Law, Economics and Society; Vol. 1, No. 1; 2025
ISSN 3066-9340 E-ISSN 3066-9359
https://doi.org/10.30560/les.v1n1p93

Illegal Cybersecurity Threats Created by Organizational Arsonists in Healthcare Organizations

Laura Ann Jones[1] & Darrell Norman Burrell[2]

[1] Dissertation Faculty, Capitol Technology University, Laurel, MD, United States. ORCID: https://orcid.org/0000-0002-0299-370X

[2] Associate Ethics Fellow, Marymount University, Arlington, VA, United States. ORCID: https://orcid.org/0000-0002-4675-9544

Correspondence: Laura Ann Jones, Dissertation Faculty, Capitol Technology University, Laurel, MD, United States. E-mail: lajones@captechu.edu

Received: February 1, 2025 Accepted: February 17, 2025 Online Published: February 28, 2025

Abstract

Insider cybersecurity threats in healthcare, often overlooked or narrowly defined as technical vulnerabilities, can be more accurately described as acts of organizational arson, representing deliberate, malicious acts designed to ignite chaos within digital ecosystems. Like physical arsonists who destroy property through fire, insider actors exploit their privileged access to organizational systems, causing financial devastation, operational disruption, and severe damage to organizational morale and stability. Insider incidents cost organizations millions annually, with cybersecurity teams dedicating significant time and resources to crisis management rather than strategic planning. This commentary-style paper reframes insider cybersecurity threats using the metaphor of organizational arsonists, offering a unique and powerful framework for understanding these complex risks. By integrating cybersecurity, law, and organizational psychology insights, the paper presents a comprehensive approach to mitigating insider threats that extend beyond technical defenses. It emphasizes the necessity of human-centric strategies, ethical accountability, and legal compliance, calling for organizations to adopt a holistic defense posture that addresses both technological vulnerabilities and behavioral risks. The paper's originality lies in bridging multiple disciplines and framing insider threats as technical challenges and full-scale organizational crises. Combining advanced technologies such as artificial intelligence with human behavior analysis provides actionable strategies for organizations to combat their own digital arsonists. This interdisciplinary approach encourages cybersecurity professionals, legal scholars, and organizational leaders to rethink insider threat management, creating a more resilient and secure organizational environment.

Keywords: insider cybersecurity threats, healthcare cybersecurity, healthcare administration, organizational arsonists, cybersecurity risk management, insider threat detection, organizational behavior, organizational culture

JEL Codes: K24, K42, M15, D23, O33, H56

1. Introduction

1.1 Introduction

Cybersecurity risks in organizations demonstrate one of the biggest challenges facing organizations today (Espinoza, 2023; Jones et al., 2023; Lewis et al., 2023). Insider cybersecurity threats represent a formidable endeavor for healthcare organizations due to the sensitive and highly valuable data they manage, including personally identifiable information (PII), protected health information (PHI), financial records, and proprietary research data (Burrell, 2023; Burrell et al., 2021; Burrell, 2024). Unlike external threats, insider threats are particularly complex because they originate from individuals who possess legitimate access to internal systems and databases, making detection and mitigation more difficult (Wright, 2023). These threats do not fit neatly into a single category but manifest in diverse ways that can lead to significant operational and reputational damage (Jones, 2021). A clearer understanding of insider threats in healthcare requires recognizing that they can generally be categorized into malicious insiders, negligent insiders, and compromised insiders. Malicious insiders are individuals who intentionally exploit their privileged access for personal gain or to inflict harm. Such actions are premeditated, often involving employees who sell patient data to external entities, such as fraudulent billing operations or identity theft rings, or those who sabotage IT systems in retaliation for perceived grievances (Burrell et al., 2023). These incidents not only expose highly sensitive data but also compromise organizational trust and patient safety. In contrast, negligent insiders are more accidental in nature, though no less damaging. Often unaware of the potential consequences of their actions, these individuals might inadvertently click on phishing emails, mishandle confidential files, or misconfigure security settings. Such errors, though unintentional, frequently result in data breaches or open the door for ransomware infections, causing widespread operational disruption and data loss (Burrell et al., 2023). Lastly, compromised insiders occur when employees' credentials are stolen and used by external actors to access systems under the guise of legitimate users. Through tactics like phishing and social engineering, external attackers can easily bypass security protocols once inside the network, leaving the organization vulnerable to deeper, more sustained attacks (Burrell et al., 2023).

Several interconnected factors have contributed to the proliferation of insider threats in healthcare organizations. The first and most significant is the sheer value of healthcare data. Cybercriminals are drawn to this data due to their high worth on the black market, with insider threats often driven by the ease of access and potential financial rewards from selling sensitive patient information (Burrell et al., 2023). Adding to this vulnerability is the inherently complex and fragmented nature of healthcare IT infrastructure. The integration of electronic health records (EHRs), telehealth platforms, connected medical devices, and cloud services, while beneficial for patient care and operational efficiency, also creates an intricate network of systems that are difficult to secure comprehensively (Burrell et al., 2023). This complexity results in multiple security gaps that can be exploited by insiders who are familiar with the system's weakest points.

Furthermore, the lack of cybersecurity training among healthcare professionals exacerbates the problem. Many employees are unprepared to recognize common cyber threats such as phishing emails, making them prime targets for attackers who rely on social engineering techniques (Burrell et al., 2023). The high-pressure nature of healthcare settings compounds the issue. Under immense stress and time constraints, employees may prioritize immediate patient care over security protocols, often forgetting to log out of shared systems or mishandling sensitive information. These seemingly small lapses in judgment can have catastrophic consequences when exploited by malicious actors (Burrell et al., 2023). Third-party risks also present a unique vulnerability for healthcare organizations. With heavy reliance on external vendors for services like data storage, billing, and IT support, organizations must contend with the possibility that a vendor's inadequate security practices could serve as a backdoor for insider threats (Burrell et al., 2023).

