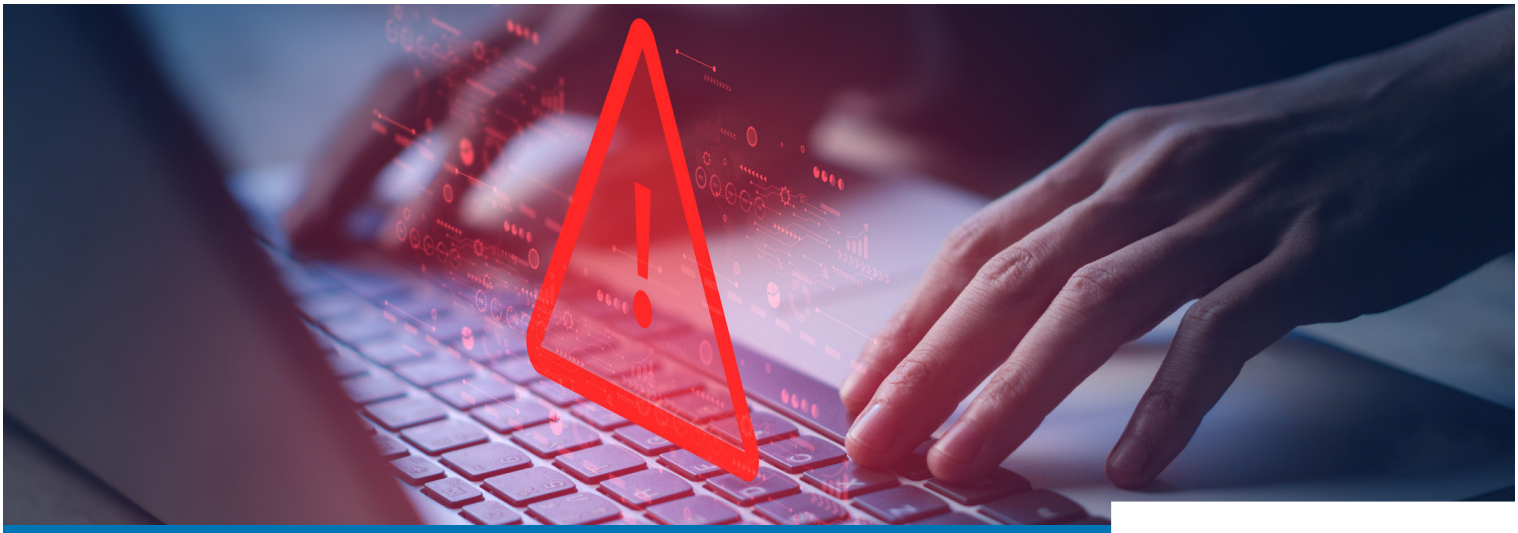


Insider Risk

Rethinking Threat Management in Financial Institutions

Recent regulatory actions and warnings from federal law enforcement underscore the breadth of insider threats facing financial institutions today. Nation state actors, criminal organizations, and terrorist groups are actively exploiting employees — either wittingly or unwittingly — to commit insider acts, including opening fraudulent accounts and divulging sensitive information. Faced with these incidents as well as risks from careless, poorly trained, or disgruntled employees, financial institutions struggle with a diverse and disconnected set of threats that existing risk management systems are ill-equipped to detect and mitigate.

Financial Services – At the Forefront of Insider Risk

Few sectors are more synonymous with security than financial services. From bank vaults and silent alarms to two-factor authentication and encryption, financial institutions are at the forefront of protecting sensitive information and, more importantly, our money. These institutions are also under pressure to maintain robust compliance programs as regulators intensify their focus on money laundering, terrorist financing, and sanctions. In response, firms have developed and adapted sophisticated controls to identify and mitigate risks. With increased reliance on new technologies, the financial sector has prioritized cybersecurity and developed systems and processes to protect IT infrastructure from bad actors and to detect fraudulent behavior.

Despite these efforts, gaps remain in institutions' approach to insider risk mitigation. Most institutions have mature risk programs to address specific threats; however, they frequently operate in silos and are reactionary in nature, rather than proactive in assessing potential threats across all avenues. Segregated reporting processes and a lack of integrated controls leave gaps in many financial institutions' ability to anticipate threats and deploy risk-reducing preventative controls.

