DOLOS IMPERATIVE

Human Elements Security

Bridging the Human Factor. Insider Risk Management Training for Healthcare Organizational Leaders

A Qualitative Case Study of Insider Risk Management Training Gaps Among Healthcare Leaders

A DOLOS IMPERATIVE APPLIED RESEARCH STUDY

Dr. Joshua L. Barrett, DSL

Researcher and Practitioner | Human-Centric Insider Risk

Based on the author's doctoral dissertation, completed at Liberty University School of Business

July 2026

Table of Contents

Executive Summary

Healthcare organizations continue to face challenges associated with insider threats, experiencing the highest costs and frequency of incidents compared to other industries, yet current training approaches remain inadequate despite rising incidents. This qualitative single case study explored insider risk management (IRM) training for organizational leaders within a healthcare organization and examined how potential training deficiencies impacted leaders' ability to prevent security incidents related to insider threats. This research specifically explored the state of IRM training for leaders, possible gaps in existing programs, leaders' perceptions of insider threat importance, and their roles and responsibilities in IRM. Using semi-structured interviews, surveys, and document analysis, the study highlighted significant disconnects between leaders' practical security awareness and formal IRM capabilities. While all participants demonstrated intuitive understanding of security vulnerabilities through daily experience, they universally lacked formal IRM training and systematic frameworks for insider risk recognition. The research identified six major themes: intuitive awareness versus formal training gaps, need for role-specific training, preferences for interactive approaches, divided security culture perceptions, varying leadership competency self-assessments despite universal skill gaps, and embedded compliance training that masks insider risk as a distinct discipline. The findings suggest current fragmented training approaches across several domains inadequately equip leaders with the specialized competencies they need for effective IRM. These results provide evidence for developing comprehensive IRM training programs that establish insider risk as a standalone discipline with role-specific components and interactive delivery methods.

1. Introduction

Insider risk, insider threat, and insider risk management (IRM) are distinct but related concepts that are often used interchangeably (Stone, 2022). Insiders are employees, contractors, business partners, or any individuals granted legitimate access to an organization's systems, networks, facilities, sensitive information, or resources (Greitzer & Purl, 2022; Whitty, 2021). Because insiders possess knowledge of an organization's operations and sensitive information, they hold the ability to exploit their access for personal gain or to cause harm. Insider risk refers broadly to the potential for harm originating from within an organization, encompassing both unintentional and intentional actions, while insider threat denotes the deliberate misuse of authorized access to cause harm, typically motivated by malicious intent or personal gain (Greitzer & Purl, 2022; Whitty, 2021). To address these risks proactively, organizations implement IRM programs that combine policy development, access controls, monitoring and detection, incident response, training and awareness, and risk assessment to identify, mitigate, and monitor insider risk (Bychkov, 2024).

In May 2023, a former Samsung executive was arrested for stealing chipmaking trade secrets valued at $233 million to benefit a foreign competitor (Choi, 2023), illustrating the growing trend and significant cost of insider-related security incidents (Mészáros & Kelemen-Erdős, 2023). Insiders with authorized access pose a greater threat than external actors because they can more easily exploit systems to commit fraud, steal intellectual property, or sabotage infrastructure (Al-Harrasi et al., 2023; Stone, 2022). Most insider incidents, regardless of industry, stem from unintentional, accidental, or negligent activity rather than malicious intent,

although malicious incidents are comparatively rarer and more costly (Lang, 2022a; Schoenherr & Thomson, 2022). Burns et al. (2023) found that nearly half of organizational security breaches are attributable to insiders, and Xiao et al. (2024) reported a 44% increase in insider incidents over two years, with an average remediation cost of $16 million. Whitelaw et al. (2024) similarly noted that insider-related breaches can cost organizations billions of dollars, and over half of all insider incidents involve ordinary employees rather than those with privileged system access (Zatonatskiy et al., 2021).

Despite this pervasive threat, organizations have largely responded with training and awareness programs as a primary defense (Whitelaw et al., 2024), yet the continued rise in insider incidents across sectors suggests these approaches remain inadequate (Lang, 2022a; Stone, 2022), particularly given that most incidents are attributable to human error (Mészáros & Kelemen-Erdős, 2023; Varga et al., 2021). Organizations continue to prioritize technological solutions over comprehensive IRM programs (Al-Harrasi et al., 2023; Lang, 2022a; Whitelaw et al., 2024), leaving IRM underfunded and creating a false sense of security (Lang, 2022a, 2022b). Compounding this problem is a notable absence of dedicated insider risk training for leaders; most organizations instead apply generic, enterprise-wide, or automated compliance training rather than role-specific instruction (Ali et al., 2021; Lang, 2022a; Triplett, 2022). Existing literature on leadership and insider risk has focused primarily on leaders' roles in communication and program support rather than the specific competencies leaders need to prevent insider threats (Alsowail & Al-Shehari, 2021; Rice & Searle, 2022; Stone, 2022).

These challenges are especially acute in healthcare, which continues to report the highest costs and frequency of insider-related security incidents of any industry (Balozian et al., 2023; Ponemon Institute, 2023, 2025; Zaiarnyi, 2025). Industry data indicate the average annual cost to remediate an insider incident in healthcare is $29.3 million, compared to $17.4 million across other industries (Ponemon Institute, 2023, 2025). Most healthcare insider incidents stem from unintentional causes, human error, and external actors targeting healthcare workers to obtain personally identifiable information, protected health information, and financial data (Bychkov, 2024; Hanson et al., 2021; Verizon, 2025), and the lack of dedicated leadership training contributes to this ongoing vulnerability (Alanazi, 2023; Lang, 2022a; Triplett, 2022).

The general problem addressed by this study was the lack of IRM training for organizational leaders, resulting in an inability to prevent insider-related security incidents. Leaders who lack IRM training may not fully understand the importance of compliance or the risks associated with noncompliance, limiting their ability to implement effective security policies (Ali et al., 2021). Similarly, untrained leaders may underestimate the nature and scope of insider threats, hindering mitigation efforts and increasing organizational risk exposure (Camp & Williams, 2022). Triplett (2022) argued that leaders are often unable to fully protect their organizations because they lack training in social engineering, human factors, information leakage, recognizing behavioral red flags, incident response, and regulatory compliance related to insider risk. Within healthcare specifically, leaders require training to understand how insider threats can compromise sensitive medical records, diagnostic data, and financial information across interconnected clinical and administrative systems (Alanazi, 2023; Hanson et al., 2021; Kumar & Shaw, 2025). The specific problem addressed by this study was the potential lack of IRM training for organizational leaders within a single healthcare organization, resulting in a possible inability to prevent insider-related security incidents.

The purpose of this qualitative case study was to explore the current state of IRM training for leaders, identify potential gaps in existing programs, examine leaders' perceptions of the importance of addressing insider threats, and understand leaders' roles and responsibilities in mitigating these risks. Through interviews with organizational leaders, a qualitative survey, and document analysis, this research sought to understand the relationship between IRM leadership training and leaders' ability to prevent insider incidents (Miller et al., 2023), with the goal of informing more effective, tailored IRM training strategies (Alanazi, 2023; Lee, 2022). This study was guided by one overarching research question and three sub-questions:

RQ: How can the problem of insufficient insider risk management training for organizational leaders be solved to enhance the prevention of security incidents related to insider threats?

- **RQa.** How do organizational leaders perceive the importance and urgency of addressing insider risk management training within the organization?
- **RQb.** What specific roles and responsibilities should organizational leaders assume in mitigating insider risks and promoting a culture of security awareness?
- **RQc.** What components of insider risk management training are most critical for equipping leaders to identify and respond to potential security incidents related to insider threats?

This study is significant because it addresses a critical gap in how organizations develop and implement IRM competencies among leaders, with direct implications for enhancing security posture and reducing losses associated with insider incidents (Lang, 2022a; Triplett, 2022). By investigating how healthcare organizations can better equip leaders with the knowledge, skills, and strategic capabilities needed to build security-conscious cultures, this research contributes actionable insight for healthcare organizations seeking to protect their assets, support their leaders, and safeguard the patients and communities they serve.