1.2 Statement of the Problem

This commentary-style academic paper aims to reframe insider cybersecurity threats as organizational arsonists, bad actors who intentionally set metaphorical fires within digital ecosystems to achieve personal or ideological goals. Like traditional arsonists, these insider actors possess intimate knowledge of their target, enabling them to exploit organizational vulnerabilities precisely. Their actions have far-reaching consequences, triggering organizational chaos, financial loss, and severe legal repercussions. This paper employs the organizational arsonist analogy to offer a vivid framework for understanding insider threats' dual technical and human-centric dimensions. By integrating cybersecurity, law, risk management and organizational psychology perspectives, the paper highlights the necessity of comprehensive strategies that extend beyond technical defenses to include cultural, ethical, and legal considerations.

Commentary papers are crucial in academic discourse because they provide a platform for thought leadership, challenge established paradigms and propose innovative solutions. This paper adheres to that tradition by synthesizing existing research and practical insights into a cohesive narrative that advocates for strategic change. It aims to stimulate dialogue among cybersecurity professionals, legal scholars, and organizational leaders, encouraging them to rethink how insider threats are perceived and addressed. By focusing on the complex interplay between human behavior, legal accountability, and technological solutions, the paper calls for a more nuanced and holistic approach to addressing insider cybersecurity threats.

1.3 Importance of the Problem

Real-world examples illustrate the gravity of insider threats in healthcare and their far-reaching consequences. One recurring example involves employees stealing and selling patient information to third parties, often resulting in widespread identity theft and fraudulent billing schemes. In other cases, unintentional data breaches arise when employees mistakenly send confidential patient records to unauthorized recipients or fail to secure portable devices containing PHI, placing sensitive information at risk (Burrell et al., 2023). Equally troubling is the propagation of ransomware attacks due to phishing scams. In these incidents, an unsuspecting employee might click on a malicious link, inadvertently introducing ransomware into the organization's network. Such attacks can cripple entire healthcare systems, bringing operations to a halt and compromising critical patient care (Burrell et al., 2023).

The illegal nature of insider threats often lies in the intentional misuse of privileged access, which can include actions such as intellectual property theft, fraud, sabotage, and espionage (Burrell et al., 2022). Legal definitions classify insider activities as crimes under various statutes, including the Computer Fraud and Abuse Act (CFAA) and the Economic Espionage Act. These laws criminalize unauthorized access to systems, data theft, and the deliberate disruption of operations. Beyond criminal law, insider threats also raise significant concerns in civil liability, employment law, and compliance with data protection regulations such as the General Data Protection Regulation (GDPR). The ambiguity of intent in insider threat cases can further complicate the legal landscape, requiring forensic investigations and legal expertise to differentiate between criminal behavior and human error.

The legal dimensions of insider threats are vast and multifaceted. Insider threat actors engaging in intentional acts such as fraud, sabotage, or espionage face severe criminal penalties under domestic and international laws. In the United States, the CFAA remains one of the primary statutes used to prosecute malicious insiders. This act criminalizes unauthorized access to computer systems, particularly when such access results in theft or damage. For example, employees who exfiltrate sensitive company data or disrupt business operations through sabotage are subject to criminal charges and civil suits. The Economic Espionage Act also plays a critical role in prosecuting insider threats, particularly when intellectual property is stolen for the benefit of a foreign entity.

Employment law intersects with cybersecurity when addressing insider threats. Termination for cause is a common response to insider misconduct, but organizations must tread carefully to avoid wrongful termination lawsuits. In negligence cases, liability can extend to the employee and the organization. Organizations may face regulatory penalties if failing to implement adequate cybersecurity measures contributes to a data breach. The GDPR, for instance, imposes significant fines for failing to protect personal data, even when the breach results from an insider's actions. These regulations create a dual layer of responsibility, with legal ramifications affecting individual perpetrators and the organizations that employ them.

Addressing insider threats is one of the most challenging aspects of modern cybersecurity operations due to the multifaceted nature of the problem (Burrell et al., 2022). Unlike external threats, which can often be mitigated with technical controls, insider threats require a combination of technological solutions and human-centric approaches (Burrell et al., 2023). Organizations must develop robust internal controls while balancing security and employee trust. The complexity arises from the difficulty in detecting malicious insiders who may be well-versed in the organization's security protocols (Jones, 2024).

Monitoring employee behavior without infringing on privacy rights is another significant challenge. Privacy concerns and legal restrictions may limit how organizations monitor employee activities, particularly in jurisdictions with strong privacy protections. Striking the right balance between proactive monitoring and respect for employee rights requires careful consideration of legal and ethical factors. This complexity is compounded by the diversity of insider threat scenarios, ranging from malicious insiders to well-meaning but negligent employees (Burrell et al., 2023).

Human factors play a critical role in the emergence of insider threats. Stress, job dissatisfaction, financial pressures, and workplace grievances are common motivators for insider misconduct (Burrell et al., 2022). Organizations that fail to address these underlying issues may inadvertently create an environment conducive to insider threats (Nobles et al., 2022). Understanding insider behavior's psychological and social dimensions is essential for developing effective prevention and mitigation strategies (Nobles, 2018).

Intentional and illegal insider-driven data loss is the digital equivalent of organizational arson, deliberate acts of sabotage that drain financial resources, disrupt workflows, and compromise the resilience of cybersecurity teams. Like an arsonist firing to destroy physical property, insider actors exploit their privileged access to ignite chaos within digital systems. The financial toll is staggering, with insider incidents costing organizations an average of $15 million annually (Staff, 2024). Beyond this direct monetary impact, the relentless crisis management cycle consumes cybersecurity professionals, leaving little room for proactive planning. On average, cybersecurity teams spend three hours each day investigating and mitigating insider-driven incidents, draining resources that could otherwise be devoted to strengthening organizational defenses (Staff, 2024).

The psychological and emotional toll on cybersecurity leaders mirrors the anxiety of a fire chief battling an unpredictable series of blazes. According to recent research, 72% of cybersecurity leaders fear job loss if an insider breach goes uninvestigated (Staff, 2024). This fear is driven by the unpredictable nature of insider threats, which can arise without warning, leaving organizations vulnerable to cascading failures in data integrity and operational continuity. Consider the scenario of a trusted employee with legitimate access who intentionally exfiltrates sensitive data to a competitor. The resulting investigation consumes workdays, breeding distrust and unraveling organizational cohesion. These incidents are not merely technical challenges but full-scale organizational crises with lasting consequences. This convergence of financial, operational, and psychological pressures underscores the urgent need for innovative, holistic strategies to address insider threats, strategies that balance technological defenses with an understanding of human behavior and organizational culture (Jones, 2024).

