, payments, and agribusiness face insider risks that concentrate around data exfiltration, procurement manipulation, and privileged access misuse, particularly at the interfaces between enterprise systems and third-party vendors.

Organizational culture in Brazil often relies on dense interpersonal networks, collaborative teams, and relationship-driven business development. These strengths can become vulnerabilities when gatekeepers accumulate informal power or when favor-based decisions erode segregation of duties. Mature firms counter these effects through clear role design, rotation of sensitive functions, and the use of behavior-based analytics that correlate HR signals with access telemetry. Labor protections and strong union presence shape monitoring practices, therefore companies invest in

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

privacy impact assessments and transparent communications to maintain trust. Incident handling is trending toward integrated security operation centers that share indicators with sectoral information sharing groups and the national incident response community.

Across Spanish-speaking Latin America, large listed companies have moved toward global standards such as ISO 27001 and COSO ERM, yet adoption remains uneven among mid-market firms. Vendor concentration, legacy systems, and complex supply chains create opportunity structures for insider collusion that combine corporate actors with external facilitators. The most effective programs in the region emphasize ethics training that is context-aware, vendor due diligence with continuous control testing, and case management workflows that allow confidential reporting without retaliation. Where judicial processes are slow, internal remediation mechanisms and negotiated separations are used to contain damage and preserve evidence for potential future action. The regional trajectory points toward gradual convergence with European privacy practices and North American technical controls, supported by growing fintech regulation and cross-border data transfer requirements.

United Arab Emirates. The UAE aligns insider threat management with national critical infrastructure protection and state priorities for digital transformation. Corporations in energy, aviation, logistics, and financial services implement prescriptive control baselines derived from national and sectoral standards, complemented by data protection requirements in free-zone jurisdictions such as DIFC and ADGM. Board oversight tends to be formalized, and security leaders maintain close coordination with government regulators and national cyber authorities. This creates strong incentives for technical rigor, detailed audit trails, and rapid incident reporting.

Workforce composition influences risk. Many organizations rely on multinational teams and contracted personnel, which increases churn at sensitive access points and expands exposure to onboarding and offboarding failures. Progressive firms mitigate these issues with identity lifecycle automation, just-in-time privilege elevation, and continuous authentication. Cultural norms favor clear hierarchy and explicit accountability, which supports decisive action once indicators cross predefined thresholds. At the same time, trust and employer reputation are protected through codified processes for evidence handling, due process, and respectful separation when misconduct is confirmed.

Programmatically, leading UAE firms combine behavior analytics with process controls that restrict toxic combinations of access across enterprise

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

resource planning, trading, and operational technology networks. Executive committees receive consolidated risk dashboards that integrate insider telemetry with third-party and fraud indicators. Investment in insider threat tabletop exercises is common in critical sectors, often paired with crisis communication playbooks that address regulatory, client, and public expectations. The UAE model illustrates how centralized policy, strong sector regulators, and high digital ambition can accelerate insider maturity when governance and technical controls evolve together.

Israel. Israeli corporations bring a distinctive security culture shaped by a deep national cyber ecosystem, high levels of R&D intensity, and rapid talent mobility between start-ups, multinationals, and academia. Insider threats here are viewed through a counterintelligence and intellectual property protection lens, with emphasis on research leakage, code exfiltration, and commercialization of sensitive know-how. Organizations adopt advanced user and entity behavior analytics early, integrate code provenance and repository monitoring into DevSecOps, and enforce granular secrets management in cloud environments. Flat organizational structures and fast iteration cycles benefit innovation, yet they also increase the likelihood that a single engineer controls critical pathways. Companies respond with automated peer review gates, service ownership maps, and access reviews that focus on toxic combinations rather than static role labels.