While this reactionary posture is not unique to financial institutions, insider incidents in the sector can have outsized financial impact and potentially erode public trust. Preventing instances before they manifest is always better than recovering after an incident. Financial institutions are uniquely positioned to develop a holistic approach to insider risk reduction by leveraging their existing, threat-specific control frameworks. Aligning policies and procedures, and centralizing governance and insider threat reporting from existing risk management efforts is a good first step. Combining this with robust training and a multidisciplinary team of experts to evaluate and act on threats can potentially close gaps and mitigate the threat of insider incidents.

$17.4M

In 2024, the total average cost of an insider incident was $17.4M USD, with the highest activity cost incurred to remediate the incident.[1]

$3B

In 2024, a large financial institution paid approximately $3 billion in penalties following a Department of Justice investigation into the institution's violations of the Bank Secrecy Act and money laundering. The investigation centered on criminal actors exploiting a small number of the financial institution's employees to launder money.[2]

Systemic Challenges (and Opportunities)

The complexity of financial service businesses and the highly regulated environment in which they operate require robust risk mitigation frameworks across all insider risk types. Legacy risk management organizational structures, however, often lead to siloed risk reporting and disconnected risk mitigation, leaving cross-category threat signals undetected.

Overreliance on IT controls as a panacea to reduce insider risk compounds the lack of integrated threat reporting, leaving financial institutions ill-positioned to anticipate insider incidents. Common hallmarks of a reactionary insider risk reduction model, as well as potential enhancement opportunities to cultivate a proactive approach, include:

Siloed Reporting

Behaviors of concern are captured in silos, reducing the organization's ability to preemptively identify and reduce insider risk. Unexplained poor performance or absenteeism is reported to HR, attempts to access sensitive files is reported to digital security, non-compliance with KYC processes is reported to fraud detection, and accepting unreported gifts from vendors is reported to business integrity.

Firms should consider enhanced and centralized reporting to a team trained to assess behaviors of concern. This allows for preemptive risk reduction by providing support to employees before they commit an insider act.

Disconnected Risk Assessments

First-line insider risk assessments — including cybersecurity, fraud, and physical security — are frequently executed independently and reported to risk-specific governance forums. Inconsistent risk taxonomies and rating scales undermine an organization's ability to assess insider risk and control gaps comprehensively.

A centralized risk assessment model allows for a common rubric against which insider risk can be assessed across all businesses and support functions. Firms can develop consistent, enterprise approaches to remediate control gaps.

Failure to Connect External and Internal Threats

Firms often fail to leverage the business lines' understanding of external threat trends that impact insider risk when executing second-line insider risk assessments. Resultant gaps in control remediation can inadvertently allow external actors to take advantage of employees.

Integration of an organization's external threat assessments into a centralized evaluation of insider risk controls allows an organization to reduce its vulnerability to external threat actors who exploit vulnerable employees.

A New Approach to Managing Insider Risk – The Behavioral Threat Assessment Model

Financial Service Chief Risk Officers ("CROs") and business leaders face a complex and diverse set of insider risks, including physical security, cyber security, AML and fraud. Increasingly sophisticated threat actors, including criminals, terrorists, and nation states, combined with heightened regulatory expectations makes the task of managing insider risk ever-more daunting. While the sector's risk landscape is unique, effective insider risk reduction can be informed by other industries' adoption of the behavioral threat assessment model.

Born from the need to anticipate and prevent workplace violence in sectors such as education and healthcare, and informed by years of analysis, the behavioral threat assessment model provides a rubric for anticipatory insider risk reduction applicable far beyond the context of workplace violence.[3] At its core, the behavioral threat assessment model is premised on two key principles.

1. Individuals who commit insider acts almost always exhibit signs of crisis *before they do harm*.[4] This is true irrespective of the type of insider act.[5]
2. Information related to an insider's signs of crisis are often identified and recorded, formally or informally, by different stakeholders in the firm.

After years of pressure testing, the behavioral threat assessment model has become the industry standard in preventing workplace violence. Structured threat assessments such as WAVR-21[6] are now commonplace in sectors with disproportionately high rates of workplace violence. While not uniquely tailored to address insider risk in the financial sector, the two key principles on which they are based — prior behavioral signs of distress and threat reporting — can support a new model of anticipatory insider risk reduction.

