Issues in Information Systems
Volume 26, Issue 1, pp. 94-109, 2025

DOI: https://doi.org/10.48009/1_iis_108

Financial insider threats: a cybersecurity STRIDE analysis

Chelsea Jane Idensohn, *The University of Tulsa, chelsea-idensohn@utulsa.edu*
Stephen Flowerday, *The University of Tulsa, stephen-flowerday@utulsa.edu*

Abstract

Insider threats pose significant cybersecurity risks, particularly in the financial sector, where privileged access can be exploited for fraud. This study applies the STRIDE threat model to analyze insider threats within a financial institution, using the real-world embezzlement case of Megan Lea Dougherty at the Exchange Bank of Missouri. The research identifies key technical vulnerabilities, including weak access controls and insufficient monitoring, facilitating fraudulent activities. By integrating the STRIDE framework with behavioral insights from the Fraud Triangle, the study demonstrates how systemic weaknesses and individual motivations intersect to enable insider threats. The findings emphasize the importance of addressing technical and human factors in financial cybersecurity, offering a structured approach to insider threat mitigation. Organizations can leverage this dual framework to enhance fraud detection, strengthen internal controls, and reduce the risk of insiders' financial exploitation. This research contributes to cybersecurity threat modeling by illustrating how STRIDE can effectively apply to financial insider threats, bridging the gap between technical security measures and behavioral risk analysis.

Keywords: insider threats, cybersecurity, STRIDE, fraud triangle, financial fraud, banking sector

Introduction

Insider threats are among the most critical issues organizations face in information security. Insider threat behavior originates from authorized users, such as employees, business partners, and contractors, who intentionally or accidentally use their legitimate access to conduct unethical actions and fraudulent behavior within organizations (NIST, 2024). While external threats are more frequent and often dominate cyberattack headlines, insider threats, whether due to malice or negligence, can pose more significant risks and incur higher costs (IBM, 2024). Verizon's Data Breach report found that external attacks accounted for approximately 200 million compromised records, while insider breaches accounted for over 1 billion exposed records (Verizon, 2023).

The 2024 *IBM Cost of a Data Breach Report* found that the global average data breach cost per individual data breach spiked by 10% in one year, totaling USD 4.99 million, making it the most significant leap since the pandemic (IBM, 2024). Malicious insider attacks were the costliest among all. Insiders pose a significant risk to organizations because they have access to sensitive data and systems. Their elevated privileges, coupled with the legitimate nature of their activities, allow them to retrieve sensitive information without raising suspicion, making these threats particularly difficult to detect and mitigate (CISA, 2024). Code42's Annual Data Exposure Report found that since 2021, there has been a 28% increase in the average number of monthly incidents involving insider-driven data exposure, loss, leakage, and theft (Code42, 2024). Alarmingly, 85% of cybersecurity leaders anticipate a rise in data loss from insider events in the next 12 months (Code42, 2024). Year after year, insider threats in organizations continue to rise, making it crucial for organizations to consider the human element of cybersecurity when implementing threat detection mechanisms. The Verizon 2023 Data Breach Investigation Report attained that 74% of all breaches comprised of a human element involving privilege misuse, use of stolen credentials, social engineering, or error (Verizon, 2023).

When examining data breach costs by industry, the financial sector ranked second, with an average breach cost of USD 6.08 million (IBM, 2024). Data is the core of most industries. In a survey conducted by Code42, cybersecurity respondents identified accounting and financial data as the most valuable (Code42, 2024). This paper's case study demonstrates the significant concern that insider threats pose to organizations, especially in the financial sector, where employees are granted access to sensitive information and critical systems.

Originally developed at Microsoft, the STRIDE model is a structured framework that identifies six categories of security threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, and is commonly used in threat modeling to systematically identify and mitigate potential security risks during system design or analysis (Shostack, 2014). This paper applies the STRIDE threat model and the Fraud Triangle to a real-world case study in the banking sector, involving the embezzlement scheme carried out by Megan Dougherty, an employee of the Exchange Bank of Missouri. The case highlights how insider access and internal vulnerabilities were exploited over a 15-year period. By analyzing the incident through technical and behavioral lenses, the study proposes targeted mitigation strategies to strengthen insider threat detection and response within financial institutions.

The novel contribution lies in applying the STRIDE threat model and the Fraud Triangle to a real-world case of an insider threat. STRIDE is conventionally used for modeling external cybersecurity threats (Shostack, 2014), while the Fraud Triangle is employed in behavioral analyses of fraud (Cressey, 1953; Jiang, 2022). Prior work typically applies these models independently; however, by integrating them, this paper offers a dual-perspective framework that links technical vulnerabilities with the behavioral and situational enablers of insider threats. This approach advances insider threat analysis by demonstrating how layered modeling can uncover risks that may be overlooked when technical or behavioral factors are considered in isolation.

Literature Review

Insider Threats

Scholarly discourse on insider threats highlights their evolving nature and challenges they pose to information security management. Bishop and Gates (2008) explore the complexities of identifying insider behavior, emphasizing the blurred lines between legitimate access and malicious intent. CISA (2024) addresses emerging trends, noting how technological shifts and remote work arrangements have broadened the scope of insider vulnerabilities. Meanwhile, NIST (2024) underscores the importance of integrating technical controls with behavioral monitoring, as many insider incidents stem from human factors rather than technical flaws.