Legal obligations for data security and incident handling are complemented by sector guidance and an active national incident response community. Boards in technology-intensive firms receive detailed metrics on insider exposure, including time to deprovisioning, anomalous repository access, and correlates of employee disengagement. Ethics and culture are addressed through founder-led communication about stewardship of intellectual property, and through transparent policies that distinguish legitimate mobility from misuse of confidential assets. Because talent markets are highly competitive, prevention programs prioritize employee experience and trust, which reduces incentive for grievance-driven behavior while maintaining strong deterrence for deliberate misconduct.

Multi-national enterprises with Israeli R&D centers often deploy split-key or attribute-based access for sensitive projects, and they segregate client data from research environments to minimize spillover risk. Collaboration with universities and start-ups is supported by contractual controls that standardize IP ownership and exit hygiene, which narrows the gray areas that typically complicate insider investigations. The Israeli model demonstrates how high technical capability, strong leadership attention to IP stewardship,

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

and mature incident response can curb insider risk without suppressing innovation.

Table 1.4. Comparative Framework of Insider Threat Management by Jurisdiction of Brazil and Latin America, United Arab Emirates and Israel

Dimension	Brazil and Latin America	United Arab Emirates	Israel
Regulatory anchor	LGPD, sectoral rules, anti-corruption frameworks, emerging fintech oversight	National and sector standards, free-zone data protection, critical infrastructure mandates	Data security law, sector guidance, strong national CERT ecosystem
Cultural context	Relationship-based business, union influence, need for transparent monitoring	Hierarchical accountability, multinational workforce, regulator engagement	High R&D intensity, rapid talent mobility, founder-driven security culture
Dominant insider patterns	Procurement and vendor collusion, data exfiltration, finance and agribusiness fraud	Privileged access misuse in OT and finance, onboarding or offboarding gaps, third-party exposure	IP and code leakage, repository abuse, startup to competitor transfer risk
Core controls in practice	Ethics programs, vendor due diligence, rotation of sensitive roles, SOC integration	Identity lifecycle automation, toxic-combination control, executive dashboards, exercises	UEBA integrated with DevSecOps, split-key and attribute-based access, exit hygiene controls
Program challenges	Uneven maturity across mid-market firms, legacy systems, slow legal processes	Managing high contractor turnover, balancing speed with strong evidence standards	Balancing openness for innovation with stringent IP safeguards, preventing privilege creep
Strategic emphasis	Convergence with global standards, privacy-aware monitoring, integrity and audit alignment	Centralized policy plus sector depth, crisis readiness, measurable board oversight	IP stewardship, rapid detection, trust-preserving prevention in competitive talent markets

Source: systematized by the author

The Table 1.4 illustrates how regional contexts shape distinct yet complementary philosophies of insider threat management. While all three operate within rapidly digitizing economies, each jurisdiction integrates insider protection into its governance architecture through different strategic priorities.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

In Latin America, insider threat governance is evolving as part of a broader integrity and compliance agenda driven by anti-corruption reforms and data protection legislation. Programs focus on transparency, ethics, and rotation of sensitive roles, reflecting efforts to compensate for uneven institutional maturity and legacy infrastructure. The United Arab Emirates, by contrast, exemplifies a top-down, policy-driven model that combines national cyber standards with strong sectoral oversight. Its insider programs emphasize precision, accountability, and readiness – balancing the need for rapid growth with the imperatives of trust and regulatory credibility. Meanwhile, Israel demonstrates how innovation ecosystems can achieve high resilience through technical excellence and cultural alignment. Insider threat programs in Israeli corporations prioritize intellectual property stewardship, rapid anomaly detection, and trust-preserving prevention mechanisms – an approach that sustains creativity while protecting strategic assets.

Collectively, these models reveal a global pattern of convergent diversity: nations and corporations adapt insider threat strategies to local conditions while moving toward shared principles of data integrity, accountability, and ethical security. Brazil and Latin America contribute the dimension of social integrity and gradual convergence with global standards; the UAE offers a framework of centralized discipline and institutional agility; and Israel provides a blueprint for integrating innovation, security, and human trust. Together, they demonstrate that sustainable insider threat management depends not on uniformity but on the capacity of each governance system to translate its cultural and institutional strengths into coherent, adaptive security practices.

