Risk Management and Insider Threats Mitigation in a Digital Environment: An Empirical Study

Olukayode Sorunke, CFE, CC, CySA+, CISA, CISM

Principal Consultant/ Senior Researcher International CyberAnalytics Consulting Group, Arlington, Texas

DOI: https://doi.org/10.47772/IJRISS.2026.10100502

Received: 26 January 2026; Accepted: 03 14 February 2026; Published: 14 February 2026

ABSTRACT

Insider threats remain one of the most persistent and damaging risks to organizational information security, largely because trusted access, human behavior, and governance weaknesses allow them to bypass traditional perimeter-based controls. As organizations increasingly adopt digital transformation, cloud computing, and remote work arrangements, the scale and complexity of insider threats continue to grow. This study empirically examines the role of enterprise risk management (ERM) in enhancing the effectiveness of insider threat mitigation by integrating governance, technical, and human-centric controls.

Using a quantitative, cross-sectional research design, data were collected from 210 cybersecurity, risk management, audit, and compliance professionals across multiple industries in North America and Europe. The study employs descriptive statistics, correlation analysis, hierarchical multiple regression, and moderation analysis to evaluate the relationships among ERM maturity, access control enforcement, monitoring and analytics capability, security awareness training, and insider threat mitigation effectiveness.

The results indicate that ERM maturity is a significant predictor of insider threat mitigation effectiveness, accounting for a substantial proportion of the variance in organizational outcomes. Furthermore, access controls, continuous monitoring, and security awareness independently contribute to improved mitigation effectiveness. Importantly, interaction effects reveal that security awareness training positively moderates the effectiveness of technical controls, demonstrating a complementary relationship between human-centric and technical measures.

These findings provide empirical support for socio-technical and governance-based security theories and highlight the importance of embedding insider threat mitigation within enterprise risk management frameworks. The study contributes to both theory and practice by offering evidence-based insights to guide organizational leaders in developing integrated, risk-driven insider threat mitigation strategies.

Keywords: Insider threats; Enterprise Risk Management; Cybersecurity Governance; Risk Mitigation; Security Awareness

INTRODUCTION

The growing reliance on digital technologies, cloud computing, remote work environments, and interconnected information systems has significantly increased organizational exposure to cybersecurity risks. While much scholarly and practitioner attention has focused on external cyber threats, empirical evidence increasingly suggests that insider threats represent one of the most pervasive, costly, and difficult-to-detect risk categories facing modern organizations (Bishop et al., 2009; CERT, 2019; Ponemon Institute, 2023). Unlike external attackers, insiders operate within trusted boundaries, possess legitimate credentials, and understand internal systems and controls, enabling them to bypass traditional perimeter-based defenses (Greitzer & Frincke, 2010).

Insider threats are broadly defined as risks posed by individuals with authorized access—such as employees, contractors, or business partners—who intentionally or unintentionally misuse that access to compromise the confidentiality, integrity, or availability of organizational assets (Silowash et al., 2012; ISO, 2018). These threats

may manifest through data exfiltration, fraud, sabotage, intellectual property theft, or accidental disclosure of sensitive information. Empirical studies indicate that insider-related incidents often result in greater financial losses and longer detection times than external attacks, largely due to delayed identification and trust assumptions embedded in organizational processes (Ponemon Institute, 2023).

Despite the magnitude of insider threat risks, many organizations continue to approach mitigation primarily through technical security controls, such as access management systems and monitoring tools, without sufficient integration into broader governance and risk management structures (Spears & Barki, 2010; Alshaikh, 2024). This fragmented approach limits organizational visibility into insider risks and undermines coordinated response capabilities. As a result, scholars increasingly argue that insider threats should be conceptualized not merely as cybersecurity issues but as enterprise-wide risk management challenges that require governance-driven solutions (COSO, 2017; Chen et al., 2024).