Malicious insiders deliberately exploit their knowledge and access to bypass security controls, posing a greater risk than external attackers (Bellovin, 2008; Willison & Warkentin, 2013). Their actions, such as fraud, espionage, and intellectual property theft, can lead to financial loss, reputational damage, and long-term organizational harm (CISA, 2024; Hunker & Probst, 2011). Once rogue, insiders can evade detection, making mitigation complex (Bellovin, 2008; Glancy et al., 2020).

Insider Threats in the Financial Sector

In the financial sector, insiders can cause breaches that significantly undermine customer trust and result in substantial financial losses, making it essential to address these threats proactively. Table 1 presents examples from SentinelOne (2019) highlighting high-profile insider cases from major financial institutions. CISA (2024) highlights that 90% of cybersecurity professionals believe their organizations are vulnerable to insider threats, a concerning statistic for security teams striving to safeguard their environments from internal and external risks. The financial sector is prone to falling prey to the wrath of malicious insider threats. Insider threats are said to be the underlying cause of almost every high-profile banking breach, with the common factor being unauthorized access to systems, which grants attackers free movement within the compromised environment or system (Pisani, 2023).

Banks are vulnerable to cyberattacks due to the rapid adoption of digital technology that offers customers convenience and accessibility while inadvertently introducing more vulnerabilities and opportunities for attackers to manipulate the system. Adopting cloud technology introduces potential risks for banks, mainly if security measures are not adequately implemented. The rise of remote and hybrid work environments expands the playing field by increasing the likelihood of breaches. Such a shift leads to the heightened use of personal devices, which often lack adequate security protections. Traditional cybersecurity solutions often fail to address the rapidly evolving nature of modern threats. In addition, response rates to these ongoing attacks are unreliable and inconsistent due to understaffed security teams (Pisani, 2023).

Table 1. High-Profile Insider Cases from Major Financial Institutions

Institution	Role of Insider	Type of Insider Threat	Case Description
JP Morgan Chase	Banker	Data Theft	Peter Persaud sold customer PII and PINs to informants and others for monetary gain.
JP Morgan Chase	Investment Advisor	Fraud and Embezzlement	Michael Oppenheim stole $20M from clients, fabricating account statements and transferring funds between accounts.
JP Morgan Chase	Banker	ATM Fraud	Dion Allison exploited elderly and deceased client accounts, issuing ATM cards and stealing $400,000.
JP Morgan Chase	Derivatives Traders	Misconduct in Trading	'The London Whale' traders Javier Martin-Artajo and Julien Grout were charged with fraud and conspiracy after concealing $6.2 billion in losses from risky derivatives trades through false records and SEC filings.
Morgan Stanley	Financial Advisor	Data Breach	Galen Marsh accessed and downloaded $730,000 worth of customer data, which hackers later stole from his home server.

Institution	Role of Insider	Type of Insider Threat	Case Description
Wells Fargo	Branch Employees and Managers	Fraudulent Account Creation	Employees created nearly 2 million unauthorized accounts to meet sales targets, leading to $3 billion in fines and lawsuits.
Punjab National Bank	Deputy Manager	Fraudulent SWIFT Transactions	Gokulnath Shetty issued unauthorized Letters of Undertaking, enabling the fraudulent transfer of $43M.

Threat Modelling

Threat modeling is a structured approach to identifying, analyzing, and prioritizing potential threats to systems, data, or environments. This process provides insights into the attack surface, highlights vulnerabilities, and assesses the impact and likelihood of various scenarios. Organizations can use threat modeling to create and implement security measures aligned explicitly with their unique needs and objectives (Shostack, 2014).

Shostack's (2014) work on threat modeling includes applications to various threats, including insider threats, where the importance of tailored threat models is emphasized to understand insider access and behavior. As previously discussed, insider threats differ from external threats in several key ways, such as having legitimate access to resources, possessing knowledge of policies and procedures, and seamlessly blending in with regular activities. These leverage the established trust and relationships. Such characteristics make insider threats more challenging to detect, prevent, and respond to effectively (Cappelli et al., 2012).

As such, threat modeling is essential in pinpointing potential sources, motives, and techniques associated with insider threats, evaluating potential impacts, and designing appropriate countermeasures (Cappelli et al., 2012). Various frameworks and tools are employed in threat modeling, including STRIDE, PASTA, OCTAVE, and DREAD, each involving defining the scope and boundaries of the data, system, or environment targeted to protect from insider threats (Shostack, 2014). Threat modeling maps out the threats and vulnerabilities exposed to insiders by identifying assets and processes. It enables analysis based on impact, methods, motives, sources, vulnerabilities, and likelihood. This approach aids organizations in defining the security controls that can mitigate or reduce threats, such as access control, encryption, monitoring, auditing, training, or awareness programs (Cappelli et al., 2012).

Fraud Triangle: Behavioral Aspects of Insider Fraud

Insider threat agents will make rational decisions influenced by opportunities, work situations, and personal factors (Wang et al., 2015). Insiders are posited to have a motive/intention to attack, to identify an opportunity or target, and then possess the capability to launch their attack. The vital personal factors in understanding computer security crimes are skills, knowledge, resources, authority, and motives used in malicious acts. It is proposed that specific behavioral indicators reveal an insider's inclination towards these malicious actions, which organizations' security departments should closely monitor. These indicators include abnormal behaviors, correlated usage patterns, and specific personality traits (Wang et al., 2015).