The Table 1.5 consolidates insider threat management practices across major global jurisdictions, highlighting how diverse legal, cultural, and institutional frameworks shape corporate security governance. It provides a structured comparison of human resource policies, technological and engineering controls, internal audit mechanisms, and performance metrics within seven distinct regulatory and cultural environments: the United States, the European Union, East Asia, Brazil and Latin America, the United Arab Emirates, and Israel. The purpose of this synthesis is to demonstrate how national traditions, labor relations, and risk appetites influence both the form and function of insider threat programs, offering a global panorama of emerging best practices.

The table 1.5 emphasizes that while each region prioritizes different aspects – compliance and deterrence in the United States, privacy and ethics in the European Union, collectivism and moral loyalty in East Asia, integrity

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

and adaptation in Latin America, centralized oversight in the UAE, and innovation protection in Israel – all converge on the principle of multi-layered defense. Across contexts, the integration of behavioral analytics, access control, ethical culture, and governance oversight forms the backbone of resilient insider threat frameworks. By mapping these dimensions side by side, the table serves as both a diagnostic and a prescriptive tool, allowing corporations to benchmark their internal policies against international standards and to identify gaps between technological sophistication and cultural readiness.

Table 1.5. Comparative Global Framework of Insider Threat Management Across Key Jurisdictions

Jurisdiction	HR policy essentials	IT and security controls	Internal audit and compliance	Core metrics and reporting	Strategic notes
United States	Proportional screening, targeted training, conflict disclosures, grievance channels, strict offboarding, role rotation	Central identity governance, least privilege, UEBA, DLP, SIEM, OT segmentation	SOX-style testing, RCSA, hotline governance, third-party monitoring, annual program review	Deprovisioning time, privileged coverage, DLP efficacy, hotline substantiation, triage time	High detection capacity, manage privacy risk and trust
European Union	Privacy-aware screening, transparency on monitoring, ethics and data protection training, mediation and wellness, documented offboarding	Privacy-preserving analytics, MFA and context checks, encryption, vendor access control	DPIAs, NIS2 alignment, insider council with HR legal IT labor, whistleblowing assurance	DPIA coverage, case cycle time, false positives, training effectiveness, vendor attestations	Rights-based model, balance prevention with proportional monitoring
East Asia	Ethics and loyalty culture, confidential reporting without loss of face, rotation for sensitive roles, contractor discipline	Granular repo and OT access, DevSecOps controls, UEBA tuned to local norms, national compliance in China and Singapore	Procurement and IP reviews, local law mapping, corrective coaching for negligence, firm sanctions for malice	Privilege removal time, anomalous repo rate, procurement exception rate, underreporting indicators	Combine cultural cohesion with codified control, improve transparency
Brazil and Latin America	Integrity pacts, focused training for high-exposure functions, rotation of gatekeepers, union	Access reviews on legacy, DLP at endpoints, vendor segregation, SOC correlation	COSO-aligned fraud risk assessment, continuous vendor testing, evidence-ready case	Vendor risk closures, SoD breaches resolved, near-miss capture, regional	Converge to global standards, address legacy constraints and

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

Jurisdiction	HR policy essentials	IT and security controls	Internal audit and compliance	Core metrics and reporting	Strategic notes
	engagement, transparent notices	across fraud and HR	management, integrity audits	training coverage	enforcement lag
United Arab Emirates	Role-sensitive screening, monitoring terms acceptance, contractor onboarding and rapid exit, protected escalation	Identity automation, privileged vaulting and session recording, toxic-combination prevention, regulator-ready dashboards, crisis exercises	Audits against national standards, evidence handling and notification playbooks, free-zone vendor assessments	MTTD, regulator response time, exercise scores, privileged review completion, third-party adherence	Central policy plus sector depth, strong coordination with authorities
Israel	IP stewardship at key moments, code reuse rules, retention levers, trust-preserving feedback	Repo anomaly monitoring, secrets management, data isolation, split-key or ABAC for crown jewels, automated exit hygiene	IP risk portfolio, insider misuse simulations, IP clause audits in supplier and university contracts, board KPIs	Anomalous repo events, enhanced control coverage, exit revocation time, code policy violations, IP incidents	Protect innovation while controlling exfiltration paths in fast-moving R&D