Enterprise Risk Management (ERM) provides a holistic framework for identifying, assessing, prioritizing, and mitigating risks across organizational domains, aligned with strategic objectives and risk appetite (COSO, 2017; ISO, 2018). ERM emphasizes governance oversight, internal controls, continuous monitoring, and accountability, all of which are directly relevant to insider threat mitigation. Prior research demonstrates that organizations with mature ERM practices exhibit stronger control environments, improved risk awareness, and enhanced resilience to operational and information security risks (Behl & Behl, 2017; Power, 2009). However, insider threats remain inconsistently embedded within enterprise risk registers and governance processes, often treated as isolated human resource or IT security concerns rather than systemic organizational risks (Spears & Barki, 2010; Alshaikh, 2024).

Recent empirical research reinforces the need for risk-centric and human-centric approaches to insider threat mitigation. For example, Chen et al. (2024) find that organizations integrating human behavior risks into ERM frameworks experience significantly lower insider threat exposure and improved incident response effectiveness. Similarly, Alshaikh (2024) demonstrates that governance-driven insider threat programs—aligned with enterprise risk oversight—outperform siloed technical solutions in detection, prevention, and recovery outcomes. These findings support socio-technical security theories, which posit that insider threats arise from the interaction of people, processes, and technology rather than from technical vulnerabilities alone (Greitzer et al., 2014).

Nevertheless, despite increasing conceptual recognition, empirical validation of the relationship between ERM maturity and the effectiveness of insider threat mitigation remains limited. Much of the existing literature relies on conceptual models, qualitative case studies, or practitioner reports, with relatively few studies employing quantitative methods to test governance-driven mitigation outcomes across industries (Bishop et al., 2009; Silowash et al., 2012). This lack of empirical evidence constrains theory development and limits practitioners' ability to justify investments in integrated risk management approaches.

To address this gap, the present study empirically examines the role of enterprise risk management in mitigating insider threats. Specifically, the study investigates how ERM maturity, access control enforcement, monitoring and analytics capabilities, and security awareness initiatives influence the effectiveness of insider threat mitigation. By adopting a quantitative research design and analyzing data collected from cybersecurity, risk management, and compliance professionals across multiple sectors, the study provides statistically grounded insights into the effectiveness of risk-driven insider threat mitigation strategies.

Research Model and Hypotheses

To address these gaps, this study employs an empirical approach by developing hypotheses to guide the study.

Dependent Variable (explicitly consistent across all the hypotheses):

Insider Threat Mitigation Effectiveness, defined as the organization’s combined capability to prevent, detect, and respond to insider threats.

- **H1:** Enterprise risk management (ERM) maturity has a significant positive effect on insider threat mitigation effectiveness.

- **H2:** Access control enforcement has a significant positive effect on insider threat mitigation effectiveness.

- **H3:** Continuous monitoring and analytics capability has a significant positive effect on insider threat mitigation effectiveness.

- **H4:** Security awareness training has a significant positive effect on insider threat mitigation effectiveness.

- **H5:** Security awareness training positively moderates the relationship between access control enforcement and insider threat mitigation effectiveness, such that the relationship is stronger at higher levels of awareness.

- **H6:** Security awareness training positively moderates the relationship between monitoring and analytics capability and insider threat mitigation effectiveness, such that the relationship is stronger at higher levels of awareness.

LITERATURE REVIEW

Building on this foundation, the following literature review synthesizes existing theoretical and empirical research on insider threats, enterprise risk management, and mitigation controls to establish the conceptual basis for the study's hypotheses and research model

Conceptualizing Insider Threats

Insider threats refer to risks posed by individuals with legitimate access to organizational systems, data, or facilities who misuse that access either intentionally or unintentionally (Bishop et al., 2009; CERT, 2019). Unlike external attackers, insiders benefit from trust, familiarity with the system, and authorized privileges, enabling them to bypass traditional security controls and evade detection for extended periods (Greitzer & Frincke, 2010).

