FStech & Bottomline Research Report

# Under the Radar

## How can financial institutions mitigate the risk of insider fraud?

FStech In collaboration with Bottomline

# Introduction

Insider fraud threats are increasingly growing within Financial Institutions (FIs). With the rising pressure from higher living costs and economic uncertainties, remote and hybrid working solutions are creating more opportunities for fraudulent activities, and with an evolving digital landscape expanding the domain for attacks, internal threats and the risk of employees committing fraud are growing.

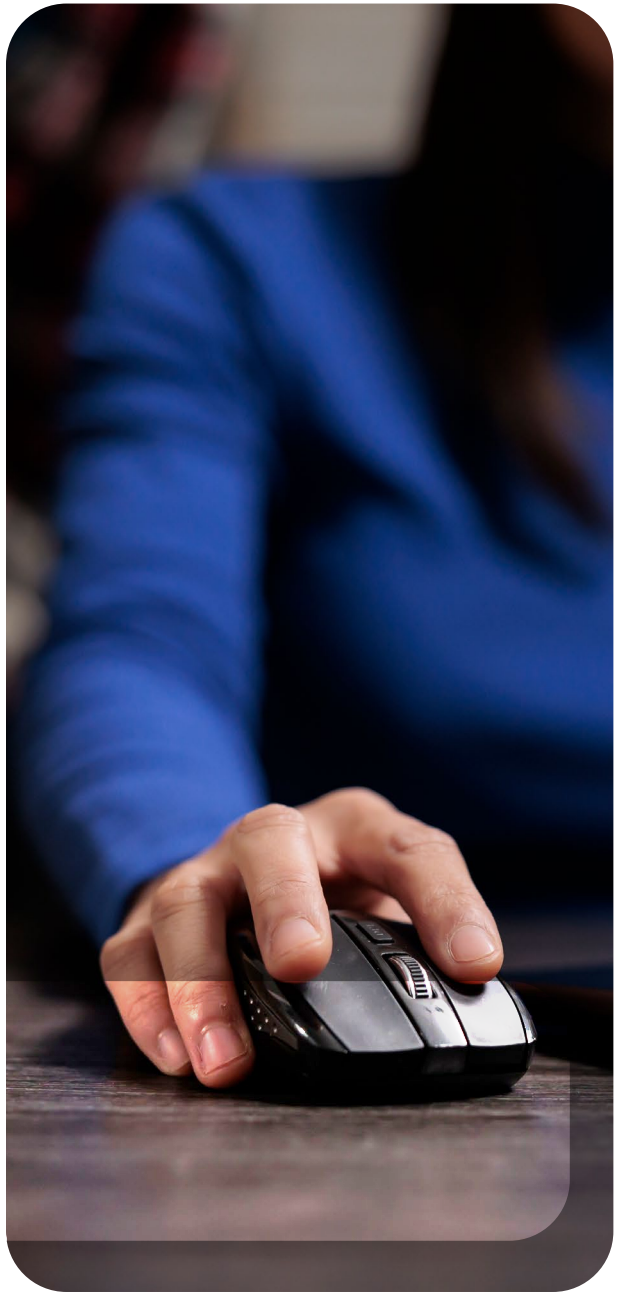
Demonstrating this alarming growth, the annual cross-sector Insider Threat Database (ITD) produced by not-for-profit membership association Cifas found that that the number of insider fraud cases increased 14% year-on-year (YoY) in 2023, with "dishonest action to obtain benefit by theft or deception" identified by 49% of respondents as the most common action.

With heightened regulatory scrutiny throughout the world, including examples such as the UK's upcoming 'Failure to Prevent Fraud' law which penalises organisations that fail to prevent employee fraud benefiting the organisation, more pressure is being deployed on financial institutions to effectively manage and mitigate insider fraud threats than ever. FIs must address these threats while simultaneously protecting customers and achieving profitable growth.

In the current landscape, the nature of insider fraud threats has become more sophisticated, leading to increasingly complex risks and overlaps between internal and external fraudulent activities which require firms to improve ways to maximise risk management and align resilience objectives to corporate goals.