1.4 Originality and Novelty of the Inquiry

The originality of this paper lies in its conceptualization of insider cybersecurity threats as organizational arsonists, a novel analogy that redefines the understanding of insider risk within the broader context of organizational security. Traditional discussions on insider threats often reduce them to isolated data incidents or technical vulnerabilities. This paper, by contrast, highlights the broader, systemic impact of these threats, emphasizing how insider actions can destabilize organizational structure, damage morale, and compromise operational stability. By framing insider threats as deliberate acts of digital arson, the paper provides a more relatable and impactful lens through which to assess the magnitude of insider risk.

This approach is particularly innovative in integrating diverse disciplines, linking technical cybersecurity measures with insights from legal frameworks, behavioral science, and organizational culture. The paper's focus on combining human-centric strategies with advanced technological solutions, such as artificial intelligence and behavioral analytics, positions it as a forward-thinking contribution to cybersecurity discourse. By bridging the gap between human behavior and technological defense, the paper offers a richer, more holistic understanding of insider threats. Ultimately, this interdisciplinary approach not only reframes the insider threat narrative but also proposes actionable solutions that address the psychological, ethical, and technological complexities of the problem, ensuring that organizations are better prepared to combat their organizational arsonists.

1.5 The Evolution and Complexity of Insider Threats

The concept of insider threats gained traction in the security lexicon during the 1990s when organizations were increasingly confronted with the paradox of granting employees access to sophisticated information technology systems while simultaneously striving to prevent those systems' misuse (Jones, 2024). Initially, insider threats seemed manageable, as most organizational networks were self-contained. However, the rapid proliferation of internet connectivity in the early 2000s shattered those boundaries, exponentially increasing the pathways through which individuals with privileged access could engage in destructive behavior (Jones, 2024). The potential for internal threats expanded in parallel with technological advances, transforming insider risk into a dynamic and complex issue.

Among the most haunting reminders of the danger posed by insiders was the case of Robert Hanssen, a trusted FBI agent who betrayed national security through espionage. His actions revealed a sobering truth: not all threats originate from external adversaries lurking in the shadows. Instead, they can arise from those within an organization’s inner circle, individuals entrusted with its most sensitive information (Jones, 2024). Such incidents forced a paradigm shift in legal and business frameworks, leading to the recognition of insider threats as a central component of organizational risk (Burrell et al., 2023).

1.6 The Rise of Behavioral Analytics

As insider threats became more deeply entrenched in the cybersecurity landscape, addressing them required a significant evolution in strategy (Burrell et al., 2023). Early efforts focused on strengthening technical defenses, firewalls, encryption protocols, and access control systems designed to prevent unauthorized entry. However, over time, it became clear that purely technical measures were insufficient for managing all cybersecurity risks (Nobles, 2022). Insider threats could no longer be addressed solely by safeguarding systems; they demanded understanding human behavior and motivation (Burrell et al., 2022).

This realization led to advanced monitoring techniques such as User and Entity Behavior Analytics (UEBA), which seek to detect deviations in user activity that may signal malicious intent (Khaliq et al., 2020). Real data are crucial to use in the identification and prevention of cyber malicious activities (Rich & Aiken, 2024).

For instance, imagine an employee who begins accessing sensitive files at odd hours or downloading large quantities of data without a clear business purpose. Traditional cybersecurity systems might overlook these actions, but behavior-based analytics can flag such anomalies as potential indicators of insider threats (Nobles, 2022). Additionally, the principle of least privilege, restricting employees’ access to only the information necessary for their roles, became a cornerstone of insider threat mitigation, reducing the attack surface available to malicious insiders while simultaneously curbing unintentional exposure to sensitive information.

1.7 Cybersecurity Leadership in the Age of Insider Risk

The role of cybersecurity leaders has evolved dramatically in response to the increasing complexity of insider threats. No longer confined to technical expertise, modern cybersecurity leadership requires a multidisciplinary approach that blends technological acumen with insights into human psychology, behavioral analysis, and organizational culture (Burrell et al., 2020; Burton, 2023). Leaders are now tasked with identifying potential insider threats by discerning behavior patterns and understanding motivational factors that could lead to malicious acts.

Motivational alignment plays a pivotal role in identifying and mitigating insider threats. Unlike external adversaries motivated by ideology or financial gain, insider threats often stem from personal grievances, disillusionment, or a desire for retribution against perceived injustices in the workplace (Burrell et al., 2022). Leaders who ignore these underlying motivators may find themselves blindsided by insider incidents that could have been prevented through early intervention. For example, a disengaged employee passed over for promotion may exhibit dissatisfaction, withdrawal from team activities, decreased productivity, and a growing sense of alienation. Without proactive engagement from leadership, such an employee may become vulnerable to malicious behavior that could compromise the organization's security.

1.8 Counterproductive Work Behaviors (CWBs)

The concept of Counterproductive Work Behaviors (CWBs), introduced by Spector and Fox (2002), highlights the spectrum of harmful actions that employees may engage in, whether unintentionally or with deliberate malice. CWBs encompass various behaviors that undermine an organization's and its members' well-being. These behaviors fall into three distinct categories: accidental, negligent, and malicious actions, each of which presents unique challenges for organizational cybersecurity. While some actions are born from ignorance or poor judgment, others arise from willful intent, creating significant risks to organizational integrity and security (Burrell et al., 2022).

Accidental insider behaviors often stem from employees' lack of knowledge regarding security protocols and best practices (Noble et al., 2022). Imagine a well-meaning employee unknowingly sending confidential data to an unauthorized recipient or uploading sensitive documents to an insecure cloud service. While the intent is not malicious, the consequences can be devastating, exposing the organization to data breaches, financial losses, and reputational damage. Negligence, on the other hand, represents a more troubling form of insider behavior, users who knowingly disregard established protocols but fail to act with malicious intent (Burrell et al., 2023). For example, an employee who routinely ignores password security policies, believing them unnecessary, unwittingly leaves the organization vulnerable to cyberattacks.