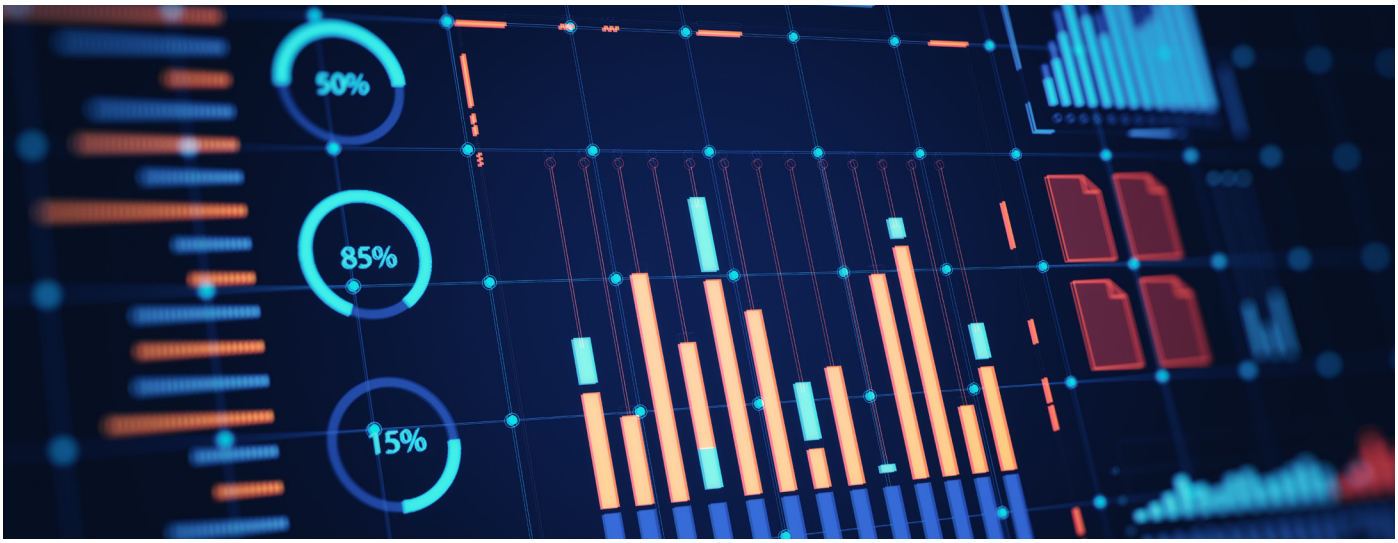
The behavioral threat assessment model contrasts with the siloed, reactionary insider risk reduction programs by not overlooking concerning behavior and actively utilizing opportunities for compassionate, preventative intervention. The table below highlights additional insider threat indicators that, when properly integrated with existing red flags, deliver a more comprehensive view of risk.

INSIDER THREAT INDICATORS*	DISCOVERED WITH AN IT SYSTEMS ONLY APPROACH	DISCOVERED WITH WHOLE PERSON APPROACH
Data exfiltration and unauthorized access	✓	✓
Unusual user behavior (logging on at odd hours)	✓	✓
Systems misuse (unauthorized removable media, hardware, or software)	✓	✓
Emailing sensitive documents	✓	✓
Attempts to escalate privileges	✓	✓
Unexplained poor performance		✓
Suspicious contractual relationships		✓
International travel paid for by a foreign government		✓
Personal stressors, including financial		✓
Unexplained wealth		✓
Attempted to access data not related to their job		✓

**These factors alone do not necessarily indicate someone will become an insider threat. However, when combined, they do increase a person's risk of becoming one.*

Individuals who commit insider acts generally fall into one of three categories – the negligent insider, the malign insider, and the co-opted insider. The table below explains each category of insider, along with identifying respective catalysts for harm and corresponding examples:

CATEGORY	CATALYST FOR HARM	EXAMPLES
Negligent Insider 	Inadvertent / Unintentional	— An employee who falls victim to a phishing email or social engineering — An employee who leaves confidential documents in a public place
Malign Insider 	Intentional	— An employee who knowingly and purposefully leaks IP or trade secrets — Acts of workplace violence
Co-opted Insider 	Coercion	— An employee threatened or paid to divulge information — An employee coerced into opening fraudulent bank accounts



Building a Holistic Insider Risk Management Program

The core of a holistic insider risk program, grounded in behavioral threat assessment and enhanced IT controls, is the **multidisciplinary insider threat assessment team**. Members are drawn from relevant first-line risk teams, including those covering physical security, cybersecurity, fraud, AML, human resources, ethics and compliance, and geopolitical risk. The team is trained in the behavioral threat assessment methodology and evaluates reporting on behaviors of concern and coordinates risk mitigation with the relevant first line teams. Team members also perform periodic evaluations of the organization's enterprise-wide insider risk profile and partner with risk owners to close control gaps.