Criminology theories offer valuable frameworks for understanding the behaviors and motivations of computer criminals, enabling the development of more effective prevention and intervention strategies for insider threats. The Fraud triangle is a widely accepted framework for understanding behavioral aspects of Fraud. Conceptualized in 1953 by criminologist Donald Cressey, the Fraud Triangle outlines three factors:

pressures or incentives, opportunities, and justifications or rationalizations that, when all present, increase the likelihood of fraudulent behavior (Cressey, 1953).

Theoretical Framework

The STRIDE Model

The STRIDE threat model effectively shifts the focus from external attackers to insider threat actors (Shostack, 2014). The model outlines insider advantages and examines how authorized access and knowledge can exploit vulnerabilities such as data access and tampering. The Spoofing, Tampering, Repudiation, Information Disclosure, Denial-of-Service, and Elevation of Privilege framework effectively analyzes how insiders may exploit weaknesses (Cappelli et al., 2012). Breaking down the elements of the STRIDE model:

- **Spoofing** occurs when an attacker impersonates a system component to deceive other entities into believing they are legitimate, undermining the system's authentication objectives (Rouland et al., 2021).
- **Tampering** refers to the unauthorized modification of data. These threats violate the integrity of a system's objectives and often target data during transmission, altering information in transit (Rouland et al., 2021).
- **Repudiation** threats arise when a system component denies actions it has executed, typically due to insufficient system auditing and accountability. Mitigating these threats requires the ability to distinguish legitimate actions from false claims. This is often accomplished through audit logs that document system operations and the involved components (Rouland et al., 2021).
- **Information Disclosure** is the exposure of information to unauthorized individuals, occurring when an unintended component gains unauthorized access to information, thereby breaching the confidentiality objectives of a system (Rouland et al., 2021).
- **Denial-of-service** threats involve unauthorized disruption or withholding of services from the system components, denying or degrading service to users, and undermining the system's availability objectives (Rouland et al., 2021).
- **Elevation of Privilege** occurs when an attacker gains unauthorized capabilities within the system and breaches authorization controls. This threat arises when an attacker manipulates vulnerabilities within the access control policy to perform restricted actions. Mitigating this threat involves rigorous policy enforcement through strict access controls and verification that block an attacker from unauthorized actions, ensuring that permissions are continuously monitored (Rouland et al., 2021).

Threat modeling for insider threats has several advantages, such as enhancing security posture and resilience to insider attacks. Exposure to risks is reduced while regulation compliance is enhanced. In addition, awareness of potential threats improves, further supporting security investment decision-making. Overall, this provides a quantifiable reduction in liabilities associated with insider risks (Cappelli et al., 2012).

The Fraud Triangle

The Fraud triangle was initially developed to identify fraudsters in accounting and has since evolved into a versatile framework applied across various disciplines, including cybersecurity (Jiang, 2022). It theorizes that fraud arises from three factors: the motivation to act fraudulently, the opportunity to carry it out, and the mindset to rationalize it (Cressey, 1953). Breaking down the three key elements of the Fraud Triangle:

- **Pressure** represents the motivation or incentive that drives an individual to commit fraud. This can be workplace pressures to meet targets, financial stress, personal debts, or unrealistic performance expectations (Dorminey et al., 2012).
- **Opportunity** refers to an individual's ability to commit fraud due to gaps in an organization's security measures, such as a lack of oversight (Jiang, 2022). Individuals are more likely to act on their pressure or rationalization if they perceive that they can commit fraud without getting caught (Homer, 2020).
- **Rationalization** is the cognitive process by which individuals justify their fraudulent actions to themselves (Cressey, 1953). They may convince themselves that they deserve the money or that their actions are not wrong (Dorminey et al., 2012).

The American Institute of Certified Public Accountants (AICPA) has adopted the concept that the magnitude of pressure will affect the rationalization of fraudulent behavior (Anindya & Adhariani, 2019). The Fraud Triangle can be applied as a causal model that highlights the progression of moral awareness to ethical decision-making (Jiang, 2022). This enriches the understanding of the psychological underpinnings of fraudulent behavior. The comprehensive approach of the Fraud Triangle incorporates the individual and organizational factors from an employee's perspective to gauge the influences of committing fraud (Jiang, 2022) or, in this case, embezzlement. Applying the Fraud Triangle to insider threats allows us to understand the pressures that motivate their malicious activity. The opportunity factor explains the vulnerabilities within an organization that insiders exploit without being detected and how these fraudulent individuals rationalize their behavior.

Case Background

Like most financial institutions, the Exchange Bank of Missouri employs standard cybersecurity and fraud prevention measures, including access controls, intrusion detection, encryption, and multi-factor authentication (MFA). Despite these controls, the embezzlement in this case remained undetected for 15 years. This case underscores how even established security measures can fail in identifying and preventing insider threats.