2. Literature Review

2.1 Leadership Practices Relevant to Insider Risk

Several leadership practices consistently appear in the literature as central to effective IRM, including risk awareness and assessment, communication, personnel management, culture-building, and information security practices. Risk awareness and assessment are core competencies leaders need to recognize early warning signs and implement preventative measures, yet without adequate training, leaders often lack the capability to distinguish complex insider risk patterns, particularly within multi-tiered healthcare systems (Alanazi, 2023; Bychkov, 2024; Millick, 2022; Stone, 2022; Zaiarnyi, 2025). Empirical research across multiple countries has linked leadership risk-assessment failures, including insufficient security training and inadequate internal oversight, to insider threat incidents (Steinle, 2022; Zeng et al., 2023), though the literature remains divided on the relative value of automated versus human judgment in identifying potential threats (Greitzer & Purl, 2022; Mishra, 2023; Xiao et al., 2024). Because insider risk assessment requires evaluating several interconnected dimensions of human behavior rather than isolated indicators, a more nuanced and balanced approach to risk assessment, one that blends technical monitoring with human judgment, is generally considered necessary (Greitzer & Purl, 2022; Jones, 2024; Lenzenweger & Shaw, 2022).

Communication and relationship-oriented leadership practices are similarly emphasized as critical to IRM, as leaders who build trust with employees are better positioned to recognize behavioral changes and encourage reporting (Balozian et al., 2023; Holden et al., 2024). Leaders also shape organizational culture directly, and culture in turn affects program success through security awareness, employee behavior, and prioritization of security initiatives (Harvey, 2022; Jun & Lee, 2023). Leaders who set clear standards, provide resources, and model ethical behavior create environments where employees are more likely to identify and report potential insider threats, while building a proactive security culture requires shifting the organizational posture from deterrence toward prevention through regular communication, transparent policies, and consistent enforcement (Lenzenweger & Shaw, 2022; Muthuswamy, 2023; Neufeld, 2023; Stone, 2022). Despite this body of research on desirable leadership practices, comparatively little empirical work has examined whether leaders possess the specific skills needed to enact these practices, or how organizations might train leaders to develop them, a gap that motivated this study's focus on leadership competencies rather than organizational policy alone.

2.2 The Overreliance on Technology

Contemporary IRM strategies reveal a persistent paradox: while research increasingly recognizes the human-centric nature of insider threats, organizations continue to prioritize technological solutions over human-focused interventions (Greitzer & Purl, 2022; Jones, 2024). Modern security infrastructures leverage sophisticated automated systems capable of monitoring networks and detecting anomalous activity at a scale beyond manual oversight (Alsowail & Al-Shehari, 2021; Thite & Iyer, 2024). Yet these technological safeguards face unique limitations when confronted with insider threats, as trusted insiders with intimate system knowledge can exploit legitimate access while evading detection (Aloraini et al., 2022; Subhani et al., 2021). A comprehensive analysis of insider threat research found that 70% of academic studies concentrated on technical detection mechanisms, while only 19% examined human behavioral aspects (Singh & Sharma, 2022), underscoring a persistent research and practice gap.

Insider incidents have continued to rise across private industry, public institutions, and government agencies despite substantial investment in technical controls, suggesting that overreliance on technology can undermine overall security posture by neglecting the human elements of threat detection (Jones, 2024; Ponemon Institute, 2023; Zangana et al., 2025). Organizations that heavily favor automated monitoring risk reducing direct leadership engagement with employees, causing them to miss vital behavioral warning signs that often precede technical indicators (Balozian et al., 2023; Greitzer & Purl, 2022; Mishra, 2023). Effective insider threat prevention therefore requires organizations to balance technical safeguards with well-trained leaders who understand the interplay of human behavior, organizational dynamics, and threat indicators (Caputo et al., 2024; Greitzer & Purl, 2022).

2.3 Leadership Training Gaps

Training and awareness strategies are widely regarded as critical to reducing insider incidents, particularly those stemming from unintentional or negligent behavior (Alsowail & Al-Shehari, 2021; Lang, 2022a). However, most organizations deliver training at the enterprise level for all employees or rely on automated, compliance-oriented modules rather than role-specific

instruction for leaders (Lang, 2022a; Triplett, 2022). Existing literature on leadership and insider risk has focused mainly on leaders' roles in communication, resource provision, and program support rather than on the specific competencies leaders need to recognize and respond to insider risk (Alassaf & Alkhalifah, 2021; Rice & Searle, 2022). Leadership perceptions and prioritization of IRM training significantly influence the success of any awareness program (Ali et al., 2021; Humaidi & Alghazo, 2022), yet clearly defined leadership roles and responsibilities for insider risk mitigation remain underdeveloped in both research and practice (Carpenter, 2022; Leslie et al., 2021; National Counterintelligence and Security Center, 2021).

Critical components of effective IRM training identified in the literature include situational awareness, information handling, communication, recognition of behavioral indicators and motives, and structured response strategies (Balozian et al., 2023; Varga et al., 2021), as well as threat appraisal, promotion of protective behaviors, and role-specific content (Humaidi & Alghazo, 2022). Despite this guidance, underfunding of IRM programs relative to technical security investment continues to undermine training efficacy (Al-Harrasi et al., 2023; Lang, 2022a; Whitelaw et al., 2024). Recent scholarship has begun to document the specific failure of generic, one-size-fits-all, and awareness-based training to build the specialized competencies leaders need (Caputo et al., 2024; Mady et al., 2023), a gap this study sought to address directly.

2.4 Insider Threats in the Healthcare Sector

Healthcare organizations face distinct challenges in addressing insider risk. Leaders in this sector must navigate complex regulatory environments, interconnected clinical and administrative systems, and heightened sensitivity of the data they protect, including protected health information and financial records (Alanazi, 2023; Hanson et al., 2021; Kumar & Shaw, 2025). Sophisticated insiders within healthcare organizations can exploit authorized access and detailed system knowledge to circumvent controls (Kumar & Shaw, 2025; Petrič & Roer, 2022; Zaiarnyi, 2025), and organizations that overly rely on automated monitoring often see reduced direct leadership engagement with staff, missing behavioral warning signs (Mishra, 2023; Whitelaw et al., 2024). The lack of dedicated leadership training remains a significant contributing factor to healthcare's ongoing vulnerability to insider threats (Alanazi, 2023; Lang, 2022a; Triplett, 2022), reinforcing the need for research that examines IRM training from the perspective of healthcare leaders themselves.

2.5 Conceptual Framework

This study was informed by a conceptual framework linking IRM to leadership training and organizational culture. The framework proposed that IRM directly influences the design of training programs; that training and development equip leaders with competencies needed for effective IRM; that organizational culture influences the effectiveness of IRM; and that insider risk and threat awareness, together with risk assessment and mitigation strategies, are essential for identifying and addressing insider risk. Organizational leaders, employees, human resources, information technology and cybersecurity personnel, compliance and legal functions, and external stakeholders such as regulators were identified as key actors whose knowledge, attitudes, skills, and organizational policies shape the effectiveness of IRM training. This

framework guided the development of the research questions and the interview and survey instruments used to explore the relationships among these concepts, actors, and constructs.