Implementing measures such as integrating the latest technology, boosting communication between departments and providing training programmes are now crucial to identify internal threats before it's too late. Failing to manage these demands could lead to financial losses, reputational damage and operational disruptions, with the long-term costs far outweighing the initial investment required to implement fraud detection and prevention measures.

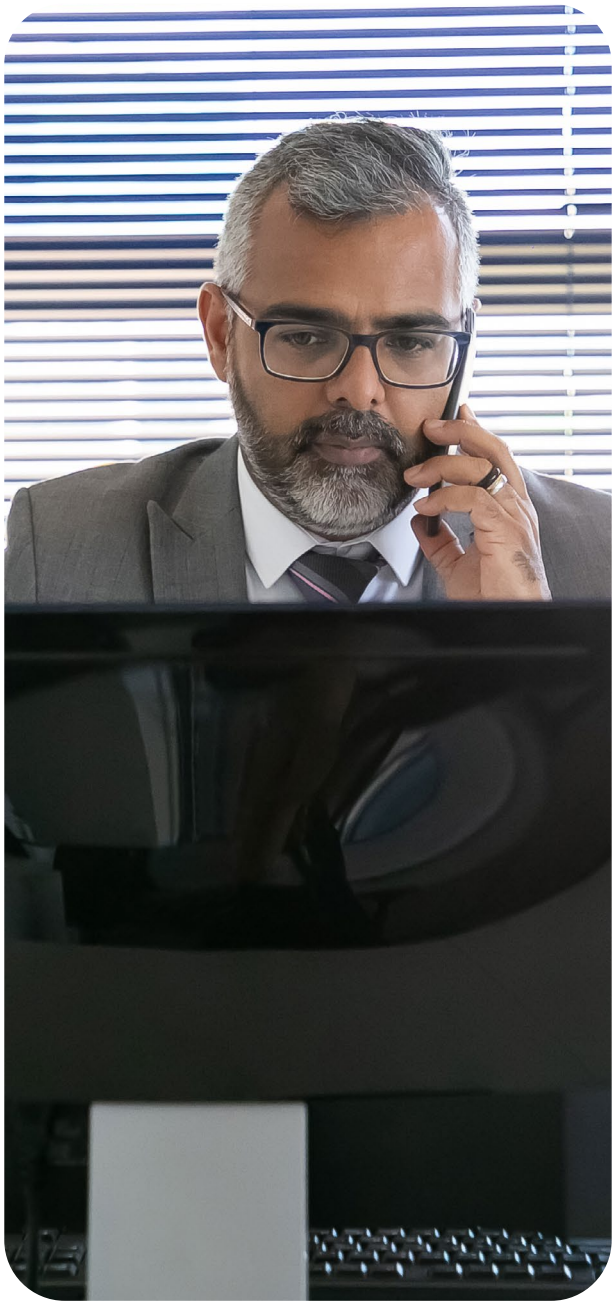
To understand how leaders at financial institutions are addressing insider fraud, Bottomline and FStech have surveyed key decision-makers in the industry to examine what is being done to mitigate the insider fraud risks they are facing. The survey shows that FIs are implementing new measures to solve the problem of insider fraud. However, they may lack access to proper unified systems that can effectively manage insider threat incidents, predict exacerbating risk factors, and help prevent and mitigate these risks.



## Methodology

FStech and Bottomline surveyed 100 financial services professionals from a range of leading financial institutions from across the globe to explore how firms are trying to mitigate the risk of insider fraud as they navigate an ever-changing risk landscape.

**Disclaimer:** Due to rounding, the percentages in this report may not add up to exactly 100%.



# Contents

# 1. Which department(s) in your organisation are responsible for investigating insider fraud incidents? [select all that apply]

The results demonstrate a range of approaches, indicating that financial services professionals rely on multiple internal departments to investigate fraud incidents. Comprising 50-56% of respondents, the top departments tasked with insider fraud investigations are compliance, HR, specialist fraud prevention teams, fraud departments, information security, and audit.

This cross-departmental collaboration is beneficial for addressing insider fraud, as it enables organisations to leverage diverse areas of expertise. Compliance teams bring regulatory know-how, HR has insights into employee behaviour and motivations, fraud departments specialize in detection techniques, information security monitors digital activities, and audit evaluates the effectiveness of internal controls. By working together, these departments can detect critical signals that may go unnoticed by any single team and respond to potential threats more holistically.