On Thursday, 25th July 2024, a former Exchange Bank of Missouri employee pleaded guilty to a $2.4 million embezzlement scheme (U.S. Department of Justice, 2024). Dougherty began working in the Fayetteville branch in 2008 as the Bank's IT and service department and strategically conducted a 15-year embezzlement scheme. Her insider knowledge enabled her to become familiar with the bank's internal systems, allowing her to detect and exploit gaps within the internal controls. She initially began with small amounts of money being transferred directly from customer accounts into her personal savings account and subsequently into her checking account. She then expanded her scheme to depositing the stolen funds into her family members' accounts.

As her confidence increased, Dougherty shifted her target to the wealthier client holders of Certificate of Deposit (CD) accounts. These accounts have significant balances and are less frequently monitored by the account holders. Dougherty concealed her malicious activity through account rotation, from which she stole funds. She avoided detection by manipulating transaction descriptions within the bank's computer systems, making them appear legitimate transfers. At this point, Dougherty also began "kiting," stealing funds from one account to reimburse another to obscure her fraudulent activities further (U.S. Department of Justice, 2024).

Dougherty's concealment tactics of rotating accounts she stole from allowed her to steal from seven bank clients, some of whom had multiple accounts. At the time of discovery, records revealed that she had victimized over a dozen clients but had tactically reimbursed their accounts when moving on to new targets. Dougherty admitted that many of the victims knew her personally, placing their trust in her and, therefore, making the betrayal particularly impactful. Her malicious scheme was only revealed in October 2023 when discrepancies were found during a routine audit of the bank's accounts. Upon further investigation, it was found that Dougherty had been manipulating account records and transferring funds without authorization. Upon arrest, she cooperated with investigators, admitting to committing fraud and providing detailed information about her methods and motivations. As part of her plea agreement, Dougherty had to pay back all money owing to the Exchange Bank of Missouri's clients and forfeit the nine real estate parcels she and her husband had purchased since the scheme. She faces a 30-year sentence in federal prison without parole (U.S. Department of Justice, 2024).

The incident revealed that Dougherty's IT and customer service role gave her the insider knowledge needed to gain unauthorized access to sensitive client information and the bank's transaction processing system. The bank's inadequate internal controls and lack of robust oversight allowed both the low-tech and sophisticated exploitation methods of these systems to go undetected for years.

The critical weaknesses of the bank that this case brought to light were the fragile internal controls, particularly in monitoring employee activities and securing transaction processes. It highlights the need for comprehensive employee training on detecting and preventing internal fraud. The case also directly aligns with the theory of insiders being uniquely positioned to exploit the trust placed in them by their organizations, making their actions challenging to detect and prevent (Cappelli et al., 2012).

Findings and Discussion

STRIDE Analysis (Technical Vulnerabilities)

To thoroughly address the security vulnerabilities exposed by the Exchange Bank of Missouri insider threat incident, the STRIDE model was applied to categorize the specific threats exploited by the insider in this case and to identify other potential threats commonly associated with banking systems. Tables 2–7 correspond to each STRIDE category and present observed and hypothetical threats, concise descriptions, and mitigation strategies. This approach considers vulnerabilities beyond those directly observed, examining how various insider threat scenarios could exploit weaknesses within banking systems. By addressing actual and potential risks, this STRIDE application offers targeted mitigation strategies relevant to the case and informs broader cybersecurity practices across the industry.

Table 2. Spoofing

Code	Threat	Description	Mitigation Strategies
S1	Impersonation of a customer	Insider impersonates a client to gain unauthorized system access.	Use robust authentication methods (e.g., MFA) for customer logins and transactions.
S2	Spoofing employee credentials	Insider uses fake internal credentials to access sensitive systems.	Use MFA and biometric verification for employee logins and monitor unusual login patterns.
S3	Spoofing web-based API calls	Insider manipulates API calls to trigger unauthorized actions in backend systems.	Enforce API authentication, monitor usage for anomalies, and apply rate limiting.

Table 3. Tampering

Code	Threat	Description	Mitigation Strategies
T1	Tampering with transaction and log data	Dougherty tampered with current and historical logs to conceal theft, making it difficult to verify transaction legitimacy in audit trails.	Implement transaction verification processes, cryptographic protection, RBAC, immutable logs, audit trails, and regular audits.
T2	Tampering with client account information	Insider alters or corrupts client account data within the database or during account management, leading to unauthorized changes or data corruption.	Encrypt data at rest, apply RBAC, use tamper-evident logs, and enforce audit logging.
T3	Tampering with security monitoring	Insider alters real-time monitoring data to conceal unauthorized activity or bypass alerts.	Enforce strict access controls, add redundancy in monitoring, encrypt data streams, and conduct regular audits.
T4	Tampering with automated transaction processing	Insider modifies scripts or processes used in automated transactions, resulting in unauthorized transfers or incorrect handling.	Implement code reviews, use checksums to verify script integrity, and enforce version control with audit trails.
T5	Tampering with input validation on web forms	Insider exploits input validation weaknesses to inject malicious data, enabling unauthorized transactions or data corruption.	Implement robust server-side input validation, sanitize inputs, and conduct regular security testing on web forms.