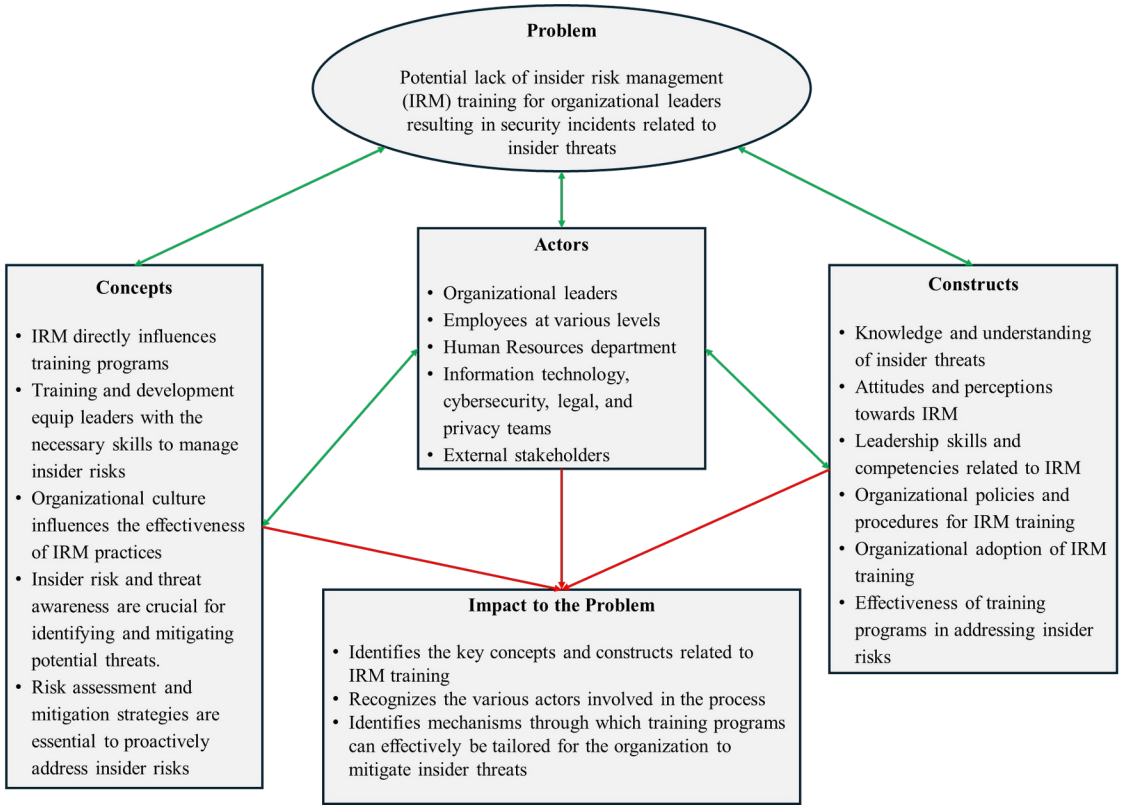

Figure 1. Research Framework

A significant gap exists in the literature regarding the relationship between leaders' formal IRM responsibilities and how they develop the competencies needed to implement IRM strategies and influence employee behavior (Caputo et al., 2024; Mady et al., 2023). This underrepresentation of leadership-specific training research has left organizations without evidence-based approaches for equipping leaders with critical IRM competencies (Islam & Ahmed, 2024; Lang, 2022a; Triplett, 2022). The current study addresses this gap by exploring, from the perspective of healthcare leaders, the state of IRM training, perceived gaps, and the roles and competencies leaders believe are most critical for effective insider risk management.

3. Method

3.1 Research Design

This qualitative single case study used a flexible design and methodological triangulation to explore IRM training for organizational leaders within a single U.S. healthcare organization. A flexible qualitative design was well suited to this research because the complexity of insider threats required an adaptable framework capable of responding to emerging insights during data collection and analysis (Bunyitai, 2023; McArdle, 2022). A single case study design provided the depth necessary to examine IRM training within a specific organizational context, allowing comprehensive exploration of multiple leadership perspectives within one

organization's unique risk environment (Camp & Williams, 2022; Okeke & Eiza, 2023; Viera, 2023). This approach was particularly appropriate given the sensitive nature of insider threat data and the deeply interconnected relationships among organizational dynamics, security practices, and leadership roles within a single healthcare institution (Alanazi, 2023; Balozian et al., 2023; Hanson et al., 2021).

Methodological triangulation, combining semi-structured interviews, a qualitative survey, and document analysis, was used to enhance the credibility and trustworthiness of the findings (Hanson-DeFusco, 2023; Kawar et al., 2024; Miller et al., 2023; Morgan, 2024). Triangulation allowed cross-verification of findings across multiple data sources and helped identify both convergence and divergence in participant perspectives (Dzwigol, 2022; Vivek et al., 2023). Throughout the study, the researcher maintained reflexivity and employed bracketing techniques, including a reflexive journal, member checking, and interview bracketing, to mitigate potential bias stemming from professional experience in the counterintelligence and insider threat field (Bukamal, 2022; Thomas & Sohn, 2023; van der Kraan et al., 2023).

3.2 Setting

The case organization was a healthcare and senior living services provider in the United States with approximately 200 employees spanning clinical, administrative, and support functions, including nursing, resident and dining services, human resources, information technology and cybersecurity, compliance, and administration. Its relatively compact organizational structure, in which leaders often oversee cross-functional responsibilities, made it a suitable single case for examining how IRM training gaps manifest across a range of leadership roles operating under a shared set of organizational policies and a common compliance infrastructure, most notably training tied to the Health Insurance Portability and Accountability Act (HIPAA).

3.3 Participants

Participants were recruited using purposive sampling with maximum variation to capture diverse leadership perspectives across organizational levels and functions (Ahmad & Wilkins, 2024; Heinrich et al., 2022). Eligible participants held formal leadership positions with direct reports, had at least one year of experience in their current role, held responsibility for implementing or enforcing information security policy, and were full-time employees of the case organization; individuals directly responsible for designing the organization's current IRM training were excluded to avoid defensive bias. The final sample included 15 participants (12 interviewees and three survey respondents) representing leadership levels from front-line supervisors to directors and officers across departments including administration, human resources, information technology and cybersecurity, compliance, resident and dining services, marketing, and nursing. This sample size aligned with research indicating that thematic saturation in interview-based studies typically occurs between 12 and 13 interviews in relatively homogeneous populations with narrowly defined research objectives (Hennink & Kaiser, 2022). Participants were interviewed with wide stratification across leadership levels, departments, tenure, and educational background to ensure a comprehensive view of the organization (see Table 1).

ID	Gender	Department	Leadership Level	Years in Role	Education Level
P1	Female	Philanthropy	Director	3.5	Bachelor's Degree
P2	Female	Environmental Services	Associate Director	9.0	Associate's Degree
P3	Female	Administrator	Officer	15.0	Bachelor's Degree
P4	Female	Human Resources	Director	19.5	Bachelor's Degree
P5	Female	Resident Services and Compliance	Director	3.0	Bachelor's Degree
P6	Male	President and Chief Executive Officer	Officer	4.0	PhD
P7	Female	Spiritual Care	Director	1.0	Master's Degree
P8	Female	Resident Service	Supervisor	3.5	High School Diploma
P9	Female	Healthcare Professional	Supervisor	1.5	Bachelor's Degree
P10	Female	Healthcare Professional	Supervisor	4.0	Associate's Degree
P11	Female	Healthcare Professional	Director	4.0	Master's Degree
P12	Female	Dining Services	Manager	9.0	High School Diploma
Survey Participants					
P13	Male	Information Technology	Manager	3.5	Vocational/ Trade School Diploma
P14	Female	Marketing and Sales	Director	4.0	Bachelor's Degree
P15	Female	Healthcare Professional	Supervisor	2.0	Associate's Degree

Table 1. Participant Information

3.4 Data Collection and Analysis

Data were collected through three methods. Semi-structured interviews, guided by a 15-question protocol organized into seven sections and directly aligned with the research question and sub-questions, served as the primary data source. Following an introductory section that

established informed consent and collected demographic information, the protocol used broad rapport-building questions before moving into sections that addressed the main research question, followed by sections corresponding to each sub-question, and concluding with an open-ended prompt inviting any additional reflections. Each core question was supported by structured probes to encourage natural conversational flow while ensuring consistent topic coverage across interviews, an approach designed to elicit rich narrative responses while minimizing leading questions (Adeoye-Olatunde & Olenik, 2021; Kawar et al., 2024). A complementary 28-item qualitative survey, administered to a separate group of respondents, used Likert-type, multiple-choice, and rating-scale items organized around participant background, perceptions of IRM importance, leadership roles and responsibilities, and critical training components, generating additional, quantifiable data to support triangulation (Clark et al., 2024; Islam & Ahmed, 2024). Document analysis of organizational training materials, security policies, and risk management documentation provided an objective, participant-independent perspective on actual training content and formally defined roles and responsibilities, helping distinguish gaps that were actually present in existing materials from those that were merely perceived by participants (Kawar et al., 2024; Morgan, 2024).

Interview and survey data were analyzed using thematic coding supported by NVivo software, beginning with automated and manual coding of interview transcripts (an initial 88 codes), followed by iterative manual re-coding to cluster codes into initial themes and, subsequently, six overarching themes (Cernasev & Axon, 2023; Naeem et al., 2023). Survey data were similarly coded and cross-referenced against interview findings to validate emerging patterns. Document analysis findings were compared against interview and survey data to identify areas of alignment or incongruence, completing the triangulation process (Miller et al., 2023).