However, this multi-pronged approach also introduces coordination challenges, such as information silos and unclear ownership of the investigation process. To mitigate these issues, organisations would benefit from implementing unified case management systems. These can reduce silos and consolidate information into a single secure source, ensuring data is properly shared in a timely manner while safeguarding the integrity of sensitive information. Automation can further ensure that only authorised personnel have access to pertinent data, maintaining confidentiality and preventing data leakage.

# 2. Which of the following measures does your organisation currently have in place to detect and prevent potential insider threats? [select all that apply]

The high adoption rates of these various measures demonstrates that financial institutions recognise the need for a multi-faceted approach to addressing insider threats, with each option being deployed at least 60% of respondents.

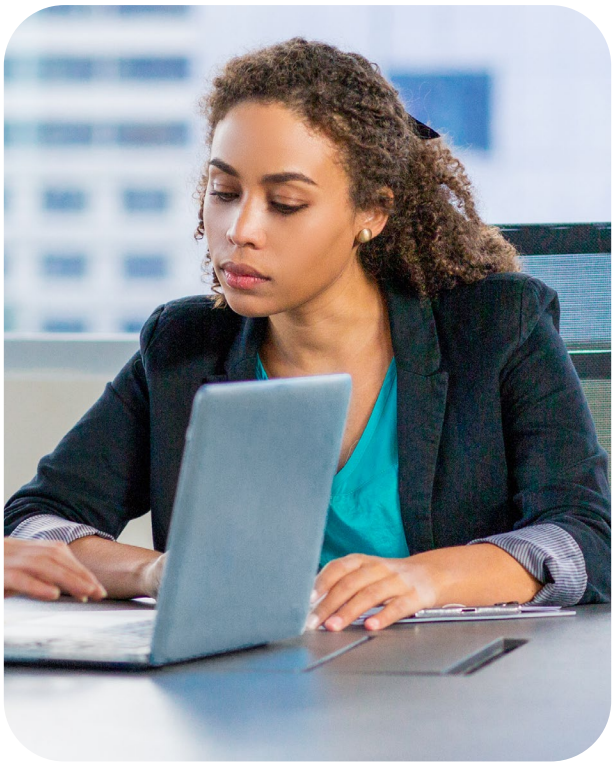
Agent-based monitoring technologies, which provide real-time visibility into employee activities, are seen as particularly valuable, as they can help detect suspicious behaviours or data access patterns that may indicate malicious intent. Similarly, behavioural analytics and anomaly detection capabilities enable organisations to develop a deeper understanding of user behaviour and identify outliers that warrant further investigation.

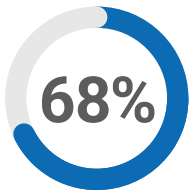
However, while all methods are useful, the implementation of these measures is not without its challenges. The use of agent-based monitoring tools by 68% of respondents raises valid concerns around employee privacy, as they have the potential to inadvertently capture sensitive personal data. Organisations must carefully balance the need for robust security controls with their obligations under privacy regulations such as GDPR.

Behavioural analytics – used by 60% of respondents – on the other hand, often rely heavily on the quality and availability of log and audit data, which can be an issue for some institutions. Organisations should ensure that they have access to comprehensive, high-quality data to enable accurate analysis and effective anomaly detection.

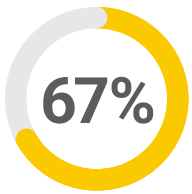
To address these trade-offs, financial institutions can adopt a multi-layered approach to insider threat management. This should involve the strategic combination of complementary measures, such as agent-based monitoring, behavioural analytics, training programmes, and regular security assessments. By implementing a holistic programme that addresses both technological and human-centric aspects of insider threats, organisations can enhance their overall resilience and better protect against the risk of malicious insider activities.

In each case, to be maximally effective organisations should choose complementary services to holistically combine multiple safeguards.