Table 4. Repudiation

Code	Threat	Description	Mitigation Strategies
R1	Denying involvement in unauthorized transactions and account management	Dougherty could have denied unauthorized transactions or changes made to client accounts, covering up fraudulent activities.	Maintain detailed audit logs, use non-repudiation (e.g., digital signatures), enforce audit logging, and strict access controls.
R2	Repudiation in transaction logs and security monitoring	Insider, including security staff, could alter or delete logs, security alerts, or security configurations, making it difficult to verify actions.	Deploy immutable logs, enforce audit trails, log all security personnel actions, use tamper-evident logs, and regularly audit logs.
R3	Repudiation of web interface configuration changes	Insider could alter critical web interface configuration settings, (e.g., access controls or session management policies), and later deny doing so.	Apply version control with detailed configuration logging, use tamper-evident settings, and require multi-level approval for critical changes.

Table 5. Information Disclosure

Code	Threat	Description	Mitigation Strategies
I1	Unauthorized access to client data	Dougherty accessed sensitive client data without authorization, exposing it to misuse.	Enforce access controls, monitor employee access, and encrypt data at rest.
I2	Information disclosure in transaction logs	Sensitive information in transaction logs could be exposed to unauthorized parties.	Encrypt logs, restrict access to sensitive log data, and implement RBAC.
I3	Information disclosure by the security team	Security team member may improperly access or leak sensitive data from the monitoring system.	Implement strict access controls, enforce need-to-know principles, and monitor sensitive access.
I4	Information Disclosure through Web Interface Caching	Sensitive data may be exposed through insecure caching in the web interface.	Disable caching in web browsers/servers, use secure cookies for session management, and regularly review caching policies.

Table 6. Denial of Service

Code	Threat	Description	Mitigation Strategies
D1	Disruption to banking operations (including client interactions)	Insider could disrupt core operations or client-facing systems, disrupt system downtime, and prevent customers from accessing their accounts or conducting transactions.	Implement redundancy, failover systems, load balancing, web application firewalls (WAF), and incident response plans.
D2	Denial of Service in Security Monitoring	Insider could launch a DoS attack on the security monitoring system, impairing the bank’s ability to detect and respond to security incidents.	Implement redundancy in monitoring, intrusion detection/prevention systems (IDS/IPS), and prepare incident response plans.
D3	Denial of Service via Web Interface Input Flooding	Insider could flood web forms or APIs with excessive requests, overwhelming the system, and delaying or denying legitimate user access.	Enforce rate limiting on web forms and APIs, use CAPTCHA to prevent automated submissions, and monitor for unusual activity patterns.

Table 7. Elevation of Privilege

Code	Threat	Description	Mitigation Strategies
E1	Exploiting Administrative Privileges	Dougherty used administrative privileges to access sensitive client data and perform unauthorized actions, such as modifying systems and transferring funds. Other employees could exploit similar vulnerabilities to gain unauthorized administrative privileges.	Enforce strict access controls, use MFA, implement RBAC, enforce security patches, and review administrative access rights regularly.
E2	Elevation of Privilege in Security Monitoring	Insider could misuse or manipulate security tools to escalate privileges, bypass alerts, disable logging, or tamper with security configurations, compromising the integrity of the entire monitoring infrastructure.	Enforce strict access controls, MFA for access to security tools, monitor unusual activity, segregate monitoring duties from other administrative tasks, and regularly audit security configurations and logs for unauthorized changes.
E3	Elevation of Privilege through Web Interface Configuration Flaws	Insider could exploit web interface flaws to gain unauthorized administration privileges.	Conduct regular security audits, restrict access to administrative panels, and enforce RBAC at web level.

Fraud Triangle Analysis (Situational Motivations)

This section analyses the insider threat case through the lens of the Fraud Triangle. In the Dougherty case, the model sheds light on how these situational factors may have intersected to enable and justify her prolonged embezzlement scheme.

- **Opportunity**: With unrestricted and privileged access to sensitive customer accounts and internal systems through her IT and customer service role, Dougherty encountered frequent opportunities to exploit oversight and account monitoring gaps. This allowed her to systematically bypass weak internal controls over 15 years by transferring funds from customer accounts to her own, falsifying records, and rotating accounts to evade detection.
- **Pressure (Incentive):** Although the specific pressures faced by Dougherty are unknown, her acquisition of multiple properties with the stolen funds suggests a desire for an elevated lifestyle, indicating that personal financial motivations may have played a role. Such motivations are common in embezzlement cases (Anindya & Adhariani, 2019).
- **Rationalization (Justification):** While we cannot fully determine her justification, it is plausible that Dougherty saw her actions as deserved compensation, rationalizing that the bank's wealthiest customers, who rarely checked their balances and had not noticed discrepancies over 15 years, were less affected by the losses. This perspective may have led her to believe that her actions had a minimal impact on others and were justified.

- Through the Fraud Triangle, Dougherty's behavior illustrates how unchecked opportunity, possible financial incentives, and personal rationalization can lead to extended fraudulent activity.

Threat Model Diagram

Figure 1 illustrates the STRIDE threat model for the Exchange Bank of Missouri, demonstrating the specific threats and mitigation strategies applied to different components of the bank's system. This model illustrates the vulnerabilities exploited in the insider threat case and potential security risks within a typical banking infrastructure.