3.5 Trustworthiness and Ethical Considerations

Trustworthiness was established through methodological triangulation, member checking of interview transcripts and preliminary findings, and sustained reflexivity throughout data collection and analysis (Geddis-Regan et al., 2022; Levitt et al., 2021; Thomas & Sohn, 2023). Given the researcher's dual insider-outsider positionality as an insider risk practitioner conducting research within a healthcare organization, bracketing techniques, including a reflexive journal and interview bracketing in which the researcher was interviewed using the same protocol prior to data collection, were used to surface and manage potential preconceptions (Bukamal, 2022; Satsanasupint et al., 2022).

The study adhered to the ethical principles articulated in the Belmont Report, including beneficence, respect for persons, and justice (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1978). All participants provided informed consent, and confidentiality was protected through the use of participant identifiers rather than names, secure password-protected data storage, and aggregate reporting of demographic information. Interview recordings were deleted following participant review and confirmation of transcript accuracy, and participants had the opportunity through member checking to review and request modifications to how their information was represented.

4. Results

Analysis of the interview, survey, and document data yielded six major themes describing the current state of IRM training and leaders' perceptions of their roles and responsibilities (see Table 2). Three themes were present universally across participants (intuitive awareness versus formal training gap, need for role-specific training, and preference for interactive leadership approaches), while three themes revealed important organizational dynamics (divided security culture perceptions, wide variance in leadership competency self-assessment despite universal skill gaps, and embedded compliance training that masks insider risk as a distinct discipline).

Theme	Description	Prevalence
1. Intuitive Awareness vs. Formal Training Gap	Leaders possess practical security awareness developed through daily experience but lack formal IRM training and terminology	Universal across all interview participants
2. Need for Role-Specific Training	Leaders request training tailored to departmental risk profiles rather than generic, organization-wide content	Most frequently requested solution (12 of 15 participants)
3. Preference for Interactive Leadership Approaches	Leaders favor in-person, scenario-based training and relationship-building over passive online modules	Nearly universal (11 of 12 interviewees)
4. Divided Security Culture Perceptions	Leaders hold sharply differing views of the organization’s security culture, ranging from strong to poor	Split: 8 strong, 6 poor, 2 neutral (with overlap)
5. Wide Variance in Leadership Competency Self-Assessment	Self-assessed IRM competency ranges from poor to strong despite universal formal training gaps, at times inversely related to training received	Present across all participants
6. Embedded Compliance Training Masks Insider Risk as a Distinct Discipline	Insider risk concepts are diluted within HIPAA, IT security, and general compliance training rather than addressed as a standalone topic	8 of 12 interviewees conflated IRM with compliance training

Table 2. Discovered Themes

4.1 Theme 1: Intuitive Awareness Versus Formal Training Gap

Every participant demonstrated a working understanding of security vulnerabilities and protective behaviors developed through daily experience, yet none had received structured education using insider risk terminology or frameworks. Eight of the 12 interviewees were unfamiliar with the terms *insider risk* or *insider threat* prior to the interview despite holding leadership positions responsible for protecting sensitive information daily. One participant candidly admitted, "when you say insider risk management, first thing I think of is what the heck is that?" while another stated, "I'm trying to understand what that insider risk term means," even while describing detailed protocols implemented to protect sensitive information. A third participant described how organizational language diverges by function: "That's not really the language that we use. We tend to just call it risk management and then safety\... IT might use a different language when they're talking about threats."

Rather than relying on formal frameworks, participants consistently described leaning on intuition and experience to identify potential risks. One leader explained, "I don't know about skills. I would be relying on intuition," while another noted, "I think most of my learning, even though I've done the training, is too many years in healthcare\... there are personality traits that tell you if someone is legit injured or faking it." Participants also described current training as fragmented across compliance, IT security, and emergency preparedness domains rather than delivered as a unified topic, and several noted that available training relied on a generic, industry-wide platform rather than content tailored to their organization. Survey data reinforced this pattern: a respondent who reported receiving no formal IRM training rated their own competency at the expert level (5 of 5), while a respondent who had completed training within the past year rated their competency lower (3 of 5), suggesting that experience-based confidence may not correspond with structured competency.

4.2 Theme 2: Need for Role-Specific Training

The most frequently articulated solution across participants was the need for training tailored to departmental risk profiles rather than generic, organization-wide content. Participants consistently noted that insider risks manifest differently across departments and that standardized training failed to reflect their specific operational realities. One leader explained that a security incident in their own department, while unlikely to be life-threatening, "does have a different type of transformational impact on my work" compared to a clinical setting, while another requested training "highly tailored to that situation\... something that tells me exactly what to do." Another participant illustrated the mismatch between generic content and daily reality: "All right, if the power goes out, what is my responsibility? What do I do in this? Of course, they'll do the generics\... but how does it directly, in a moment, affect me?" A leader responsible for resident-facing services similarly explained that department-specific framing shapes what training should prioritize: "The higher-up leaders are more worried about things on an organizational level. And in my lead position, I'm more focused on the residents than the entire organization." Survey respondents reinforced this pattern, requesting "a structured decision-making model for evaluating observed behaviors," "leadership specific guidance," and "a framework for assessing insider risks," with each respondent, drawn from different functional areas, identifying distinct training gaps. This variation across departments and roles suggested that a single standardized program is unlikely to meet the practical needs of a functionally diverse leadership population.

4.3 Theme 3: Preference for Interactive Leadership Approaches

With one exception, all participants advocated for in-person, scenario-based training over passive online modules. Participants described existing computer-based training as disengaging, noting that it "starts to get boring after the first hour" and that information delivered this way tends to go "in one ear and out the other." Several participants emphasized that in-person formats allow for dialogue and clarifying questions that online modules cannot support. Beyond training format, participants repeatedly identified relationship-building as foundational to effective IRM. One leader explained, "It's relationship building, getting to know their people, so they recognize if something's off," while another described actively checking in with staff when noticing behavioral changes: "When there's a change, I call them to my office and I'm just like, 'hey, you look like something's not right today. Are you doing OK?'" These findings suggest that

leaders view interpersonal engagement, not just formal instruction, as central to insider risk detection.

4.4 Theme 4: Divided Security Culture Perceptions

Participants held sharply divergent views of the organization's security culture. Some described security as "foremost in everyone's mind," while others characterized the culture as "naive" about potential threats and described being told to "stay in your lane" when raising cross-departmental security concerns. Several participants noted that resource constraints and competing priorities, including budgeting and staff retention, frequently overshadowed insider risk concerns, particularly at the middle management level. Despite an organizational ethos of "see something, say something," many participants described significant reporting hesitancy driven by fears of retaliation, concerns about the effectiveness of anonymity protections, and inconsistent disciplinary accountability across tenure levels. One participant explained, "I think a lot of people would be very hesitant to report something and believe that it's actually anonymous\... they think that's going to come back to them in the long run," while another observed that employees who raise concerns can become "disheartened or discouraged to speak up." A related tension emerged around leaders' willingness to act on concerns outside their own department: one leader acknowledged having the authority to address a policy violation but described feeling it was "not their place," while another firmly disagreed, stating that "it is our business regardless of who it is\... to take responsibility for the organization as a whole." Several participants also linked cultural inconsistency to accountability, describing uneven disciplinary responses to similar violations depending on an employee's tenure, and a felt absence of follow-through when concerns were raised. Survey data confirmed this division at a smaller scale: respondents gave conflicting assessments of whether senior leadership recognized the importance of IRM and whether resources allocated to it were adequate, and reported differing frequencies of conflict between security requirements and operational efficiency.