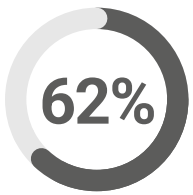




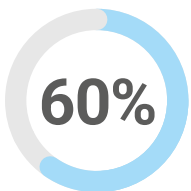

Agent-based Monitoring Technologies: monitoring employee digital actions and communications within the organisation, typically from their devices




Employee training and awareness programmes: providing training and awareness programmes to educate employees about insider threat risks



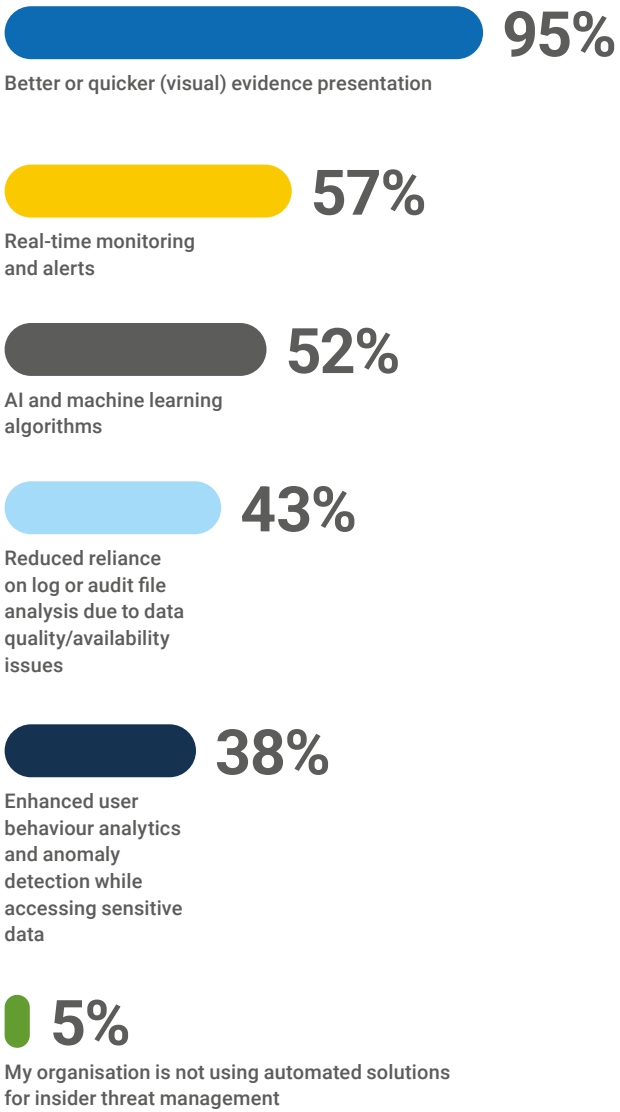

Regular security audits and assessments: conducting periodic audits and assessments of access logs, system configurations, and user privileges to identify security gaps




Behaviour analytics and anomaly detection: implementing behavioural profiling algorithms to analyse employee behaviour patterns and identify deviations or anomalies while accessing sensitive data


We currently do not have any of the measures listed in place

## 3. Which of the following capabilities do you think would make the automated solutions currently used by your organisation for insider threat management more effective? [select top three]




The report highlights that a striking 95% of respondents think better, or quicker visual evidence presentation would improve their automated systems for insider threat management. The most advanced approach combines screen-by-screen data capture with record-and-replay functionality, significantly enhancing investigative accuracy. This capability allows investigators to create a visual storyboard that shows exactly what the employee was doing within an application, including replaying all searches and actions performed. Since the activity is captured exactly as it happened, there is no missing data or alternative perspective to dispute the facts.

By providing decision-makers with data-driven insights, visual evidence presentation can support faster and more informed risk mitigation actions. The lack of clear visual evidence and reliance on traditional models could cause struggles despite the implementation of other systems such as behavioural analytics and anomaly detection systems.

The second most desired capability, as indicated by 57% of respondents, is real-time monitoring and alerts. This emphasises the need for proactive threat detection, where organisations can be immediately notified of anomalies or suspicious activities, enabling them to swiftly address potential insider incidents before significant damage occurs.