1.9 The Shadow Within

The most dangerous form of CWB is malicious behavior, where individuals deliberately act to harm the organization (Burrell et al., 2022). These actions are often driven by financial gain, personal vendettas, or espionage (Burrell et al., 2023). Consider the case of an employee who intentionally plants a virus within the company's network, causing catastrophic data loss and operational disruptions. Such acts are not just technical breaches but psychological assaults on the organization, breaking down trust and morale while costing millions in recovery efforts. Sabotage, in particular, stands out as a severe and often overlooked form of workplace violence. Spector and Fox (2002) describe sabotage as the deliberate infliction of harm on an organization intending to disrupt or damage its operations. This behavior can manifest in various forms, from deleting critical files to leaking sensitive information, each leaving a trail of chaos in its wake.

The impact of sabotage goes far beyond the immediate technical damage (Burrell et al., 2023). Imagine a scenario where an employee intentionally uploads a virus that corrupts the entire company's computer system. The organization must allocate substantial resources, purchase new hardware, reinstall software, and hire external consultants to rebuild its digital infrastructure. Meanwhile, productivity grinds to a halt, and clients lose confidence in the organization's ability to protect their data. In more extreme cases, sabotage can lead to legal repercussions if other employees or clients are adversely affected. For instance, an employee subjected to targeted sabotage might sue the organization for failing to protect their mental and emotional well-being.

1.10. Understanding Organizational Arsonist Metaphor

Arson has long been recognized as the deliberate act of setting property ablaze with the intent to destroy or cause damage (Miller, 2020). Traditionally associated with physical fire-setting, this concept has evolved in modern organizational contexts to describe a different kind of destructive behavior that thrives in the digital sphere. Carthy et al. (2024) differentiate arson from broader acts of fire-setting by reserving the term for intentional actions that lead to legal convictions.

Arsonists exhibit complex psychological profiles driven by a variety of motivations, such as anger, revenge, thrill-seeking, or a deep-seated need for control (Labree et al., 2010). Often, they may simply crave the chaos and power that comes with starting a fire. This convergence of psychological factors makes it difficult to predict or understand their actions, increasing the challenge for mental health professionals and law enforcement in identifying and managing this type of offender (Labree et al., 2010).

The danger posed by arsonists extends beyond physical destruction to encompass severe psychological and economic harm (Labree et al., 2010). Fires destroy lives, homes, and businesses, leaving victims with long-lasting trauma and financial devastation. The unpredictability of fire combined with the arsonist's often elusive nature compounds the risk, creating a heightened state of fear within communities. Beyond physical harm, the emotional toll, feelings of vulnerability, grief, and anger, deepens the trauma for those affected (Labree et al., 2010). This blend of psychological disturbance in the offender and widespread, often irreversible consequences makes arson a particularly insidious crime.

The archetype of the arsonist is steeped in history, with early societies chronicling acts of fire-setting as criminal and ritualistic (Mojtahedi et al., 2017). This ancient concept, once relegated to physical acts of destruction, has re-emerged in a digital age where computers have become critical components of organizational infrastructure (Jones, 2024). Starting in the 1970s, the increasing complexity of digital systems gave rise to new opportunities for insider threats. However, within the realm of cybersecurity, the term "organizational arsonist" has emerged to describe malicious insiders who, instead of using fire and accelerants, deploy digital tools and insider access to ignite metaphorical "fires" that disrupt operations and compromise sensitive information (Jones, 2024). Instead of physical flames, these modern arsonists wield malicious software, insider knowledge, and elevated access to sow organizational chaos and destruction (Jones, 2024). Their motivations are varied, ranging from financial incentives and ideological causes to personal grievances, and their impact can be just as catastrophic as traditional arson.

2. Discussion

2.1 Motivational Complexity and Behavioral Patterns

The complexity of modern organizational arson lies in its tools and methods and the diverse motivations driving insiders to commit these acts (Jones, 2024). Traditional criminological frameworks, such as Routine Activity Theory, offer valuable insights into understanding this behavior. According to Cohen and Felson (2010), a crime will likely occur when three conditions converge: a motivated offender, a suitable target, and the absence of capable guardians. In the context of insider threats, the "motivated offender" is the disgruntled employee or financially driven saboteur, the "suitable target" is the organization's sensitive data and digital infrastructure, and the "capable guardian" may be absent due to insufficient monitoring or weak access controls (Burrell et al., 2022).

For instance, imagine an employee passed over for a promotion who grows increasingly resentful. Over time, the individual gains access to a sensitive database and, motivated by feelings of injustice, deliberately alters or deletes critical records, leaving the organization scrambling to recover. In another scenario, a financially desperate insider might be lured into selling proprietary information to a competitor, causing irreparable harm to the organization's competitive advantage. These modern arsonists do not simply act on impulse; their behaviors are often deliberate and calculated, leveraging their deep understanding of organizational systems to inflict maximum damage while concealing their tracks (Jones, 2024).

2.2 Cybersecurity Strategies as Modern Firefighting

The challenge of countering organizational arsonists has led cybersecurity leaders to turn to interdisciplinary approaches, including criminology and behavioral science, for effective solutions. Routine Activity Theory provides a powerful framework for developing preventive measures by addressing the convergence of the motivated offender, the target, and the absence of capable guardians (Cohen & Felson, 2010). In adapting this theory to the digital realm, cybersecurity leaders have focused on two key elements: reducing motivation and enhancing guardianship.

One critical strategy is implementing stricter access controls and advanced monitoring systems to serve as capable guardians within the digital environment. Organizations can reduce the likelihood of insider incidents by limiting employees' access to only the data necessary for their roles (Burrell et al., 2023). Real-time monitoring and anomaly detection tools can flag suspicious behavior, such as unusual login patterns or attempts to access restricted files, allowing security teams to intervene before an incident escalates (Burrell et al., 2023). Such measures act as digital firewalls designed to smother emerging threats before they become full-blown crises.