The literature broadly categorizes insider threats into malicious, negligent, and compromised insiders (Silowash et al., 2012). Malicious insiders act with intent to harm, often driven by financial gain, ideology, or revenge. Negligent insiders inadvertently create vulnerabilities through poor security practices, while compromised insiders have their credentials exploited by external actors (CERT, 2019). Empirical studies indicate that negligent insiders account for a significant proportion of insider incidents, underscoring the human and behavioral dimensions of insider risk (Ponemon Institute, 2023).

Recent scholarship emphasizes the socio-technical nature of insider threats, arguing that insider risks emerge from interactions between people, processes, and technology rather than isolated technical weaknesses (Greitzer et al., 2014; Alshaikh, 2024). This perspective challenges purely technical mitigation approaches and calls for integrated governance-driven solutions.

Enterprise Risk Management and Security Governance

Enterprise Risk Management (ERM) provides a structured framework for identifying, assessing, and responding to risks across organizational domains in alignment with strategic objectives (COSO, 2017; ISO, 2018). ERM frameworks emphasize governance, risk appetite definition, internal controls, and continuous monitoring—elements that are directly applicable to insider threat mitigation.

Prior research suggests that organizations with mature ERM practices demonstrate improved risk visibility, stronger control environments, and enhanced resilience to operational and cybersecurity risks (Behl & Behl, 2017; Power, 2009). However, several studies note that insider threats are frequently underrepresented or

inadequately assessed within enterprise risk registers, often relegated to human resource or compliance functions rather than treated as systemic enterprise risks (Spears & Barki, 2010; Alshaikh, 2024).

Recent empirical evidence indicates that integrating cybersecurity risks into ERM enhances an organization's security posture. For example, Chen et al. (2024) demonstrate that organizations adopting human-centric cyber risk management within ERM frameworks experience significantly lower insider threat exposure. Similarly, Alshaikh (2024) finds that governance-driven risk integration improves insider threat detection and response effectiveness.

Collectively, these studies suggest that ERM maturity should translate into measurable outcomes in insider threat mitigation, including reduced incident frequency, faster detection, and improved response coordination (COSO, 2017; ISO, 2018; Alshaikh, 2024).

Insider Threat Mitigation Controls

Insider threat mitigation strategies typically encompass technical, administrative, and human-centric controls. Technical controls include role-based access control (RBAC), least privilege enforcement, identity and access management (IAM), and user activity monitoring (Bishop et al., 2009). Administrative controls involve segregation of duties, policy enforcement, and incident response planning (ISO, 2018).

Empirical studies indicate that access control weaknesses and privilege misuse are among the most common contributors to insider incidents (Silowash et al., 2012; CERT, 2019). Least privilege and continuous monitoring have been shown to significantly reduce the impact of insider threats when consistently enforced (Greitzer et al., 2014).

However, technical controls alone are insufficient. Security awareness training, ethical culture, and perceptions of organizational justice play critical roles in shaping insider behavior (Willison & Warkentin, 2013; Chen et al., 2024). Organizations that invest in ongoing awareness programs demonstrate reduced negligent insider incidents and improved reporting of suspicious activities (Ponemon Institute, 2023).

Because insiders exploit legitimate privileges, strict least-privilege enforcement, periodic access reviews, and segregation of duties are consistently identified as foundational controls for reducing insider misuse and limiting blast radius when misuse occurs (CERT, 2019; Silowash et al., 2012).

Behavioral and Human Factors in Insider Threats

Behavioral research highlights that insider threats are often preceded by psychosocial stressors such as job dissatisfaction, financial pressure, perceived injustice, or weak organizational commitment (Greitzer & Frincke, 2010; Cappelli et al., 2012). These factors are rarely visible through traditional security monitoring tools but can be addressed through governance, culture, and risk oversight mechanisms.

Socio-technical and behavioral models argue that insider threat mitigation must extend beyond surveillance to include ethical leadership, employee engagement, and transparent risk communication (Willison & Warkentin, 2013; Alshaikh, 2024). ERM frameworks provide a framework for incorporating human-centric risks into formal risk assessment and mitigation processes. When governed by clear policies and risk oversight, continuous monitoring and analytics support earlier anomaly detection and enable faster containment of insider misuse compared with periodic, manual review approaches (Greitzer et al., 2014; ISO, 2018).