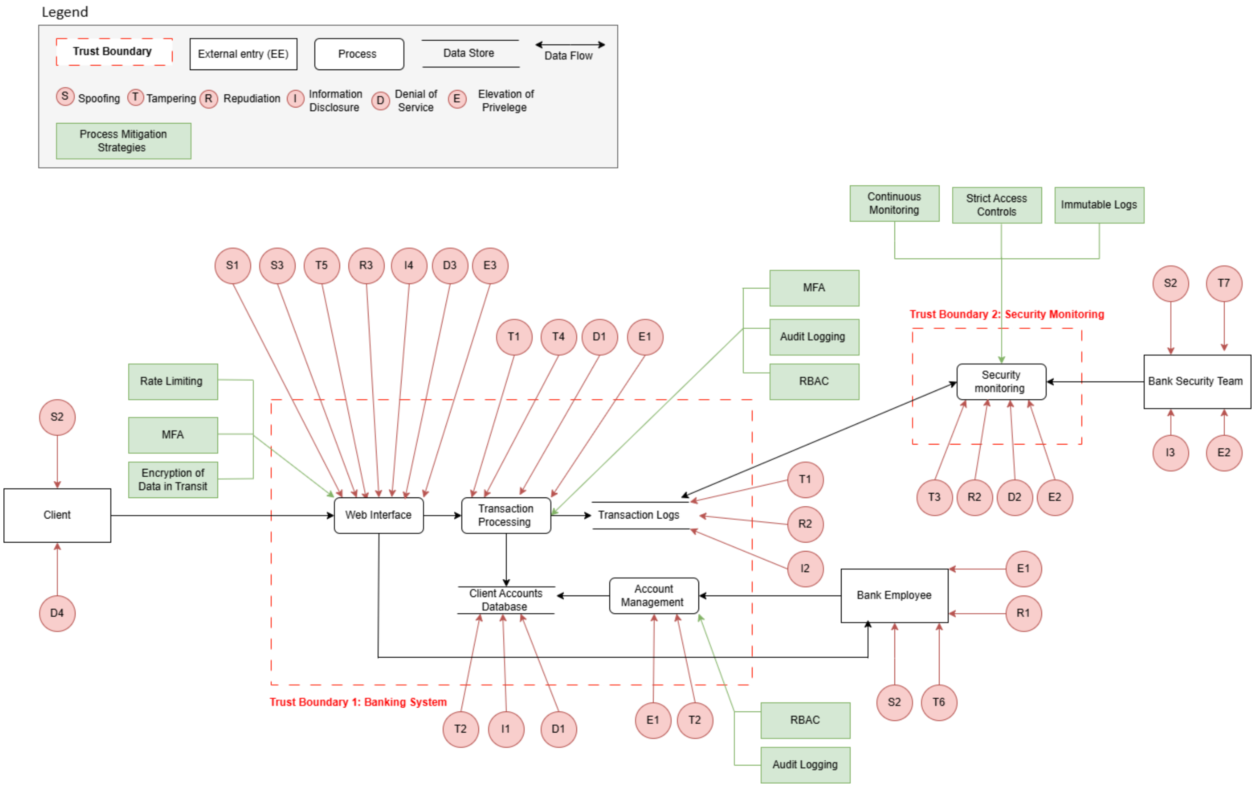

Figure 1. Threat Model Diagram of Missouri Exchange Bank

By leveraging the STRIDE framework in our model, we enhance threat identification and analysis by incorporating a systematic threat elicitation process that integrates an attack taxonomy, mapping information assets and attack vectors into structured threat descriptions (Khalil et al., 2023). Threat modeling provides defenders with a logical examination of the probable aggressor's profile, identifying areas of high vulnerability and where attack vectors may go unnoticed (Haider et al., 2019). Trust boundaries form a key feature of the model, which separate areas of varying security controls and risk exposure, identifying where data transitions between different privilege levels (Khan et al., 2017; Sion et al., 2020).

The model is structured around two key trust boundaries: (1) Banking System and (2) Security Monitoring, delineating areas where security risks and insider threats are most prevalent. Within these trust boundaries, the data flows between critical components, including the web interface, transaction processing, and account management systems, are susceptible to spoofing, tampering, and elevation of privilege attacks. Potential attack scenarios include an insider leveraging elevated access to modify account data and bypassing detection through log tampering or repudiation tactics. To mitigate such risks, the model integrates multi-factor authentication (MFA), role-based access control (RBAC), audit logging, and continuous monitoring, ensuring that unauthorized access attempts and suspicious activities are detected and logged. However, residual risks remain, particularly concerning social engineering attacks, employee collusion, or gaps in privilege escalation monitoring, which could enable sophisticated fraud schemes. Additionally, Denial-of-Service (DoS) threats targeting security monitoring infrastructure could delay fraud detection, exacerbating financial and operational consequences. By aligning STRIDE threats with real-world financial attack vectors, this model offers a structured approach to mitigating insider risks, balancing technical security controls with behavioral threat consideration.

Integration of Insights from STRIDE and the Fraud Triangle

The integration of STRIDE and the Fraud Triangle allows for an in-depth view of the interaction between technical and behavioral vulnerabilities within a system, in this case, a financial institution system. Analyzing Dougherty's abuse of access at the bank, technical vulnerabilities, and behavioral motivations come into play. The STRIDE model reveals that Dougherty exploited several technical weaknesses, such as Tampering with transaction records and the Elevation of Privilege, by misusing her role to access sensitive information. These technical vulnerabilities are directly tied to her access privileges granted within the bank's IT and customer service systems.