Combining behavioral threat assessments with existing IT controls, tailored to the unique risks facing financial institutions, can improve the detection and prevention of insider risks. In addition to the multi-disciplinary insider threat assessment team, key components of a holistic insider risk management program, oriented around anticipatory threat detection and risk mitigation include:

Enhanced Pre-Employment Screening

Tailored screening based on the sensitivity of job type, ongoing assessments of external threat actors' capability, and their intent to leverage employees to do harm. Additional tailoring can address job-specific risks.

Digital Monitoring and Controls

IT controls should be calibrated to detect behaviors of concern, informed by the threat assessment team. Creating a cyber fusion center connecting the security information and event monitoring team with other security functions and established insider threat indicators is a leading practice.

Training and Reporting Mechanisms

Employees are the first line of defense against insider risk and must be trained accordingly. Training should cover all insider risks and risk management best practices. Employees should have access to multiple reporting tools including ethics and compliance hotlines, human resources, and employee support groups.

Reporting Policies and Procedures

Align policies and procedures to break down silos and centralize all information related to an employee's behavior. Create a multi-disciplinary threat assessment team to analyze data. Integrate external threat assessments including physical security, geopolitical risk, and nation state and criminal actors.

Conclusion

The increasingly diverse and complex insider threat landscape facing financial institutions presents unique challenges to legacy, siloed risk management frameworks. Yet, the interconnectedness of different insider risk categories presents a unique opportunity: Financial institutions can establish a more holistic and effective approach to identifying and mitigating these risks. Established models like the Behavioral Threat Assessment Model, implemented by a multi-disciplinary insider threat assessment team, allow firms to adopt a "Whole of Person" approach to detecting insider risks. By bringing together experts to analyze previously fragmented data sets, institutions take a critical first step toward reducing insider threats and strengthening overall resilience.

1 https://ponemon.dtexsystems.com/

2 "TD Bank Pleads Guilty to Bank Secrecy Act and Money Laundering Conspiracy Violations in $1.8B Resolution," U.S. Department of Justice Office of Public Affairs (October 10, 2024), https://www.justice.gov/archives/opa/pr/td-bank-pleads-guilty-bank-secrecy-act-and-money-laundering-conspiracy-violations-18b; Balu, Nivedita, "Exclusive: TD Bank appoints compliance monitor after $3 billion US penalty for money laundering," Reuters (February 27, 2025), https://www.reuters.com/business/finance/td-bank-appoints-compliance-monitor-after-3-billion-us-penalty-money-laundering-2025-02-27/.

3 "Behavioral Threat Assessment Units: A Guide for State and Local Law Enforcement to Prevent Targeted Violence," U.S. Department of Homeland Security (October 2024), https://www.secretservice.gov/sites/default/files/reports/2024-10/Behavioral-Threat-Assessment-Units-A-Guide-for-State-and-Local-Law-Enforcement-to-Prevent-Targeted-Violence.pdf.

4 "Module 2: Recognizing Indicators that Someone is on the Pathway to Violence," Emergency Management Institute, FEMA, https://emilms.fema.gov/is_0904/groups/47.html#:~:text=There%20are%20often%20visible%20concerning,with%20the%20average%20being%204.7.; "FBI Helps Public to Recognize Signs of Concerning Behavior," FBI Cleveland Field Office (July 2024), https://www.fbi.gov/contact-us/field-offices/cleveland/news/fbi-helps-public-to-recognize-signs-of-concerning-behavior#:~:text=Comments%2C%20jokes%2C%20or%20threats%20about,associated%20with%20violent%20extremist%20causes.

5 "Insider Threat Awareness Briefing," Defense Counterintelligence and Security Agency (2024), https://securityawareness.dcsa.mil/cdse/nitam/docs/Insider-Threat-Awareness-Brief-2024.pdf.

6 WAVR-21 (Workplace Assessment of Violence Risk) is a structured, evidenced-based way to conduct threat assessments and manage violence risk. It is increasingly used as the basis to conduct violence threat assessments in education settings and workplaces. (https://wavr21.com/).

MARK SEXTON
Senior Managing Director
+1 646.576.8138
mark.sexton@fticonsulting.com

JENN CHRISTIAN
Senior Director
+1 240.962.6666
jenn.christian@fticonsulting.com

09302025 | VN04459-v02