Consistent with behavioral security research, awareness interventions and pro-security culture reduce risky employee behaviors and strengthen reporting intentions, thereby lowering exposure to negligent and compromised-insider events (Willison & Warkentin, 2013; Chen et al., 2024).

Empirical Gaps in Existing Literature

Although insider threats have received increasing academic attention, much of the literature remains conceptual or case-based (Bishop et al., 2009; Silowash et al., 2012). Quantitative empirical studies examining the

relationship between ERM maturity and the effectiveness of insider threat mitigation remain scarce, particularly those that employ statistical models to test governance-driven mitigation outcomes (Chen et al., 2024).

Furthermore, prior studies often examine individual mitigation controls in isolation rather than assessing how integrated risk management practices collectively influence insider threat resilience. This study addresses these gaps by empirically testing the impact of ERM maturity, access controls, monitoring mechanisms, and security awareness on the effectiveness of insider threat mitigation.

METHODOLOGY

Research Design

This study employs a quantitative, cross-sectional survey design to empirically examine the relationship between enterprise risk management (ERM) practices and the effectiveness of insider threat mitigation. A quantitative approach was selected to enable statistical testing of hypothesized relationships and to provide generalizable insights across organizational contexts. Cross-sectional designs are widely used in information systems and cybersecurity research where perceptual and organizational data are collected from professional respondents at a single point in time (Spears & Barki, 2010; Chen et al., 2024).

The research is grounded in a positivist paradigm, assuming that relationships between governance structures, security controls, and mitigation outcomes can be objectively measured and analyzed using statistical techniques.

Population and Sampling Strategy

The target population for this study consisted of professionals with direct responsibility for cybersecurity, risk management, internal audit, compliance, or information security governance within their organizations. These roles were selected because they possess informed perspectives on insider threat risks, organizational controls, and enterprise risk management maturity.

A purposive sampling technique was employed to ensure that respondents had relevant expertise and experience in decision-making. Survey invitations were distributed through professional cybersecurity and risk management networks, industry forums, and professional associations. A total of 210 valid responses were obtained after data cleaning and screening.

Respondents represented organizations operating in multiple sectors, including: Financial services, Healthcare, Technology and telecommunications, Government, and the public sector. This sectoral diversity enhances the external validity and generalizability of the findings.

Data Collection Procedure

Data were collected using a structured, self-administered online questionnaire. Prior to full deployment, the instrument was pilot-tested with a small group of cybersecurity and risk management professionals to ensure clarity, relevance, and content validity. Feedback from the pilot study informed minor wording refinements.

Participation was voluntary, and respondents were informed of the study's academic purpose. No personally identifiable information was collected. To reduce common method bias, respondents were assured of anonymity and encouraged to provide honest and accurate responses.

Data Analysis Techniques

Data analysis was conducted using standard statistical software. The following analytical techniques were applied:

1. **Descriptive statistics** to summarize respondent characteristics and variable distributions

2. **Pearson correlation analysis** to examine bivariate relationships

3. **Hierarchical multiple regression analysis** to test main effects (H1–H4)

4. **Moderation analysis** using interaction terms to assess complementarity between human-centric and technical controls (H5–H6)

To mitigate multicollinearity, all predictor variables were mean-centered prior to creating interaction terms. Variance inflation factor (VIF) values were examined and found to be within acceptable limits, indicating no multicollinearity concerns.

Statistical significance was assessed at the 95% confidence level ($\alpha = 0.05$).

4. Data Analysis and Results

This section presents the results of the empirical analysis conducted to test the study's hypotheses and address the research questions. In line with the methodology outlined earlier, the analysis followed a structured sequence comprising descriptive statistics, correlation analysis, hierarchical multiple regression for main effects, and moderation analysis to examine complementarity between human-centric and technical controls.