The Fraud Triangle provides a complementary perspective by exploring underlying behavioral motives that steered her actions. Perceived financial pressure and her justification of the crime are probable to have reinforced her decision to abuse her role and misuse her access. The combination of her elevated access and her rationalized sense of entitlement formed a scenario where technical controls alone were insufficient to prevent fraud.

The intersections between the STRIDE model's technical threats and the Fraud Triangle's behavioral factors are particularly apparent. Tampering with transaction data and Elevation of Privilege traverse with the Fraud Triangle's concept of opportunity, the conditions or access that enable fraud. Dougherty's role provided unrestricted access to transaction records, which became both a technical vulnerability and a behavioral opportunity. The dual nature of her access privileges further complicated the oversight, as the bank's system was not equipped to flag her repeated actions over time. For instance, her ability to alter transaction logs without immediate detection enabled the continuation of her embezzlement scheme, leveraging technical flaws in the oversight mechanisms in combination with her behavioral drive to exploit them. This overlap sheds light on how insider threats frequently exploit both types of vulnerabilities, making them more difficult to detect when using purely technical controls.

The revealed overlap of technical and behavioral factors in the Dougherty case highlights the limitations of addressing insider threats from a solely technical or purely behavioral standpoint. An entirely technical approach risks overlooking the personal motivations that drive individuals to commit fraud. In contrast, a purely behavioral approach could fail to identify specific system vulnerabilities that create opportunities for fraudulent activity.

This case exemplifies the need for an integrated insider threat analysis perspective, where technical controls and behavioral indicators are continually monitored. Our approach of combining models like STRIDE and the Fraud Triangle creates a more holistic assessment of insider risks, equipping organizations with tools to better identify, mitigate, and respond to such threats. This integrated analysis illuminates more robust safeguards against insider threats and highlights the importance of preventative measures to address the root causes of malicious insider behavior.

Recommendations

Cybersecurity threats are constant, making a robust, evolving security plan essential for financial firms to protect their systems and processes (Kay et al., 2021). Implementing continuous monitoring systems, such as Anomaly Detection Systems and Real-Time Log Analysis, is crucial for detecting insider threats, especially for employees with elevated access (NIST, 2020). In the Dougherty case, stronger monitoring could have flagged suspicious transactions and unauthorized access earlier, enabling prompt intervention. Access management is equally vital. Organizations should enforce Access Control and conduct periodic access reviews to limit employees' system access to their roles and revoke unnecessary privileges (NIST, 2020). Dougherty's embezzlement could have been reduced with more restrictive access controls.

While technology is central to cybersecurity, fostering a strong security culture through leadership, consistent investment, and regular staff training is essential to protecting organizational systems (Tetteh, 2024). Employee support programs addressing behavioral risk factors can help mitigate insider threats (ACFE, 2024). As the Fraud Triangle highlights, personal stressors often drive unethical behavior (Cressey, 1950). Programs such as mental health resources, stress management initiatives, and financial counseling can reduce pressures that lead to misconduct. Together, continuous monitoring, access management, and employee support programs form a multi-layered defense strategy, addressing both technical and behavioral risks to enhance insider threat detection and prevention.

Limitations and Future Work

While this study offers valuable insights into insider threats within a single financial institution, its findings may have limited generalizability due to the case-specific, qualitative nature of the analysis. Future research should apply the combined STRIDE and Fraud Triangle frameworks across multiple cases and industries to validate their effectiveness and improve generalizability. Multi-case studies or quantitative methods with larger samples can further strengthen findings. Additionally, exploring variations of these frameworks across industries and threat scenarios will test their adaptability and effectiveness. Such advancements will enhance understanding of insider threats and improve detection and mitigation strategies across sectors.

Conclusion

This study highlights the need to address technical vulnerabilities and behavioral motivations in mitigating insider threats within financial institutions. The Dougherty case demonstrates how insider threats regularly emerge from a juncture of technical weaknesses and personal/situational pressures. Technical vulnerabilities, including inadequate access controls and ineffective monitoring systems, create opportunities for malicious actions when shared with behavioral motivations that encompass financial stress and personal justification of actions.

This paper offers a comprehensive approach to insider threat detection and prevention by integrating the STRIDE model and the Fraud Triangle. Through the leverage of STRIDE, organizations can systematically identify and address technical risks, while the Fraud Triangle offers insights into the behavioral factors that may drive insider misconduct. Together, these frameworks provide a layered defense strategy that augments an organization's ability to detect, prevent, and rapidly respond to insider threats more effectively. This paper also underscores the significance of an integrated approach that combines technical controls and behavioral understanding to fortify security practices and safeguard against multifaceted insider risks within the banking sector and beyond.