However, technical defenses alone are insufficient for managing the full array of cybersecurity risks (Nobles, 2019). Addressing the human element is essential for reducing the risk of insider threats. Cybersecurity leaders increasingly adopt holistic approaches that align organizational security strategies with employee motivations (Espinoza, 2023). For example, creating a workplace culture that values transparency, open communication, and employee well-being can significantly reduce the feelings of disenfranchisement and discontent that often motivate insider threats (Burton et al., 2023). Programs that offer employees opportunities for growth, recognition, and involvement in security efforts foster a sense of shared responsibility for organizational well-being, transforming potential risks into collaborative strengths.

2.3 The Cost of Neglect

The failure to address insider threats, especially those driven by malicious intent, can have devastating consequences for organizations (Burrell et al., 2023). Modern organizational arson leaves a wide swath of destruction in its wake. Financial losses from compromised data and system outages are often accompanied by less tangible but equally damaging consequences, such as employee trust erosion and stakeholder confidence. Restoring the organization's reputation after an insider attack can take years (Jones, 2021), while the psychological impact on affected teams may linger long after the technical systems have been restored (Burrell et al., 2023).

For example, in a high-profile case, an insider with deep access to a company's network deliberately introduced malicious code that disabled key systems, forcing the organization to shut down operations for days. While the immediate financial losses were significant, the long-term damage was even more severe. Clients abandoned the company in droves, employees began leaving due to the toxic atmosphere of mistrust, and the brand's reputation never fully recovered. This incident served as a stark reminder that insider threats are not simply cybersecurity issues; they are organizational crises that require comprehensive risk management and human-centered solutions (Burrell et al., 2022; Nobles, 2019).

2.4 The Long-Term Costs of Sabotage and Neglect

Sabotage inflicts immediate financial and operational damage and leaves lasting scars on the organization's culture (Burrell et al., 2022). Restoring trust among employees after an insider incident is a formidable challenge. The psychological toll on teams can be significant; colleagues become wary of one another, and an atmosphere of suspicion pervades the workplace. This breakdown in trust undermines collaboration, innovation, and overall productivity. Additionally, leadership must devote considerable time and resources to rebuilding morale, often through team-building initiatives and counseling services, to restore the workplace culture to its former state.

The broader implications of CWBs make them a central concern for organizational leaders seeking to safeguard against insider threats. These behaviors blur the lines between cybersecurity and human resource management, necessitating a holistic approach that combines technological safeguards with robust employee engagement strategies (Burrell et al., 2022). Organizations that fail to address the root causes of these behaviors, such as workplace dissatisfaction, lack of recognition, or perceived injustices, may inadvertently create fertile ground for insider threats to flourish. Addressing CWBs, therefore, requires strong technical defenses and a keen understanding of employee behavior and workplace dynamics (Burrell et al., 2022).

2.5 The Overlooked Danger

Traditional security frameworks have long been designed to guard against external cyberattacks, leaving organizations vulnerable to a more insidious threat that emerges from within (Burrell et al., 2022; Burrell et al., 2023). Insider threats pose a unique and increasingly significant risk because they exploit trusted access and often go unnoticed until considerable damage has been done (Georgiadou, Mouzakitis, & Askounis, 2021). Unlike external attacks that break through security barriers, insider threats exist within these perimeters, making detection more difficult and the potential impact more devastating. The internal landscape of cybersecurity is not monolithic; insider threats manifest in various forms, from accidental negligence to calculated and malicious intent (Nobles, 2022).

Three primary categories of insider threats illustrate the complexity of this challenge. The malicious insider is a trusted individual who intentionally exploits their access for personal gain or to settle grievances, using insider knowledge of security protocols and weaknesses to execute their plan (Georgiadou, Mouzakitis, & Askounis, 2021). Consider an employee who decides to sell sensitive company data to a competitor after being passed over for promotion. In contrast, the careless insider poses an equally significant threat without malicious intent. Often serving as an unwitting agent of external actors. For instance, an employee might unknowingly click on a phishing link, inadvertently infecting the network with malware. Finally, the mole represents an even more alarming scenario. This individual is an outsider who infiltrates an organization, gaining insider access under pretenses with the explicit purpose of sabotage or data theft (Georgiadou, Mouzakitis, & Askounis, 2021). These varied insider threat profiles show how threats can arise in diverse and unpredictable ways, each demanding tailored detection and prevention strategies.

2.6 Behavioral and Digital Warning Signs

Identifying insider threats requires careful monitoring of both behavioral and digital patterns, as the indicators of malicious intent often emerge in subtle and fragmented ways. Behavioral indicators offer a window into potential insider threats' psychological state and motivations. Dissatisfied employees may resent coworkers, increasingly circumvent security policies, or isolate themselves from the team. These shifts in behavior, when paired with signs such as working irregular hours or openly discussing plans to resign, can signal deeper issues that warrant closer attention (Georgiadou, Mouzakitis, & Askounis, 2021; Gheyas & Abdallah, 2016).

Digital indicators, on the other hand, are often the earliest and most objective signs of insider threat activity. Sudden surges in network traffic, particularly at odd hours, can indicate an attempt to extract large amounts of data. Unauthorized access to sensitive resources and repeated requests for elevated permissions are clear red flags, especially when such access falls outside the scope of an employee's job responsibilities. Imagine an employee who begins signing into secure systems at 3 a.m. and transferring confidential documents to personal storage devices. This behavior is not simply an operational anomaly but a potential threat to the organization's data integrity and security (Georgiadou, Mouzakitis, & Askounis, 2021).

Modern insider threat detection systems rely on advanced real-time monitoring tools to analyze these behaviors and digital patterns. However, such systems must be balanced with an understanding of human context. Suspicious behavior may also result from legitimate business needs. Thus, effective monitoring is not about over-surveillance but about contextually informed vigilance.