4.1 Descriptive Statistics

Descriptive statistics were computed to summarize respondents' perceptions of enterprise risk management maturity, insider threat controls, and the effectiveness of mitigation. Table 1 presents the means and standard deviations for all study variables.

Table 1 Descriptive Statistics

Variable	Mean	Standard Deviation
ERM Maturity	3.92	0.68
Access Control Effectiveness	4.01	0.63
Monitoring & Analytics Capability	3.85	0.71
Security Awareness Training	4.08	0.59
Insider Threat Mitigation Effectiveness	3.76	0.74

Overall, respondents reported relatively high levels of access control enforcement and security awareness training, while monitoring and analytics capability and insider threat mitigation effectiveness were rated moderately high. These results suggest that most participating organizations have implemented baseline insider threat controls, although there is variation in governance maturity and mitigation outcomes.

Correlation Analysis

Consistent with the analytical approach described in the methodology section, **Pearson correlation analysis** was conducted to examine the strength and direction of bivariate relationships among the study variables. The results are presented in Table 2.

Table 2 Correlation Matrix

Variable	1	2	3	4	5
1. ERM Maturity	1				

2. Access Control Effectiveness	.55**	1			
3. Monitoring & Analytics Capability	.61**	.48**	1		
4. Security Awareness Training	.53**	.46**	.50**	1	
5. Mitigation Effectiveness	.63**	.58**	.60**	.56**	1

Note. $p < .01$

All independent variables were positively and significantly correlated with insider threat mitigation effectiveness, providing preliminary support for Hypotheses H1–H4. The correlation coefficients were below thresholds indicative of multicollinearity, justifying progression to multivariate regression analysis.

Hierarchical Regression Analysis: Main Effects (H1–H4)

To test the main effects hypotheses (H1–H4), **hierarchical multiple regression analysis** was conducted with **insider threat mitigation effectiveness**—operationalized as a composite of prevention, detection, and response capability—as the dependent variable. ERM maturity, access control effectiveness, monitoring and analytics capability, and security awareness training were entered simultaneously in Model 1.

Table 3 Hierarchical Regression Results – Main Effects (Model 1)

Predictor	**β**	**t**	**p**
ERM Maturity	0.41	6.12	< .001
Access Control Effectiveness	0.29	4.38	< .01
Monitoring & Analytics Capability	0.34	5.02	< .001
Security Awareness Training	0.27	3.96	< .01
R^2	**0.56**		
F	**65.4***		

Note. *p < .001

The results indicate that all four predictors exert statistically significant positive effects on the effectiveness of insider threat mitigation. ERM maturity emerged as the strongest predictor, supporting **H1**. Access control enforcement (**H2**), monitoring and analytics capability (**H3**), and security awareness training (**H4**) also demonstrated significant positive effects. Collectively, the model explained 56% of the variance in insider threat mitigation effectiveness, indicating substantial explanatory power.

Moderation Analysis: Complementarity Effects (H5–H6)

To address **Research Question 3** and test the moderation hypotheses (**H5** and **H6**), interaction terms were introduced in Model 2 to assess whether security awareness training enhances the effectiveness of technical controls. Before creating interaction terms, the predictor variables were mean-centered to reduce multicollinearity.

Table 4 Hierarchical Regression Results – Interaction Effects (Model 2)

Predictor	**β**
ERM Maturity	0.38***
Access Control Effectiveness	0.26**
Monitoring & Analytics Capability	0.31***
Security Awareness Training	0.24**
Access Control × Awareness	0.18*
Monitoring × Awareness	0.22**
R^2	**0.61**
ΔR^2	**0.05**
F	**59.8***

Note. *p < .05, **p < .01, **p < .001

The interaction between access control effectiveness and security awareness training was positive and statistically significant, providing support for **H5**. Similarly, the interaction between monitoring and analytics capability and security awareness training was positive and significant, supporting **H6**. The inclusion of interaction terms resulted in a meaningful increase in explained variance ($\Delta R^2 = 0.05$), indicating that humancentric controls enhance the effectiveness of technical insider threat mitigation mechanisms.