Source: systematized by the author

The comparative analysis underscores that no single jurisdiction provides a universal blueprint for insider threat management; instead, effective strategies emerge from contextual adaptation and cross-cultural learning. Despite differences in regulatory scope and organizational culture, successful programs share several constants: leadership commitment, cross-departmental coordination, and data-informed decision-making supported by ethical governance. The convergence toward hybrid, transnational models – combining U.S. compliance rigor, European human-centric governance, Asian cultural coherence, Latin American integrity frameworks, and Middle Eastern strategic control – illustrates a maturing global consensus.

Ultimately, the table reveals that insider threat mitigation is evolving beyond reactive surveillance into a pillar of corporate resilience and sustainability. Organizations that align technical controls with human values and governance transparency not only reduce insider risks but also strengthen stakeholder confidence and institutional trust.

https://doi.org/10.36690/ITSC
ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

4. Insider Threats as a Governance and Strategic Challenge. In modern corporations, insider threats represent not isolated incidents of individual misconduct but systemic failures of governance, culture, and strategic coherence. The contemporary organization functions as a complex socio-technical system where human behavior, digital infrastructure, and governance processes are deeply intertwined. Within this environment, the insider threat emerges as a critical indicator of structural weaknesses – insufficient ethical leadership, fragmented accountability, and the erosion of trust across hierarchies. Scholars such as Greitzer and Frincke (2010) and Nurse (2022) argue that insider incidents rarely arise spontaneously; they result from cumulative failures in communication, leadership empathy, and risk anticipation. When employees experience alienation, injustice, or burnout, organizational loyalty weakens, and the boundary between loyalty and opportunism becomes blurred.

From a governance perspective, insider risk is inseparable from the quality of decision-making and control within corporate structures. Weak board oversight, lack of transparency in management practices, and ineffective whistleblowing systems create fertile ground for both deliberate misconduct and negligence. As organizations expand globally, the dispersion of responsibilities across subsidiaries and contractors multiplies the potential points of vulnerability. Insider threats often materialize where governance control is weakest – within complex outsourcing networks, joint ventures, and remote teams where monitoring and culture-building are limited. Consequently, insider management has evolved into a strategic dimension of corporate governance, on par with financial risk management and ESG compliance.

The phenomenon of hybrid threats further intensifies this challenge. Hybrid actors blur the traditional distinction between internal and external adversaries, leveraging digital technologies to infiltrate organizational networks through trusted insiders. These actors exploit compromised credentials, social engineering, or financial coercion to execute attacks that combine cyber intrusion with human manipulation. Such convergence requires corporations to integrate cybersecurity, behavioral science, and governance intelligence within a single analytical framework. The ISO/IEC 27035 standard and the NIST Risk Management Framework exemplify this integrated logic, advocating for continuous monitoring, contextual analysis, and dynamic response mechanisms.

To counter these intertwined risks, leading corporations are transitioning toward holistic security governance models. These models combine human resource management, IT security, compliance, and ethics

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

into unified risk ecosystems. Human resource departments now play an anticipatory role, identifying behavioral anomalies through well-being indicators and engagement surveys. Cybersecurity divisions monitor technical anomalies using AI-powered behavioral analytics, while compliance officers ensure regulatory alignment and investigate ethical breaches. This triadic collaboration transforms insider threat management from a reactive policing activity into a proactive, predictive, and preventive process.

Strategically, the insider threat is now seen as a litmus test of corporate resilience. Its effective management reinforces stakeholder confidence, protects intellectual property, and sustains operational continuity. Conversely, each insider incident damages not only assets but also the corporation's intangible capital – trust, reputation, and employee morale. Integrating insider risk management into enterprise risk frameworks allows organizations to assess exposure through quantitative and qualitative metrics, linking security outcomes with strategic performance indicators. Boards increasingly require regular reports on insider program effectiveness, cultural risk metrics, and ethical climate audits as part of governance assurance.