References

American Bankers Association. (2024). *Cybersecurity & Data Security*. American Bankers Association. https://www.aba.com/banking-topics/technology/cybersecurity

Anindya, J. R., & Adhariani, D. (2019). Fraud risk factors and tendency to commit fraud: Analysis of employees' perceptions. *International Journal of Ethics and Systems*, 35(4), 545–557. https://doi.org/10.1108/IJOES-03-2019-0057

Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations.* Association of Certified Fraud Examiners. https://legacy.acfe.com/report-to-the-nations/2024/

Bellovin, S. M. (2008). The insider attack problem: Nature and scope. In S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith, & S. Sinclair (Eds.), *Insider attack and cyber security* (Advances in Information Security, Vol. 39, pp. 1–4). Springer. https://doi.org/10.1007/978-0-387-77322-3_1

Bishop, M., & Gates, C. (2008). Defining the insider threat. Proceedings of the 2008 *Cybersecurity Innovation and Research Workshop*. https://doi.org/10.1145/1413140.1413158

Burch, G. F., Batchelor, J. H., Reid, R., Fezzey, T., & Kelley, C. (2021). The influence of employee personality on information security. *ISACA Journal.*

Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*. Addison-Wesley.

Cybersecurity & Infrastructure Security Agency. (2024). *Defining insider threats*. U.S. Department of Homeland Security. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

Code42. (2024). *Annual data exposure report 2024*. Code42 Software Inc., from https://www.code42.com/resources/reports/

Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

Exchange Bank of Missouri. (2024). https://www.ebmo.com/

Federal Financial Institutions Examination Council. (2023). *IT examination handbook: Information security*. https://ithandbook.ffiec.gov/it-booklets/information-security.aspx

Glancy, F., Biros, D. P., Liang, N., & Luse, A. (2020). Classification of malicious insiders and the association of the forms of attacks. *Journal of Criminal Psychology*, 10(3), 233–247. https://doi.org/10.1108/JCP-03-2020-0012

Haider, W., Seeam, A., Ghogho, M., & Adebayo, S. (2019). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access*, 7, 167593–167605. https://doi.org/10.1109/ACCESS.2019.2954423

Hunker, J., & Probst, C. W. (2011). Insiders and insider threats: An overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications,* 2(1), 4–27. https://doi.org/10.22667/JOWUA.2011.02.01.004

IBM. (2024). *Cost of a data breach report 2024*. IBM Security. https://www.ibm.com/security/data-breach

Jiang, R. (2022). Exploring employees' computer fraud behaviors using the fraud triangle theory. Pacific Asia *Journal of the Association for Information Systems*, 14, 100–121. https://doi.org/10.17705/1pais.14404

Kay, A., Hutcherson, C., Keene, C., Zhang, X., & Terwilliger, M. G. (2021). How financial Institutions address cybersecurity threats: A critical analysis. *Issues in Information Systems*, *22*(1), 63-74. https://doi.org/10.48009/1_iis_2021_63-74

Khalil, S. M., Bahsi, H., Dola, H. O., Korõtko, T., McLaughlin, K., & Kotkas, V. (2023). Threat modeling of cyber-physical systems: A case study of a microgrid system. *Computers & Security, 124*, 102950. https://doi.org/10.1016/j.cose.2022.102950

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017). STRIDE-based threat modeling for cyber-physical systems. *Proceedings of the IEEE International Conference on Smart Grid Communications*, 1, 1-6. https://doi.org/10.1109/ICSGC.2017.8105891

National Institute of Standards and Technology (NIST). (2020). Security and privacy controls for information systems and organizations (SP 800-53, Rev. 5). https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

National Institute of Standards and Technology (NIST). (2024). *Insider threat.* https://csrc.nist.gov/glossary/term/insider_threat

Pisani, R. (2023). Insider threats: What banks don't know can definitely hurt them. *Exabeam.* https://www.exabeam.com/blog/incident-response/insider-threats-what-banks-dont-know-can-definitely-hurt-them/

Rouland, Q., Hamid, B., & Jaskolka, J. (2021). Specification, detection, and treatment of STRIDE threats for software components: Modeling, formal methods, and tool support. *Journal of Systems Architecture*, 117, Article 102073. https://doi.org/10.1016/j.sysarc.2021.102073

Security Intelligence. (2015). *Morgan Stanley breach is a reminder of insider risks*. https://securityintelligence.com/news/morgan-stanley-breach-reminder-insider-risks/

SentinelOne. (2019). *Financial cyber threats: 10 cases of insider bank attacks.* https://www.sentinelone.com/blog/financial-cyber-threats-10-cases-of-insider-bank-attacks/

Sion, L., Yskout, K., Van Landuyt, D., van den Berghe, A., & Joosen, W. (2020). Security threat modeling: Are data flow diagrams enough? *In IEEE/ACM 42nd International Conference on Software Engineering Workshops* (ICSEW'20) (pp. 254-257). ACM. https://doi.org/0.1145/3387940.3392221

Shostack, A. (2014). *Threat modeling: Designing for security*. Wiley.

Tetteh, A. K. (2024). Cybersecurity needs for SMEs. *Issues in Information Systems*, 25(1), 235–246. https://doi.org/10.48009/1_iis_2024_120

U.S. Department of Justice. (2024). *Former bank employee pleads guilty to $2.4 million embezzlement scheme*. https://www.justice.gov/usao-wdmo/pr/former-bank-employee-pleads-guilty-24-million-embezzlement-scheme

Verizon. (2023). *2023 data breach investigations report*. Verizon Enterprise. https://www.verizon.com/about/news/media-resources/attachment?fid=65e1e3213d633293cd82b8cb

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, 39(1), 91-112. Retrieved from https://www.jstor.org/stable/10.2307/26628342

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1-20. https://www.jstor.org/stable/43825935