4.5 Theme 5: Wide Variance in Leadership Competency Self-Assessment Despite Universal Skill Gaps

Participants' self-assessed IRM competency varied widely, from low to high confidence, often within the same interview, despite a consistent underlying pattern of reliance on intuition rather than structured frameworks. Several participants expressed confidence in their ability to detect behavioral changes among staff but, when asked for specific indicators or escalation thresholds, were unable to provide concrete examples, falling back on descriptions such as "a fine line" or general appeals to intuition. A smaller number of participants offered specific, observable indicators, such as changes in attendance, documentation quality, or the emergence of narratives framing the organization as uniformly adversarial, but these insights were not systematically shared across the organization. One participant captured the difficulty of translating confidence into concrete criteria when asked to distinguish ordinary workplace frustration from a potential warning sign: "That's a fine line. If their behavior is destructive, or if it seems to be really out of line, I may ask for help." Another, reflecting on their own limitations, offered a more candid self-assessment: "I'm not always right. I certainly can't know everyone's true intentions. All I can do is be observant and record if possible." Survey data illustrated a paradoxical pattern consistent with the interview findings: the respondent with no formal training

rated all measured competencies at the expert level, while the respondent with the most recent formal training rated their competencies lowest among the three respondents, a pattern consistent with a potential overconfidence effect among untrained leaders (Jordan et al., 2022).

4.6 Theme 6: Embedded Compliance Training Masks Insider Risk as a Distinct Discipline

Eight of the 12 interviewees conflated IRM with existing compliance training, most commonly HIPAA-related instruction. Participants described how related concepts were addressed within broader compliance or risk committee structures rather than as a distinct discipline, with one noting plainly of HIPAA training, "The terms are not used." This fragmentation appeared to create genuine conceptual confusion: despite the fact that a majority of participants, across interviews and surveys, indicated that insider threats concerned them more than external threats, IRM was not treated as a distinct focus of organizational training. One participant summarized the terminology gap directly: "I've just heard it as 'risk,' not 'insider' or things of that sort\... this conversation kind of gave me a little idea." Another explained how compliance framing shapes the message employees receive: "The compliance training covers some of that, and it talks about ensuring that you don't leave your computer on or don't leave files open on your desk," without ever naming insider risk as a distinct concept. Because compliance training is typically oriented toward rule-following to avoid regulatory penalties, embedding insider risk within it risks employees perceiving the topic as another compliance checkbox rather than a distinct security discipline warranting sustained attention. Document analysis corroborated this pattern, showing that insider risk concepts were addressed only incidentally within broader regulatory compliance materials rather than through standalone content, reinforcing participants' descriptions of a diluted and diffuse approach to insider risk education.

5. Discussion

The findings of this study directly address the research questions by demonstrating that the case organization's fragmented, compliance-embedded approach to training fundamentally failed to develop the specialized competencies leaders need for effective insider risk management. In response to the overarching research question, the results indicate that solving the problem of insufficient IRM training requires establishing insider risk as a distinct training domain with dedicated terminology, rather than continuing to diffuse related concepts across compliance, IT security, and emergency preparedness programs. With respect to RQa, leaders' perceptions of IRM importance and urgency were shaped less by disagreement over whether insider risk mattered and more by inconsistent prioritization relative to competing operational demands, producing a largely reactive rather than proactive organizational posture. Regarding RQb, the findings suggest that leaders' core responsibilities in mitigating insider risk center on relationship-building, behavioral observation, and the creation of psychological safety for reporting, responsibilities that current training does little to formally develop. Finally, in response to RQc, participants identified foundational terminology and awareness, behavioral recognition skills, structured decision-making and escalation frameworks, department-specific scenarios, and interactive delivery methods as the most critical components of effective IRM training.

These findings both confirm and extend the existing literature. Consistent with prior research on the ineffectiveness of generic, awareness-based training (Caputo et al., 2024; Mady et al., 2023; Stone, 2022), participants described current training as disengaging and poorly matched to their operational realities. The study also corroborates literature documenting organizations' persistent overemphasis on technological solutions relative to human-centered approaches (Greitzer & Purl, 2022; Jones, 2024). However, the findings diverge from the literature in at least two important respects. First, while prior research emphasized technology and human-factor integration as a central challenge (Balozian et al., 2023; Singh & Sharma, 2022), this theme was largely absent from participant accounts; instead, leaders in this smaller healthcare organization emphasized relationship-building and direct behavioral observation over technology integration concerns. Second, while the literature has documented the general failure of one-size-fits-all training, it has not previously examined how *embedding* insider risk concepts within broader compliance frameworks can actively dilute their distinctiveness. This study's identification of the embedded compliance theme suggests that the problem of ineffective IRM training extends beyond simple resource allocation or training absence to encompass structural flaws in how organizations conceptually organize insider risk content.

The wide variance in leadership competency self-assessment, and its apparent inverse relationship with formal training in this sample, raises the possibility of an overconfidence effect among untrained leaders consistent with the Dunning-Kruger phenomenon (Jordan et al., 2022). If leaders with the least formal preparation are also the most confident in their capabilities, organizations may face a compounding risk: leaders unaware of their own knowledge gaps may be less likely to seek out or engage meaningfully with future training, even as their organizations remain exposed to preventable insider incidents.

The findings also help refine the conceptual framework that guided this study. The framework proposed that IRM directly shapes training design, that training equips leaders with necessary competencies, and that organizational culture influences IRM effectiveness. The results affirm each of these relationships while adding an important qualification: the effect of training on competency was not straightforwardly additive in this sample, and organizational culture did not operate as a single, unified influence but instead varied meaningfully by leadership level and department. Similarly, while the framework identified organizational leaders as the central actors in IRM, the findings suggest that leaders' effectiveness in this role depends heavily on interpersonal relationships with frontline employees, positioning relationship quality as a construct that may deserve more explicit treatment in future conceptual models of IRM leadership training.

6. Implications for Practice

6.1 Core IRM Leadership Competencies

Analysis of participant responses identified six core competency areas that organizations can use to structure IRM leadership training: observation and recognition skills, such as identifying behavioral warning signs and unusual patterns; communication and relationship skills, including building strong employee relationships and conducting sensitive conversations; analytical and decision-making skills, such as situational analysis and risk assessment; leadership and management skills, including coaching team members and creating psychological safety for

reporting; knowledge and awareness skills, such as understanding departmental risk profiles and staying current on emerging threats; and investigative and response skills, including gathering information and following appropriate escalation procedures. Twelve of the 15 participants identified observation and recognition, together with communication and relationship skills, as the foundation of effective IRM, echoed in one leader's description of IRM as fundamentally about "relationship building, getting to know their people, so they recognize if something's off." Framing IRM training around these explicit competencies represents a shift away from assuming leaders intuitively understand their security responsibilities and toward a structure that organizations can deliberately train, evaluate, and reinforce.

6.2 A Five-Pillar Framework for IRM Training Design

Building on these competencies, the findings support a five-pillar framework organizations can use to redesign IRM training for leaders. The pillars are interdependent: removing any one weakens the others, and organizations that have addressed only one or two pillars, most commonly delivering some form of training without customizing or institutionalizing it, are the ones most likely to reproduce the fragmentation this study identified.

- **Recognition.** Establish insider risk as a distinct discipline with its own terminology and competencies, rather than folding it into HIPAA, IT security, or general compliance training. This directly addresses the *Embedded Compliance Training Masks Insider Risk as a Distinct Discipline* theme, in which participants consistently conflated IRM with routine regulatory content (Caputo et al., 2024; Mady et al., 2023).
- **Customization.** Tailor training content to each department's specific risk profile and operational context instead of deploying a single generic, organization-wide curriculum, consistent with the *Need for Role-Specific Training* theme and participants' repeated requests for content that reflects their actual work.
- **Integration.** Combine behavioral recognition skills with structured decision-making frameworks so leaders can move from unsystematic intuition toward a repeatable evaluation process for assessing observed behavior.
- **Implementation.** Deliver training through interactive, scenario-based methods rather than passive online modules, reflecting participants' strong and near-universal preference for in-person, applied learning over computer-based training they described as disengaging.
- **Institutionalization.** Embed insider risk awareness into leadership performance expectations and organizational culture so it functions as an ongoing responsibility rather than an annual compliance event, addressing the inconsistent prioritization documented in the *Divided Security Culture Perceptions* theme.