3. Conclusion

3.1 Discussion

Given the multifaceted nature of insider threats in healthcare organizations, the implementation of a diversified detection strategy becomes paramount to ensuring patient safety and safeguarding sensitive data. Insider threat management in these settings must go beyond traditional security protocols and embrace a combination of behavioral monitoring, anomaly detection, and contextual analysis to accurately assess potential risks. For instance, when a hospital employee accesses electronic health records (EHRs) late at night without a clear business purpose, this may raise red flags. However, a comprehensive assessment should not rely solely on time-based activity. Cross-referencing this action with recent workplace events, such as grievances filed, disciplinary actions, or noticeable changes in behavior like increased absenteeism or uncharacteristic withdrawal, can offer a more nuanced perspective on whether the activity constitutes a true threat (Gheyas & Abdallah, 2016). This layered approach allows healthcare organizations to differentiate between harmless anomalies and genuine risks, ensuring that responses are both proportionate and evidence based.

Legal compliance and organizational transparency form the foundation of effective insider threat detection and response in healthcare environments. Security teams must be trained to recognize the fine line between legitimate business needs, such as medical staff accessing patient data for late-shift consultations, and activities that could indicate malicious intent. Missteps in these assessments can lead to breaches of employee trust or wrongful accusations, which could have serious legal and reputational consequences for the institution. Clearly defined response protocols, supported by collaboration with legal counsel, are essential to maintaining fairness and ensuring that investigations adhere to both internal policies and external regulatory standards. For instance, the Health Insurance Portability and Accountability Act (HIPAA) mandates strict protocols for handling patient data breaches. Ensuring that investigative processes align with HIPAA compliance requirements not only reduces liability but also protects patient privacy and employee rights. The goal is not merely to respond to insider threats once they have already inflicted damage but to foster a culture of accountability and security that dissuades potential insider misconduct before it begins (Burrell, 2023; Burrell et al., 2021; Burrell, 2024).

In healthcare, protecting critical assets, such as patient records, intellectual property from clinical research, and life-saving medical devices, requires far more than sophisticated technology or a set of written policies (Burrell, 2023; Burrell et al., 2021; Burrell, 2024). A successful strategy must be interdisciplinary, integrating technological innovation, legal frameworks, and human-centered approaches that prioritize both organizational security and employee well-being. For example, an advanced monitoring system that flags unusual data access patterns can be combined with regular staff training sessions on cybersecurity awareness and ethical data usage. Engaging employees in these efforts, rather than treating them as potential threats, fosters a supportive environment where security becomes a shared responsibility. Legal teams, IT security professionals, and human resources must work in tandem to build a system that not only deters harmful activity but also promotes a culture of trust and openness.

3.2 Ethical Challenges in Insider Threat Management

While detecting and mitigating insider threats is crucial, these efforts must be tempered by a firm commitment to ethics and employee rights. The most significant ethical challenge is balancing security with employee privacy and autonomy. If not handled transparently and responsibly, monitoring employee behavior and digital activity can easily cross the line into invasive surveillance. Excessive monitoring risks creating a toxic culture of suspicion, eroding trust, and morale among employees (Burrell et al., 2023). Transparency is essential in mitigating this risk; organizations must establish clear policies that define the scope and purpose of monitoring practices, ensuring employees understand how and why such measures are implemented.

Another ethical challenge arises in the investigation of potential insider threats. Accusations without sufficient evidence can damage an employee's career and reputation. Organizations must adhere to strict due process standards, ensuring investigations are thorough, fair, and impartial. For cases of negligence, adopting a punitive approach is rarely effective. Instead, organizations should focus on education, training, and process improvements to prevent future incidents (Burrell et al., 2023). For example, an employee who inadvertently introduces malware into the system should be given additional training and support rather than immediate disciplinary action.

Building an ethical framework for insider threat management requires collaboration between legal, human resources, and cybersecurity professionals. It demands policies grounded in fairness and respect for employee rights while maintaining organizational security. This ethical approach mitigates insider risk and fosters a work environment where employees feel valued and respected, making them less likely to become insider threats in the first place.

3.3 Combating Organizational Arsonists

The complexity of insider threats requires organizations to approach them as acts of organizational arson, intentional actions aimed at igniting chaos, disrupting operations, and eroding trust within digital ecosystems. Cybersecurity leaders must serve as both detectives and architects to counteract these threats (Nobles, 2022). Like fire investigators who examine the cause of a blaze, they must identify potential arsonists within the organization while simultaneously constructing a resilient culture that deters such destructive behavior. Programs focused on improving employee well-being and engagement can act as "fire prevention systems," reducing the emotional fuel that often motivates malicious insiders.

Routine cybersecurity training is akin to conducting regular fire drills. Employees must have the knowledge and tools necessary to recognize potential hazards and prevent careless acts that can spark organizational fires. Advanced behavioral analytics and anomaly detection systems serve as modern "fire alarms," alerting cybersecurity teams to early warning signs without infringing on employee privacy (Cohen & Felson, 2010). Organizations can establish a comprehensive defense by combining technological vigilance with ethical oversight and human-centered policies. This approach, grounded in prevention, education, and transparency, protects sensitive data and strengthens the organization's culture and resilience against future arsonist-like attacks.

3.4 Preventing the Organizational Blaze

Protecting critical organizational assets, whether physical infrastructure, proprietary technology, or intellectual property, has become increasingly complex in an era where insider threats act as organizational arsonists. These digital arsonists know precisely which assets are most vulnerable and can strike with precision, leaving organizations scrambling to contain the damage. Assets such as customer databases, internal schematics, and proprietary software are prime targets. The failure to prioritize and protect these assets exposes organizations to operational and legal risks, creating fertile ground for insider sabotage (Georgiadou, Mouzakitis, & Askounis, 2021; Gheyas & Abdallah, 2016).

Intellectual property (IP) theft represents one of the most destructive forms of insider arson. Unauthorized disclosure of trade secrets, intentional or accidental, can lead to costly legal battles under statutes such as the Defend Trade Secrets Act (DTSA). For example, an employee with access to proprietary algorithms might leak them to a competitor for financial gain, sparking a firestorm of legal consequences. In severe cases, these incidents escalate to criminal prosecution if the theft involves foreign entities. Thus, organizations must establish enforceable security policies and educate employees on the legal ramifications of IP misuse.