Yet, the governance paradox remains. Corporations must empower employees to innovate, collaborate, and share information – the very openness that drives competitiveness – while instituting mechanisms that prevent the abuse of that trust. Excessive control undermines creativity and morale; insufficient oversight invites exploitation. The equilibrium between trust and verification thus defines the modern philosophy of corporate security. Achieving this balance requires more than compliance: it demands ethical leadership, transparent governance, and a culture of shared responsibility.

In this sense, insider threats act as a mirror reflecting the organization's inner state. They expose the tension between declared corporate values and the lived reality of management practices. Institutions that cultivate fairness, psychological safety, and purpose-based engagement experience fewer insider incidents, while those that rely solely on surveillance or fear-based deterrence risk internal erosion. The most advanced corporate strategies therefore treat insider threat management not merely as defense but as a driver of ethical renewal – a continuous process through which the corporation strengthens its moral core, governance discipline, and collective resilience in an era of hybrid risk and digital interdependence.

Conclusion. The comparative analysis of insider threat management across global jurisdictions reveals that while regulatory frameworks and

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

cultural orientations vary widely, all regions converge on a shared recognition: insider threats represent not only a cybersecurity issue but a systemic challenge to corporate integrity, trust, and governance. Each jurisdiction has developed mechanisms consistent with its institutional traditions – technical rigor and accountability in the United States, rights-based proportionality in the European Union, cultural cohesion in East Asia, adaptive compliance in Latin America, centralized oversight in the United Arab Emirates, and innovation protection in Israel. Despite their differences, these models collectively emphasize the integration of human, technological, and ethical controls within a unified resilience strategy.

The synthesis of practices demonstrates that successful insider threat programs rely on three fundamental principles. First, contextual governance – security policies must align with local labor law, privacy expectations, and societal norms. Second, cross-functional coordination – human resources, cybersecurity, and internal audit must operate as a cohesive ecosystem supported by leadership commitment and transparent accountability. Third, predictive intelligence and ethical leadership – organizations must combine behavioral analytics and technical monitoring with trust-based communication, training, and moral stewardship.

In the globalized digital economy, where corporate data and personnel operate across borders, no single national framework is sufficient. The emerging paradigm is hybrid and transnational, blending U.S. compliance precision, European ethical oversight, East Asian cultural integrity, and Middle Eastern–Latin American adaptive governance. This convergence points toward a future in which insider threat management becomes an integral element of corporate resilience and sustainability, embedding cybersecurity within broader agendas of organizational ethics, ESG governance, and global trust.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this article are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

References:

1. Anderson, J. P. (1972). *Computer security technology planning study* (ESD-TR-73-51). U.S. Air Force Electronic Systems Division. https://apps.dtic.mil/sti/pdfs/AD0755935.pdf
2. Brazil. (2018). *Lei No. 13.709, de 14 de agosto de 2018 (Geral de Proteção de Dados Pessoais – LGPD).* Presidency of the Republic of Brazil. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf
3. Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT® guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud).* Addison-Wesley. https://doi.org/10.5555/2381048
4. Colombia. (2012). *Law 1581 of 2012 – Protection of Personal Data.* Diario Oficial de Colombia. https://www.sic.gov.co/sites/default/files/files/Ley1581de2012.pdf
5. Colwill, C. (2009). Human factors in information security: The insider threat - Who can you trust these days? *Information Security Technical Report, 14*(4), 186–196. https://doi.org/10.1016/j.istr.2010.04.004
6. European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union,* L 119. https://eur-lex.europa.eu/eli/reg/2016/679/oj
7. European Union. (2023). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union,* L 333. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
8. European Union Agency for Cybersecurity (ENISA). (2023). *Threat Landscape: Insider threats and organizational resilience.* ENISA Publications. https://www.enisa.europa.eu/publications
9. Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cybersecurity audit data with psychosocial data: Toward predictive modeling for insider-threat mitigation. In C. W. Probst et al. (Eds.), *Insider threats in cyber security* (pp. 85–113). Springer. https://doi.org/10.1007/978-1-4419-7133-3_5
10. Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A., Mundie, D., & Cowley, J. (2021). A socio-technical approach to mitigating insider threats. *Journal of Cybersecurity, 7*(1), taab018. https://doi.org/10.1093/cybsec/taab018
11. Hunker, J., & Probst, C. W. (Eds.). (2011). *Insider threats in cyber security.* Springer. https://doi.org/10.1007/978-1-4419-7133-3
12. International Organization for Standardization (ISO/IEC). (2022 → maintained edition). *Information security management systems – Requirements (ISO/IEC 27001:2022).* ISO. https://www.iso.org/standard/82875.html
13. Israel. (1981). *Protection of Privacy Law, 5741-1981.* Government of Israel. https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf
14. Japan. (2022). *Act on the Protection of Personal Information (APPI), Act No. 57 of 2003 (amended April 1 2022).* Japanese Law Translation. https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025