The importance placed on AI and machine learning algorithms, selected by 52% of respondents, reflects the growing recognition of the role that advanced analytics can play in enhancing insider threat management. However, it's important to recognise that the effectiveness of AI and machine learning is heavily dependent on the quality and availability of data. Without robust, clean, and comprehensive datasets, the reliability of predictive models can be compromised, leading to inaccurate insights or flawed decision-making. High-quality data is the foundation for building AI models that are both accurate and trustworthy. By leveraging these technologies, organisations can more effectively identify patterns, detect outliers, and uncover subtle indicators of malicious intent that may be difficult to discern through traditional rule-based approaches.

In contrast, capabilities related to reducing reliance on log or audit file analysis due to data quality/availability issues, as well as enhanced user behaviour analytics and anomaly detection, were ranked lower in priority. Organisations may feel more comfortable with traditional approaches, despite their limitations, and may not see an urgent need to upgrade or change them, believing their current systems are adequate. However, as internal threats become more complex and advanced, these organisations may mistakenly assume they are fully protected, unaware of the risks they don't yet understand.

To address the top desired capabilities, our report recommends that financial institutions invest in developing robust visual analytics platforms that can consolidate data from various sources and present it in a clear, actionable manner. Such platforms would not only facilitate comprehensive data analysis but also enable institutions to compile this information as documented evidence, which can be crucial in making a case against an employee or initiating legal action.

Additionally, organisations should implement real-time monitoring and alert systems that leverage advanced analytics to proactively identify and respond to insider threats. Adopting AI and machine learning-powered solutions can further enhance the effectiveness of these systems by improving the accuracy and timeliness of threat detection.

# 4. How frequently do malicious insider threat incidents impact your organisation?
[select the most appropriate answer]

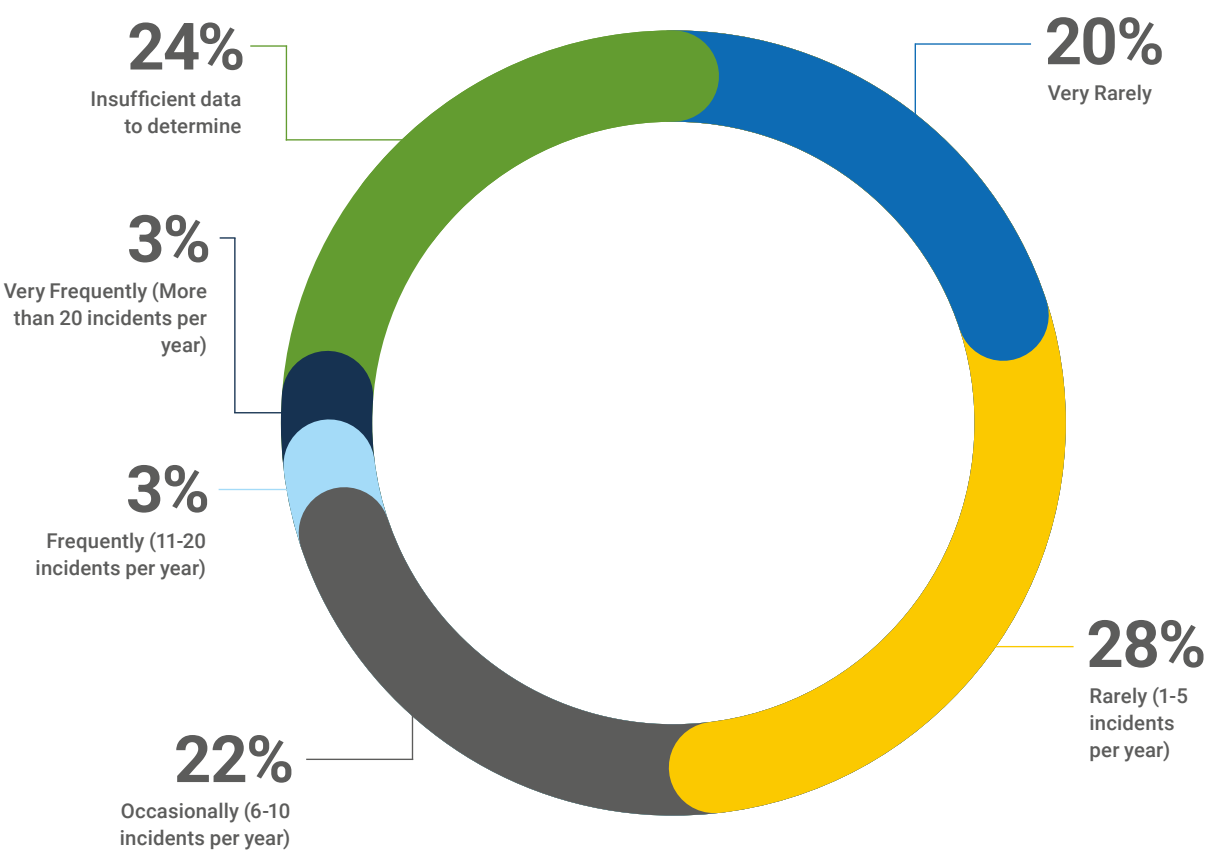
The finding that over 50% of respondents report experiencing some form of malicious insider threat incident each year, even if at a low frequency, underscores the persistent nature of this challenge for financial institutions. While it is reassuring that most organisations rarely or very rarely (48%) face such incidents, the severity of each case can have significant consequences, from financial losses, due to the potential size of transactions, to reputational damage.