3.5 Constructing Firewalls Against Insider Arson

Preventing insider sabotage is not merely a governance issue but a critical legal obligation for organizations. Just as municipalities enforce strict fire codes to prevent devastating blazes, organizations must develop and publicize robust policies that clearly define the consequences of insider misconduct. These policies must go beyond mere symbolism. They must be consistently enforced and embedded within the corporate culture. Some organizations, for instance, include provisions in employee handbooks that allow for inspecting company property if sabotage is suspected. While these measures can deter malicious behavior, they must be implemented with respect for employee privacy and legal standards to avoid exposing the organization to wrongful termination lawsuits or discrimination claims.

A written policy alone is not enough. A culture of open communication and fair employee relations is essential to extinguishing potential fires before they ignite. Employees who feel ignored or mistreated may resort to retaliatory behavior, whereas those who feel heard and valued are far less likely to engage in sabotage. Employee assistance programs and regular feedback opportunities can help organizations identify and address grievances early. By proactively managing employee concerns, organizations can reduce the risk of insider-driven arsonist behavior.

3.6 Insider Threat Detection: Monitoring the Flames

Detecting insider threats is akin to identifying an arsonist (Jones, 2024) who has entered the building. Traditional security measures such as firewalls and intrusion detection systems are designed to stop external attackers, not insiders with authorized access. Malicious insiders who exploit authorized logins can evade these traditional security mechanisms, making real-time behavioral monitoring essential (Georgiadou et al., 2021). However, this monitoring introduces legal and ethical challenges, especially when balancing security with employee privacy.

Organizations must implement transparent monitoring practices that clearly define their scope and purpose. Deception technology, for example, can act as a "controlled burn," creating decoy systems to lure malicious insiders and observe their activities without invading legitimate workspaces (Gheyas & Abdallah, 2016). Legal compliance is paramount in this process, particularly under regulations like the General Data Protection Regulation (GDPR). Organizations must ensure that these regulations handle any data collected and that disciplinary actions are based on objective evidence and due process.

3.7 Safeguarding Critical Healthcare Assets

Ultimately, the path to safeguarding critical healthcare assets lies in the seamless alignment of security practices, regulatory compliance, and proactive employee engagement initiatives (Burrell, 2023; Burrell et al., 2021; Burrell, 2024). This alignment reduces the likelihood of insider threats while enhancing overall organizational resilience. Much like a hospital's infection control program aims to prevent outbreaks rather than merely treat infections, insider threat management must focus on early intervention and prevention. By fostering a secure environment where employees are empowered to act responsibly and security systems are robust and fair, healthcare organizations can protect both their people and their mission. Security and legal accountability must work hand in hand to prevent the metaphorical fires of insider threats from igniting, creating a safer and more resilient healthcare landscape for all.

Table 1. Laura Jones and Darrell Norman Burrell Cybersecurity Insider Threat Organizational Arsonist Prevention Framework

Organizational Actions	Framework Component	Description
1	Develop and Implement a Comprehensive Insider Threat Policy	Organizations must establish a formal, written insider threat policy that clearly defines insider threats, the legal consequences of engaging in such behavior, and the organization's expectations for employee conduct. This policy should be grounded in respect for fairness, transparency, and due process. The document must be reviewed and updated regularly to align with evolving legal standards and technological advancements.
2	Foster a Security-Conscious Organizational Culture	Leadership must prioritize cultivating an organizational culture that values security awareness, open communication, and ethical responsibility. Building trust and maintaining transparency is key to ensuring employees feel engaged and invested in protecting organizational assets.
3	Enhance Leadership Engagement and Non-Technical Training	Non-technical leaders play a crucial role in mitigating insider threats by modeling ethical behavior, promoting fairness, and understanding the broader implications of cybersecurity policies.
4	Invest in Continuous Employee Education and Awareness Programs	Employee education is the cornerstone of a successful insider threat prevention strategy. Organizations should offer regular training programs on cybersecurity best practices, intellectual property protection, and the legal consequences of insider threats.
5	Adopt Advanced Technological Solutions with an Emphasis on Fairness and Privacy	Organizations should deploy advanced insider threat detection systems that combine behavioral analytics, anomaly detection, and data correlation from multiple sources.
6	Integrate Insider Threat Detection with Broader Risk Management Processes	Insider threat detection should be part of the organization’s overall risk management strategy rather than an isolated initiative.
7	Develop Leadership Accountability Structures	Hold senior leaders accountable for promoting ethical conduct and maintaining organizational security.
8	Create Multidisciplinary Insider Threat Response Teams	Insider threat management requires a collaborative approach involving security professionals, legal counsel, human resources, and senior leadership.
9	Prioritize Psychological Safety and Employee Well-being	Employee dissatisfaction and workplace grievances are common precursors to insider threats.
10	Establish Clear Legal and Ethical Boundaries for Investigation and Monitoring	Organizations must ensure that insider threat investigations are conducted with full respect for employee rights and privacy.
11	Deploy AI-Driven Threat Detection Systems	Organizations should adopt advanced AI-based tools that monitor user behavior, detect anomalies, and flag potential insider threats in real-time.
12	Integrate AI into Risk Management Frameworks	AI should be incorporated into the organization's broader risk management strategy to continuously assess insider threats.
13	Automate Threat Response Protocols	AI can streamline and automate incident response processes, reducing the time it takes to contain insider threats.
14	Use AI for Behavioral Risk Analysis and Early Warning Systems	AI can be leveraged to analyze employee behavioral patterns and provide early warnings of potential risks.
15	Enhance Stakeholder Communication with	AI-powered dashboards can provide real-time insights

	AI-Driven Dashboards	into insider threat metrics, helping stakeholders understand the organization’s security posture.
16	Apply AI to Incident Forensics and Post-Incident Analysis	After a security incident, AI can assist in forensic investigations by rapidly analyzing logs and correlating data across systems.
17	Integrate AI with Identity and Access Management (IAM)	AI can enhance IAM systems by continuously monitoring and adjusting user access based on contextual factors such as job role, location, and recent behavior.
18	Leverage AI for Predictive Stakeholder Engagement	AI can help organizations anticipate stakeholder concerns and develop proactive communication strategies.
19	Establish AI Governance and Ethical Frameworks for Insider Threat Management	AI governance is critical to ensuring that AI-based tools are used responsibly and comply with legal and ethical standards.