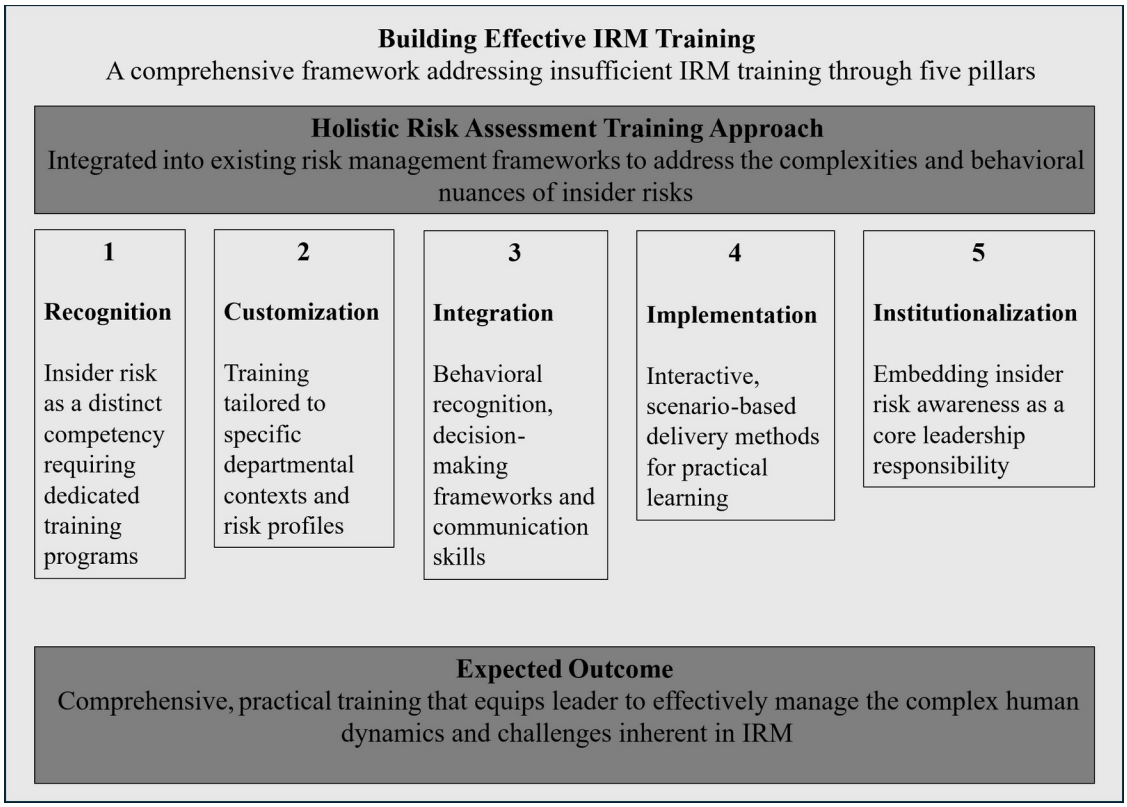

Figure 2. Holistic Risk Assessment Training Approach

6.3 Practical Implementation Strategies

Several concrete strategies can support this framework. Organizations can develop clear, context-specific behavioral indicators that help leaders distinguish ordinary workplace stressors from behaviors that merit reporting, while explicitly differentiating negligent from intentional policy violations. A structured assessment framework, evaluating observed behavior along dimensions such as policy compliance, intent, access level, and potential impact, can help leaders move beyond intuition toward a more systematic, repeatable evaluation process. Scenario- and skills-based training, built around realistic case examples relevant to each department, directly addresses leaders' expressed preference for practical, applied learning over passive instruction. Finally, establishing clear escalation thresholds, ranging from watchful awareness to urgent reporting, along with defined "red line" behaviors that require immediate escalation regardless of other factors, can reduce the uncertainty that often prevents leaders from acting on early warning signs.

Taken together, these findings suggest that healthcare organizations, and potentially organizations in other sectors facing similar challenges, should treat leadership-focused IRM training as a distinct strategic investment rather than a subordinate component of general compliance training. Doing so may improve leaders' ability to recognize and respond to insider risk while fostering the kind of security culture that supports, rather than discourages, early reporting.

7. Limitations and Directions for Future Research

This study is subject to several limitations inherent to its design. As a single case study of one healthcare organization with approximately 200 employees, the findings are not intended to be statistically generalizable to other organizations or industries, though they may offer analytic insight applicable to similar contexts. The relatively small qualitative survey sample (n = 3), while useful for triangulation, limits the extent to which survey findings alone can be considered representative. Additionally, the researcher's professional background in counterintelligence and insider threat management, while providing valuable subject-matter expertise, required ongoing reflexive management of dual insider-outsider positionality; although bracketing techniques were employed throughout, some degree of interpretive influence cannot be fully eliminated.

Several directions for future research emerge from these findings. First, the paradoxical relationship observed between formal training and self-assessed competency merits further investigation through mixed-methods designs that combine self-report data with objective competency assessment, behavioral observation, or incident-response simulation, to determine whether overconfident but undertrained leaders pose greater organizational risk than those who more accurately assess their own gaps. Second, this study examined IRM exclusively from the leadership perspective; future research should explore employees' perceptions of their leaders' IRM competency and how these perceptions shape reporting behavior and organizational security culture. Third, a multi-case study comparing IRM training effectiveness across healthcare organizations of varying size and structure would help determine whether the patterns identified here, particularly the gap between intuitive awareness and formal training, generalize across the broader healthcare sector. Finally, quantitative research using larger samples could statistically test the relationships suggested by this study's qualitative findings, including the association between training exposure, delivery format, and leadership confidence in IRM competencies.

8. Conclusion

This qualitative single case study explored potential IRM training deficiencies among healthcare leaders and their impact on organizational security posture. Through methodological triangulation involving semi-structured interviews, a qualitative survey, and document analysis, the research identified six themes demonstrating a fundamental disconnect between organizational security needs and current training approaches. While all participants possessed intuitive security awareness developed through daily operational experience, none had received formal IRM training using standardized terminology or systematic frameworks, and the majority were unfamiliar with basic insider risk terminology despite holding leadership positions requiring daily protection of sensitive information.

Rather than treating insider risk as a distinct discipline, the case organization's training approach diffused related concepts across compliance, IT security, and emergency preparedness domains, preventing leaders from developing the specialized competencies needed for effective recognition and response. Leaders expressed a strong and consistent preference for role-specific, interactive training over generic, passive instruction, and the study surfaced significant divisions in perceived security culture alongside a troubling, potentially inverse relationship between formal training exposure and leadership confidence. Based on

these findings, this study proposes a five-pillar implementation framework, recognition, customization, integration, implementation, and institutionalization, to guide healthcare organizations in developing more effective, human-centered IRM training for their leaders. These findings offer healthcare organizations, and potentially organizations in other sectors facing comparable challenges, evidence-based direction for strengthening leadership capability and organizational resilience against insider threats.

References

Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. Journal of the American College of Clinical Pharmacy, 4(10), 1358-1367. https://doi.org/10.1002/jac5.1441

Ahmad, M., & Wilkins, S. (2024). Purposive sampling in qualitative research: A framework for the entire journey. Quality & Quantity. https://doi.org/10.1007/s11135-024-02022-5

Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2023), Towards protecting organisations' data by preventing data theft by malicious insiders. International Journal of Organizational Analysis, 31(3), 875-888. https://doi.org/10.1108/IJOA-01-2021-2598

Alanazi, A. T. (2023). Clinicians' perspectives on healthcare cybersecurity and cyber threats. Curēus (Palo Alto, CA), 15(10), e47026-e47026. https://doi.org/10.7759/cureus.47026

Alassaf, M., & Alkhalifah, A. (2021). Exploring the influence of direct and indirect factors on information security policy compliance: A systematic literature review. IEEE Access, 9, 162687-162705. https://doi.org/10.1109/ACCESS.2021.3132574

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Applied Sciences, 11(8), 3383. MDPI AG. http://dx.doi.org/10.3390/app11083383

Aloraini, F., Javed, A., Rana, O., & Burnap, P. (2022). Adversarial machine learning in IoT from an insider point of view. Journal of Information Security and Applications, 70, 103341. https://doi.org/10.1016/j.jisa.2022.103341

Alsowail, R. A., & Al-Shehari, T. (2021). A multi-tiered framework for insider threat prevention. Electronics (Basel), 10(9), 1005. https://doi.org/10.3390/electronics10091005

Balozian, P., Burns, A. J., & Leidner, D. E. (2023). An adversarial dance: Toward an understanding of insiders' responses to organizational information security measures. Journal of the Association for Information Systems, 24(1), 161-221. https://doi.org/10.17705/1jais.00798