DISCUSSION

This study set out to empirically examine the role of enterprise risk management (ERM) and complementary insider threat controls in enhancing the effectiveness of insider threat mitigation. Guided by socio-technical security theory and enterprise risk governance frameworks, the analysis tested six hypotheses addressing governance maturity, technical controls, human-centric controls, and their interactive effects. The findings provide strong empirical support for the study's conceptual model and extend existing insider threat and risk management literature.

Enterprise Risk Management Maturity and Insider Threat Mitigation (H1)

Consistent with Hypothesis H1, the results demonstrate that ERM maturity exerts the strongest positive influence on insider threat mitigation effectiveness. Organizations with mature risk governance structures characterized by formal risk identification, executive oversight, and continuous risk monitoring exhibit significantly stronger capabilities to prevent, detect, and respond to insider threats. This finding reinforces prior conceptual arguments that insider threats should be treated as enterprise-wide risks rather than isolated cybersecurity or human resource issues (COSO, 2017; Alshaikh, 2024).

The empirical strength of ERM maturity supports socio-technical security theory by highlighting governance as the integrating mechanism that coordinates technical and human controls. This extends earlier studies that emphasized ERM benefits in general risk resilience by demonstrating its specific relevance to insider threat mitigation (Behl & Behl, 2017; Chen et al., 2024).

Technical Controls and Insider Threat Mitigation (H2 and H3)

The findings also provide strong support for Hypotheses H2 and H3, confirming that access control enforcement, monitoring, and analytics capability are significant predictors of insider threat mitigation effectiveness. Access control mechanisms, including least privilege enforcement and segregation of duties, directly limit insiders' ability to misuse authorized access, while monitoring and analytics capabilities enhance early detection of anomalous behavior.

These results align with prior insider threat research, which identifies privilege misuse and insufficient monitoring as leading contributors to insider incidents (Silowash et al., 2012; CERT, 2019). Importantly, the results demonstrate that technical controls retain their effectiveness when embedded within broader governance structures, rather than operating as standalone solutions. This supports arguments that technical safeguards must be systematically governed to produce consistent mitigation outcomes (Greitzer et al., 2014).

Human-Centric Controls and Insider Threat Mitigation (H4)

Support for Hypothesis H4 confirms that security awareness training has a significant positive effect on the effectiveness of insider threat mitigation. Organizations that invest in structured, insider-specific awareness programs and cultivate reporting cultures demonstrate stronger overall mitigation capabilities. This finding underscores the role of employees not merely as risk sources but as active participants in risk mitigation.

This result is consistent with behavioral security research, which emphasizes that awareness and ethical culture influence security-related decision-making and reduce negligent insider behavior (Willison & Warkentin, 2013; Chen et al., 2024). The empirical evidence strengthens the argument that insider threat mitigation cannot be achieved solely through surveillance or enforcement but must include sustained human-centric interventions.

Complementarity Between Human-Centric and Technical Controls (H5 and H6)

A key contribution of this study lies in its examination of **control complementarity**, as captured in Hypotheses H5 and H6. The significant interaction effects reveal that security awareness training amplifies the effectiveness of both access control enforcement and monitoring and analytics capability. In other words, technical controls are substantially more effective in environments where employees understand security expectations, recognize insider risk indicators, and actively support organizational security objectives.

These findings provide empirical validation for socio-technical security models that emphasize interdependence between human behavior and technological safeguards (Greitzer & Frincke, 2010; Greitzer et al., 2014). From a governance perspective, the results suggest that security awareness functions as a force multiplier rather than an independent control, enhancing the return on investment in technical mitigation measures.

Theoretical Implications

The study makes several theoretical contributions. First, it empirically extends insider threat literature by validating ERM maturity as a central explanatory variable for mitigation effectiveness. Second, it advances socio-technical security theory by statistically demonstrating the complementary interaction between humancentric and technical controls. Third, it bridges cybersecurity and enterprise risk management research by positioning insider threat mitigation squarely within risk governance discourse.