References

Burrell, D. N. (2023). Cybersecurity in healthcare through the 7-S model strategy. *Scientific Bulletin, 28*(1), 26-35.

Burrell, D. N. (2024). Understanding healthcare cybersecurity risk management complexity. *Land Forces Academy Review, 29*(1), 38-49. https://doi.org/10.1108/ijse11-2022-0719

Burrell, D. N., Aridi, A. S., McLester, Q., Shufutinsky, A., Nobles, C., Dawson, M., & Muller, S. R. (2021). Exploring system thinking leadership approaches to the healthcare cybersecurity environment. *International Journal of Extreme Automation and Connectivity in Healthcare (IJEACH), 3*(2), 20-32.

Burrell, D. N., Courtney-Dattola, A., Burton, S. L., Nobles, C., Springs, D., & Dawson, M. E. (2020). Improving the quality of "The Internet of Things" instruction in technology management, cybersecurity, and computer science. *International Journal of Information and Communication Technology Education (IJICTE), 16*(2), 59-70.

Burrell, D. N., Nobles, C., Cusak, A., Jones, L. A., Wright, J. B., Mingo, H. C., & Richardson, K. (2023). Cybersecurity and cyberbiosecurity insider threat risk management. In *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems* (pp. 121-136). IGI Global.

Burrell, D. N., Nobles, C., Cusak, A., Omar, M., & Gillesania, L. (2022). Cybercrime and the nature of insider threat complexities in healthcare and biotechnology engineering organizations. *Journal of Crime and Criminal Behavior, 2*(2), 131-144.

Burton, S. L. (2023). Cybersecurity risk: The business significance of ongoing tracking. In *Transformational Interventions for Business, Technology, and Healthcare* (pp. 245-268). IGI Global.

Burton, S. L., Burrell, D. N., & Nobles, C. (2023). Adapting to the cyber-driven workforce: A battle for the discouraged worker. In *Real-World Solutions for Diversity, Strategic Change, and Organizational Development: Perspectives in Healthcare, Education, Business, and Technology* (pp. 130-152). IGI Global.

Burton, S. L., Burrell, D. N., Nobles, C., Jones, L. A., White, Y. W., Bessette, D. I., & Aridi, A. (2024). Cyber leadership excellence: Bridging knowledge gaps, maximizing returns. In *Evolution of Cross-Sector Cyber Intelligent Markets* (pp. 184-199). IGI Global.

Cohen, L. E., & Felson, M. (2010). Social change and crime rate trends: A routine activity approach (1979). In *Classics in environmental criminology* (pp. 203-232). Routledge.

Espinoza, M. D. (2023). Cybercrime and insider threats in healthcare organizations: Motive, prevention, and mitigation. In *Transformational Interventions for Business, Technology, and Healthcare* (pp. 1-15). IGI Global.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Detecting insider threat via a cybersecurity culture framework. *Journal of Computer Information Systems, 62*(4), 706-716. https://doi.org/10.1080/08874417.2021.1903367

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Analytics, 1*(1), 1-29. https://bdataanalytics.biomedcentral.com/articles/10.1186/s41044-016-0006-0

Jones, L. A. (2021). A content analysis review of literature to create a usable framework for reputation risk management. *Handbook of Research on Multidisciplinary Perspectives on Managerial and Leadership Psychology*, 91-133.

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), 43-63. https://doi.org/10.61093/sec.8(2).44-63.2024

Jones, L. A., Burrell, D. N., Nobles, C., Richardson, K., Hines, A., Kemp, R., Mingo, H. C., Ferreras-Perez, J., & Khanta, K. (2023). Real estate cybersecurity, adaptive management strategy, and risk management in the age of COVID-19. In *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems* (pp. 305-324). IGI Global.

Khaliq, S., Tariq, Z. U. A., & Masood, A. (2020). Role of user and entity behavior analytics in detecting insider attacks. In *2020 International Conference on Cyber Warfare and Security (ICCWS)* (pp. 1-6). IEEE.

Labree, W., Nijman, H., Van Marle, H., & Rassin, E. (2010). Backgrounds and characteristics of arsonists. *International Journal of Law and Psychiatry, 33*(3), 149-153.

Lewis, E., Burrell, D. N., Nobles, C., Ferreras-Perez, J., Richardson, K., Jones, A. J., & Jones, L. A. (2023). Cybercrime and cybersecurity challenges in the automotive industry utilizing agent-based modeling (ABM). In *Transformational Interventions for Business, Technology, and Healthcare* (pp. 134-159). IGI Global.

Mojtahedi, D., Prince, R. J., & Ryan, S. (2017). Making an arsonist: A psychological approach to understanding expressive arson. *EC Psychology and Psychiatry, 4*(3), 94-99.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration, 9*(3), 71-88.

Nobles, C. (2019). Establishing human factors programs to mitigate blind spots in cybersecurity. *MWAIS 2019 Proceedings*, 22.

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–Journal of Business and Public Administration, 13*(1), 49-72.

Nobles, C., Robinson, N., Cunningham, M., Robinson, N., Cunningham, M., & Cunningham, M. (2022). Straight from the human factors professionals' mouth: The need to teach human factors in cybersecurity. In *Proceedings of the 23rd Annual Conference on Information Technology Education* (pp. 157-158).

Rich, M. S., & Aiken, M. P. (2024). An interdisciplinary approach to enhancing cyber threat prediction utilizing forensic cyberpsychology and digital forensics. *Forensic Sciences, 4*(1), 110-151.

Staff, S. (2024, March 6). Insider-driven data loss incidents cost an average of $15 million. Retrieved from: https://www.securitymagazine.com/articles/100483-insider-driven-data-loss-incidents-cost-an-average-of-15-million

Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. *Health Economics and Management Review, 4*(4), 17-27. https://doi.org/10.61093/hem.2023.4-02.

Copyrights