Bukamal, H. (2022). Deconstructing insider\--outsider researcher positionality. British Journal of Special Education, 49(3), 327-349. https://doi.org/10.1111/1467-8578.12426

Bunyitai, Á. (2023). Insider threat mitigation in high security facilities. Nemzetbiztonsagi Szemle = National Security Review, 11(1), 49-61. https://doi.org/10.32561/nsz.2023.1.4

Burns, A. J., Roberts, T. L., Posey, C., Lowry, P. B., & Fuller, B. (2023). Going beyond deterrence: A middle-range theory of motives and controls for insider computer abuse. Information Systems Research, 34(1), 342-362. https://doi.org/10.1287/isre.2022.1133

Bychkov, D. (2024). Insider threats to the military health system: A systematic background check of TRICARE west providers. JMIRx Med, 5, e52198-e52198. https://doi.org/10.2196/52198

Camp, N. J., & Williams, A. D. (2022). Lessons learned from a comparative analysis of counterintelligence and insider threat mitigation case studies in nuclear facilities. SN Computer Science, 3(2), 143. https://doi.org/10.1007/s42979-021-00996-9

Caputo, D. D., Danley, L., & Ratcliff, N. J. (2024). Employee risk recognition and reporting of malicious elicitations: Longitudinal improvement with new skills-based training. Frontiers in Psychology, 15, 1410426. https://doi.org/10.3389/fpsyg.2024.1410426

Carpenter, T. (2022). How can misconduct behaviours and abuse of position be better identified, and what are the drivers for committing fraud and theft? Journal of Financial Compliance, 6(1), 40-48. https://doi.org/10.69554/ZRWS1702

Cernasev, A., & Axon, D. R. (2023). Research and scholarly methods: Thematic analysis. Journal of the American College of Clinical Pharmacy, 6(7): 751-755. doi:10.1002/jac5.1817

Choi, S. H. (2023, June 12). Ex-Samsung electronics executive accused of stealing secrets for China chip factory. Reuters. https://www.reuters.com/technology/south-korea-indicts-ex-samsung-elec-executive-alleged-data-leak-china-2023-06-12/

Clark, N., Quan, C., Elgharbawy, H., David, A., Li, M. E., Mah, C., Murphy, J. K., Costigan, C. L., Ganesan, S., & Guzder, J. (2024). Why collect and use Race/Ethnicity data? A qualitative case study on the perspectives of mental health providers and patients during COVID-19. International Journal of Environmental Research and Public Health, 21(11), 1499. https://doi.org/10.3390/ijerph21111499

Dzwigol, H. (2022). Research methodology in management science: Triangulation. Virtual Economics, 5(1), 78-93. https://doi.org/10.34021/ve.2022.05.01(5)

Geddis-Regan, A. R., Exley, C., & Taylor, G. D. (2022). Navigating the dual role of clinician-researcher in qualitative dental research. JDR Clinical and Translational Research, 7(2), 215-217. https://doi.org/10.1177/2380084421998613

Greitzer, F. L., & Purl, J. (2022). The dynamic nature of insider threat indicators. SN Computer Science, 3(102), 2-15. https://doi.org/10.1007/s42979-021-00990-1

Hanson-DeFusco, J. (2023). What data counts in policymaking and programming evaluation \-- relevant data sources for triangulation according to main epistemologies and philosophies within social science. Evaluation and Program Planning, 97, 102238. https://doi.org/10.1016/j.evalprogplan.2023.102238

Hanson, J., Thorsen, T., & Hunstad, N. (2021). Insider threat programmes: Time to hit restart. Cyber Security, 4(3), 213-222. https://doi.org/10.69554/GZFF9998

Harvey, D. (2022). The insider threat to financial services: Why a shift in mindset is required to combat this silent risk. Cyber Security, 6(1), 34-40. https://doi.org/10.69554/DVHB3890

Heinrich, C. H., McHugh, S., McCarthy, S., & Donovan, M. D. (2022). Barriers and enablers to deprescribing in long-term care: A qualitative investigation into the opinions of healthcare professionals in Ireland. PloS One, 17(12), e0274552-e0274552. https://doi.org/10.1371/journal.pone.0274552

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. Social Science & Medicine (1982), 292, 114523-114523. https://doi.org/10.1016/j.socscimed.2021.114523

Holden, H., Munro, V., Tsakiris, L., & Wilner, A. (2024). "The pull to do nothing would be strong": Limitations & opportunities in reporting insider threats. Information Security Journal: A Global Perspective, 34(1), 63\--78. https://doi.org/10.1080/19393555.2024.2387347

Humaidi, N. & Alghazo, A. S. H. (2022). Procedural information security countermeasure awareness and cybersecurity protection motivation in enhancing employee's cybersecurity protective behaviour. 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, 2022, Institute of Electrical and Electronics Engineers (IEEE), 1-10. https://doi.org/10.1109/ISDFS55398.2022.9800834

Islam, S. M., & Ahmed, M. M. (2024). Evaluating security risk among source operators in nuclear and radiological facilities. Annals of Nuclear Energy, 206. https://doi.org/10.1016/j.anucene.2024.110656

Jones, L. A. (2024). Unveiling human factors: Aligning facets of cybersecurity leadership, insider threats, and arsonist attributes to reduce cyber risk. Socioeconomic Challenges, 8(2), 44-63. https://doi.org/10.61093/sec.8(2).44-63.2024

Jordan, K., Zajac, R., Bernstein, D., Joshi, C., & Garry, M. (2022). Trivially informative semantic context inflates people's confidence they can perform a highly complex skill. Royal Society Open Science, 9(3), 211977. https://doi.org/10.1098/rsos.211977

Jun, K., & Lee, J. (2023). Transformational Leadership and followers' innovative behavior: Roles of commitment to change and organizational support for creativity. Behavioral sciences (Basel, Switzerland), 13(4), 320. https://doi.org/10.3390/bs13040320

Kawar, L. N., Dunbar, G. B., Aquino-Maneja, E. M., Flores, S. L., Squier, V. R., & Failla, K. R. (2024). Quantitative, qualitative, mixed methods, and triangulation research simplified. The Journal of Continuing Education in Nursing, 55(7), 1-344. https://doi.org/10.3928/00220124-20240328-03

Kumar, S., & Shaw, D. K. (2025). Efficient access requests management for healthcare data with security and privacy-preserving. Expert Systems with Applications, 267, 126194. https://doi.org/10.1016/j.eswa.2024.126194

Lang, E. L. (2022a). Seven (Science-Based) commandments for understanding and countering insider threats. Counter-Insider Threat Research and Practice, 1(1). https://citrap.scholasticahq.com

Lang, E. L. (2022b). The security net, safety net, and stakeholder net for countering insider theat. Counter-Insider Threat Research and Practice, 1(1). https://citrap.scholasticahq.com

Lee, I. (2022). Analysis of insider threats in the healthcare industry: A text mining approach. Information (Basel), 13(9), 404. https://doi.org/10.3390/info13090404

Lenzenweger, M. F., & Shaw, E. D. (2022). The critical pathway to insider risk model: Brief overview and future directions. Counter-Insider Threat Research and Practice, 1(1). https://citrap.scholasticahq.com

Leslie, I., Van Sickle, M., Lynch, P., & Crawford, C. (2021). The role of human resources function in the mitigation of insider threats in organizations. Institute of Nuclear Materials Management, 1-10. https://resources.inmm.org

Levitt, H. M., Morrill, Z., Collins, K. M., & Rizo, J. L. (2021). The methodological integrity of critical qualitative research: Principles to support design and research review. Journal of Counseling Psychology, 68(3), 357\--370. https://doi.org/10.1037/cou0000523

Mady, A., Gupta, S., & Warkentin, M. (2023). The effects of knowledge mechanisms on employees' information security threat construal. Information Systems Journal (Oxford, England), 33(4), 790-841. https://doi.org/10.1111/isj.12424

McArdle, R. (2022). Flexible methodologies: A case for approaching research with fluidity. The Professional Geographer, 74(4), 620-627. https://doi.org/10.1080/00330124.2021.2023593

Mészáros, A. A., & Kelemen-Erdős, A. (2023). Industrial espionage from a human factor perspective. Journal of International Studies (Kyiv), 16(3), 97-116. https://doi.org/10.14254/2071-8330.2023/16-3/5