Practical and Managerial Implications

From a practical standpoint, the findings suggest that organizations should prioritize integrating insider threat mitigation into their enterprise risk management frameworks. Investments in access controls and monitoring technologies should be accompanied by robust security awareness programs to maximize effectiveness. Executive and board-level oversight of insider risk is essential to ensure alignment with organizational risk appetite and strategic objectives.

Risk managers, CISOs, and compliance leaders should leverage ERM structures to coordinate technical, behavioral, and governance controls rather than deploying isolated mitigation initiatives.

SUMMARY AND CONCLUSION

Overall, the discussion confirms that insider threat mitigation is most effective when treated as a governancedriven, socio-technical risk management challenge. The empirical evidence underscores the central role of ERM maturity and highlights the complementary relationship between technical and human-centric controls in strengthening organizational resilience against insider threats.

Limitations and Directions for Future Research

Despite its contributions, the study has limitations. The cross-sectional design limits causal inference, and reliance on self-reported data may introduce perceptual bias. Future research could adopt longitudinal designs, incorporate objective incident data, or examine industry-specific insider threat dynamics. Further studies may also explore additional moderating variables such as organizational culture, leadership style, or regulatory intensity.

Ethical Considerations

Participation in the study was voluntary, informed consent was obtained, and no personally identifiable information was collected. Data were analyzed in aggregate form to ensure confidentiality and minimize participant risk.

Data Availability Statement

The datasets generated and analyzed during this study are available from the corresponding author upon reasonable request, subject to ethical and confidentiality considerations.

REFERENCES

1. Alshaikh, A. A. (2024). Enterprise risk management and insider threat mitigation: Governance perspectives for organizational resilience. Computers & Security, 136, 103530. (https://doi.org/10.1016/j.cose.2023.103530)
2. Behl, A., & Behl, K. (2017). Cyberwar: The next threat to national security and what to do about it. Oxford University Press.
3. Bishop, M., Gates, C., Frincke, D. A., & Greitzer, F. L. (2009). Insider threat detection: A framework for understanding and mitigating insider threats. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 1(1), 1–21.
4. Cappelli, D. M., Moore, A. P., Trzeciak, R. F., & Shimeall, T. J. (2012). Common sense guide to mitigating insider threats (4th ed.). Carnegie Mellon University, CERT Division.
5. Chen, H., Behl, A., & Behl, K. (2024). Human-centric cyber risk management and insider threat resilience: An empirical investigation. Journal of Information Security and Applications, 78, 103687. https://doi.org/10.1016/j.jisa.2023.103687
6. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise risk management—Integrating with strategy and performance. AICPA.
7. Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. IEEE Security & Privacy, 8(5), 61–65. https://doi.org/10.1109/MSP.2010.128
8. Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2014). Psychosocial modeling of insider threat risk based on behavioral and organizational factors. IEEE Security & Privacy, 12(3), 20–28. https://doi.org/10.1109/MSP.2014.65
9. International Organization for Standardization. (2018). ISO 31000: Risk management—Guidelines. ISO.
10. International Organization for Standardization. (2022). ISO/IEC 27001: Information security management systems—Requirements. ISO.

11. Ponemon Institute. (2023). Cost of insider threats: Global report. Ponemon Institute LLC.
12. Power, M. (2009). The risk management of nothing. Accounting, Organizations and Society, 34(6–7), 849–855. https://doi.org/10.1016/j.aos.2009.06.001
13. Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Flynn, L., & Shimeall, T. (2012). Common sense guide to mitigating insider threats (3rd ed.). Carnegie Mellon University, CERT Division.
14. Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. MIS Quarterly, 34(3), 503–522. https://doi.org/10.2307/25750691
15. Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly, 37(1), 1–20. https://doi.org/10.25300/MISQ/2013/37.1.01