15. Kim, S., & Park, H. (2020). Organizational culture and insider threat management in Korean corporations. *Asian Journal of Information Security, 9*(2), 45–62. https://doi.org/10.3390/info9020045
16. Liu, L., Yu, J., & Zhao, X. (2018). Data-driven insider-threat detection using user behavior analytics. *Computers & Security, 77,* 720–735. https://doi.org/10.1016/j.cose.2018.04.008
17. Mexico. (2010). *Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP).* Chamber of Deputies of the United Mexican States. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
18. National Institute of Standards and Technology (NIST). (2021). *NIST Special Publication 800-53 Rev. 5: Security and privacy controls for information systems and organizations.* U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5
19. Nurse, J. R. C. (2015). Insider threat research: A review and agenda for the future. *Computers & Security, 55,* 1–18. https://doi.org/10.1016/j.cose.2015.06.001
20. Nurse, J. R. C. (2022). Human-centered approaches to insider risk management. *Journal of Information Security and Applications, 65,* 103091. https://doi.org/10.1016/j.jisa.2022.103091
21. Parker, D. B. (1981). Computer security management. *Computers & Security, 1*(2), 93–98. https://doi.org/10.1016/0167-4048(82)90001-4
22. People's Republic of China. (2017). *Cybersecurity Law of the People's Republic of China.* National People's Congress. https://www.cac.gov.cn/2016-11/07/c_1119867116.htm
23. People's Republic of China. (2021). *Personal Information Protection Law (PIPL) of the People's Republic of China.* National People's Congress. https://www.npc.gov.cn/englishnpc/c23934/202112/b9d593a6d9314d7580df5c41f8d1f3c3.shtml
24. Republic of Korea. (2020). *Personal Information Protection Act (PIPA).* Korea Legislation Research Institute. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53844&lang=ENG
25. Shaw, E., & Fischer, L. (2005). *Ten tales of betrayal: The threat to corporate infrastructure by information-technology insiders – Analysis and observations.* Defense Personnel Security Research Center. https://apps.dtic.mil/sti/pdfs/ADA465730.pdf
26. Singapore. (2020). *Personal Data Protection Act 2012 (Amendment 2020).* Singapore Statutes Online. https://sso.agc.gov.sg/Act/PDPA2012
27. United Arab Emirates. (2021). *Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data.* Government of the United Arab Emirates. https://www.uaelegislation.gov.ae/en/legislations/1972/download
28. United States Congress. (2002). *Sarbanes–Oxley Act of 2002 (Public Law 107-204).* U.S. Government Publishing Office. https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter98
29. U.S. Department of Defense. (2018). *DoD Directive 5205.16: The Insider Threat Program (DoD ITP).* Washington, DC. https://www.esd.whs.mil/DD

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)
© Scientific Center of Innovative Research, 2025