Miller, E., Porter, J., & Barbagallo, M. (2023). Simplifying qualitative case study research methodology: A step-by-step guide using a palliative care example. Qualitative Report, 28(8), 2363-2379. https://doi.org/10.46743/2160-3715/2023.6478

Millick, B. (2022). Counter-Insider Threat: A Process of Evolution\... and a Point of Departure. Counter-Insider Threat Research and Practice, 1(1). https://citrap.scholasticahq.com

Mishra, S. (2023). Exploring the impact of ai-based cyber security financial sector management. Applied Sciences, 13, 5875. https://doi.org/10.3390/app13105875

Morgan, H. (2024). Using triangulation and crystallization to make qualitative studies trustworthy and rigorous. Qualitative Report, 29(7), COV4-1856. https://doi.org/10.46743/2160-3715/2024.6071

Muthuswamy, V. V. (2023). Cyber security challenges faced by employees in the digital workplace of Saudi Arabia's digital nature organization. International Journal of Cyber Criminology, 17(1), 40-53. https://doi.org/10.5281/zenodo.4766603

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. International Journal of Qualitative Methods, 22, 1-18. https://doi.org/10.1177/16094069231205789

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1978). The Belmont report: Ethical principles and guidelines for the protection of human subjects of research. Department of Health, Education, and Welfare, National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. www.hhs.gov

National Counterintelligence and Security Center. (2021). Insider threat mitigation for U.S. critical infrastructure entities. Guidelines from an intelligence perspective. Office of the Director of National Intelligence. https://www.dni.gov

Neufeld, D. (2023). Computer crime motives: Do we have it right? Sociology Compass, 17(4), 1-42. https://doi.org/10.1111/soc4.13077

Okeke, R. I., & Eiza, M. H. (2023). The application of role-based framework in preventing internal identity theft related crimes: A qualitative case study of UK retail companies. Information Systems Frontiers, 25(2), 451-472. https://doi.org/10.1007/s10796-022-10326-w

Petrič, G., & Roer, K. (2022). The impact of formal and informal organizational norms on susceptibility to phishing: Combining survey and field experiment data. Telematics and Informatics, 67, 101766. https://doi.org/10.1016/j.tele.2021.101766

Ponemon Institute. (2023). 2023 cost of insider risks global report. DTEX Systems Inc. https://www2.dtexsystems.com

Ponemon Institute. (2025). 2025 cost of insider risks global report. DTEX Systems Inc. https://ponemon.dtexsystems.com

Rice, C., & Searle, R. H. (2022). The enabling role of internal organizational communication in insider threat activity \-- evidence from a high security organization. Management Communication Quarterly, 36(3), 467-495. https://doi.org/10.1177/08933189211062250

Satsanasupint, P., Daovisan, H., & Phukrongpet, P. (2022). Enhancing active ageing in later life: Can community networks enhance elderly health behaviours? Insights from a bracketing qualitative method. Journal of Community & Applied Social Psychology, 32(6), 1133-1147. https://doi.org/10.1002/casp.2628

Schoenherr, J. R. (2022). Insider threats and individual differences: Intention and unintentional motivations. IEEE Transactions on Technology and Society, 3(3), 175-184. https://doi.org/10.1109/TTS.2022.3192767

Singh, A.P. & Sharma, A. (2022). A systemic literature review on insider threats. arXiv:2212.05347v1 [cs.CR], 1-9. https://doi.org/10.48550/arXiv.2212.05347

Steinle, M. J. (2022). Assessing and mitigating risk in airport greenfield and redevelopment programmes. Journal of Airport Management, 16(4), 388-402. https://doi.org/10.69554/EDIR1751

Stone, A. G. (2022). The role risk-management plays in reducing insider threat's in the federal government. Information Security Journal, 31(3), 338-345. https://doi.org/10.1080/19393555.2021.1998735

Subhani, A., Khan, I. A., & Zubair, A. (2021). Review of insider and insider threat detection in the organization. Journal of Advanced Research in Social Sciences and Humanities, 6(4), 167-174. https://dx.doi.org/10.26500/JARSSH-06-2021-0402

Thite, M., & Iyer, R. (2024). Addressing the gap in information security: An HR-centric and AI-driven framework for mitigating insider threats. Personnel Review. https://doi.org/10.1108/PR-04-2023-0358

Thomas, S. P., & Sohn, B. K. (2023). From uncomfortable squirm to self-discovery: A phenomenological analysis of the bracketing experience. International Journal of Qualitative Methods, 22. https://doi.org/10.1177/16094069231191635

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. Journal of Cybersecurity and Privacy, 2(3), 573-586. https://doi.org/10.3390/jcp2030029

van der Kraan, Yvonne M., Paap, D., Lennips, N., Veenstra, E. C. A., Wink, F. R., Kieskamp, S. C., & Spoorenberg, A. (2023). Patients' needs concerning patient education in axial spondyloarthritis: A qualitative study. Rheumatology and Therapy, 10(5), 1349-1368. https://doi.org/10.1007/s40744-023-00585-7

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. Computers & Security, 105, 102239. https://doi.org/10.1016/j.cose.2021.102239

Verizon. (2025). 2025 Data breach investigations report. https://www.verizon.com

Viera, C. A. (2023). Case study as a qualitative research methodology. Performance Improvement (International Society for Performance Improvement), 62(4), 125-129. https://doi.org/10.56811/PFI-23-0005

Vivek, R., Nanthagopan, Y., & Piriyatharshan, S. (2023). Beyond methodology: Theoretical foundations of triangulation in qualitative and multi-method research: A literature review. Naukovì Studìï Ìz socìal'noï Ta Polìtičnoï Psihologìï, 29(2), 53-62. https://doi.org/10.61727/sssppj/2.2023.53

Whitelaw, F., Riley, J., & Elrmabit, N. (2024). A review of the insider threat, a practitioner perspective within the UK financial services. IEEE Access, 12, 34752-34768. https://doi.org/10.1109/ACCESS.2024.3373265

Whitty, M. T. (2021). Developing a conceptual model for insider threat. Journal of Management & Organization, 27(5), 911-929. https://doi.org/10.1017/jmo.2018.57

Xiao, H., Zhu, Y., Zhang, B., Lu, Z., Du, D., & Liu, Y. (2024). Unveiling shadows: A comprehensive framework for insider threat detection based on statistical and sequential analysis. Computers & Security, 138, 103665. https://doi.org/10.1016/j.cose.2023.103665

Zaiarnyi, O. (2025). Cyber risk management in the business strategies of healthcare institutions and compliance with digital patients' rights: Eu experience and proposals for Ukraine in wartime. Baltic Journal of Economic Studies, 11(1), 95-103. https://doi.org/10.30525/2256-0742/2025-11-1-95-103

Zangana, H. M., Sallow, Z. B., & Omar, M. (2025). The human factor in cybersecurity: Addressing the risks of insider threats. Jurnal Ilmiah Computer Science, 3(2), 76-85. https://doi.org/10.58602/jics.v3i2.37

Zatonatskiy, D., Marhasova, V., & Korogod, N. V. (2021). Insider threat management as an element of the corporate economic security. Fìnansovo-Kreditna dìâl'nìst': Problemi Teorìï Ta Praktiki (Online), 1(36), 149-158. https://doi.org/10.18371/fcaptp.v1i36.227690

Zeng, M., Dian, C., & Wei, Y. (2023). Risk assessment of insider threats based on IHFACS-BN. Sustainability, 15(1), 491. https://doi.org/10.3390/su15010491

About the Author

Dr. Joshua L. Barrett, DSL, is a human-centric insider risk researcher and practitioner who studies all things insider risk and threat through a human lens, with specific focus on leaders, security culture, and reporting cultures. A retired U.S. Marine Corps Chief Warrant Officer with a counterintelligence and human intelligence background spanning the Intelligence Community, the Department of Defense, and the financial services sector, he holds a Doctor of Strategic Leadership from Liberty University and is the founder of Dolos Imperative LLC. This applied

research study is drawn from his doctoral dissertation, a qualitative case study of insider risk management training gaps among organizational leaders within a healthcare organization.

About Dolos Imperative

Dolos Imperative LLC delivers human elements security consulting, research, and training, helping organizations understand and manage the human dimension of insider risk. Learn more at dolosimperative.com.