The Banking and Financial Services industry is particularly vulnerable to sophisticated and damaging insider threats, as employees in these sectors often possess the financial expertise to exploit weaknesses in control systems. According to the latest Association of Certified Fraud Examiners (ACFE) report, this industry is among the hardest hit by insider fraud, highlighting the critical need for financial institutions to strengthen their security measures.

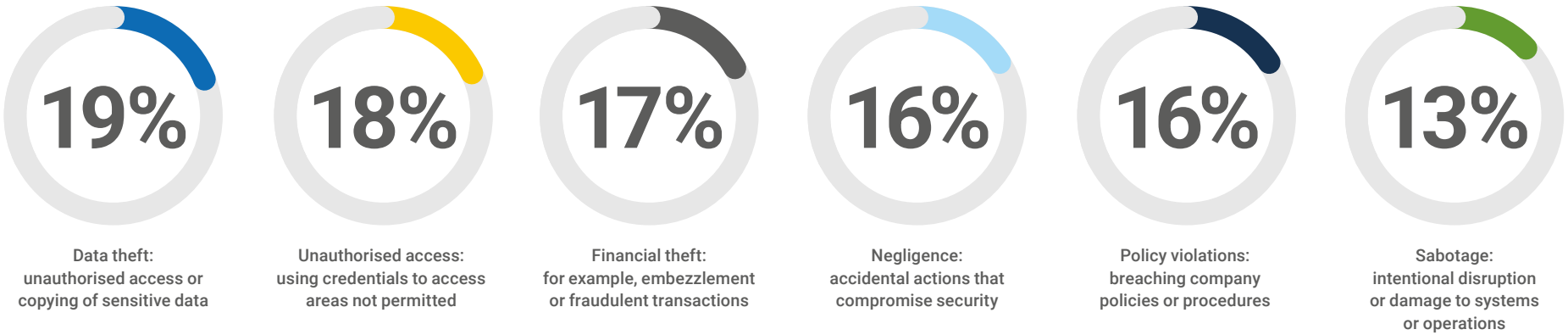
A concerning gap in security controls is revealed by 24% of respondents claiming they lack insufficient data to determine the extent of insider threats in their organisations. This suggests that a significant portion of financial institutions may be unaware of the true scale and impact of insider risks, potentially leaving them exposed to fatal threats in the coming years if they do not take action to implement comprehensive monitoring and reporting capabilities.

To address this, our report recommends that financial institutions invest in developing robust security monitoring and analytics solutions that provide a clear, evidence-based understanding of the insider threat landscape within their organisations. By enhancing their incident tracking and reporting processes, institutions can better identify patterns, quantify the frequency and impact of incidents, and make informed decisions to strengthen their defences.

Additionally, organisations should consider implementing advanced security analytics platforms that can consolidate data from multiple sources, detect anomalies in user behaviour, and provide real-time alerts on potential threats. By gaining better visibility into the evolving nature of insider risks, financial institutions can proactively address vulnerabilities and develop more effective mitigation strategies.



## **5.** Which of the following is the most prevalent type of insider threat in your organisation?
[select one answer]



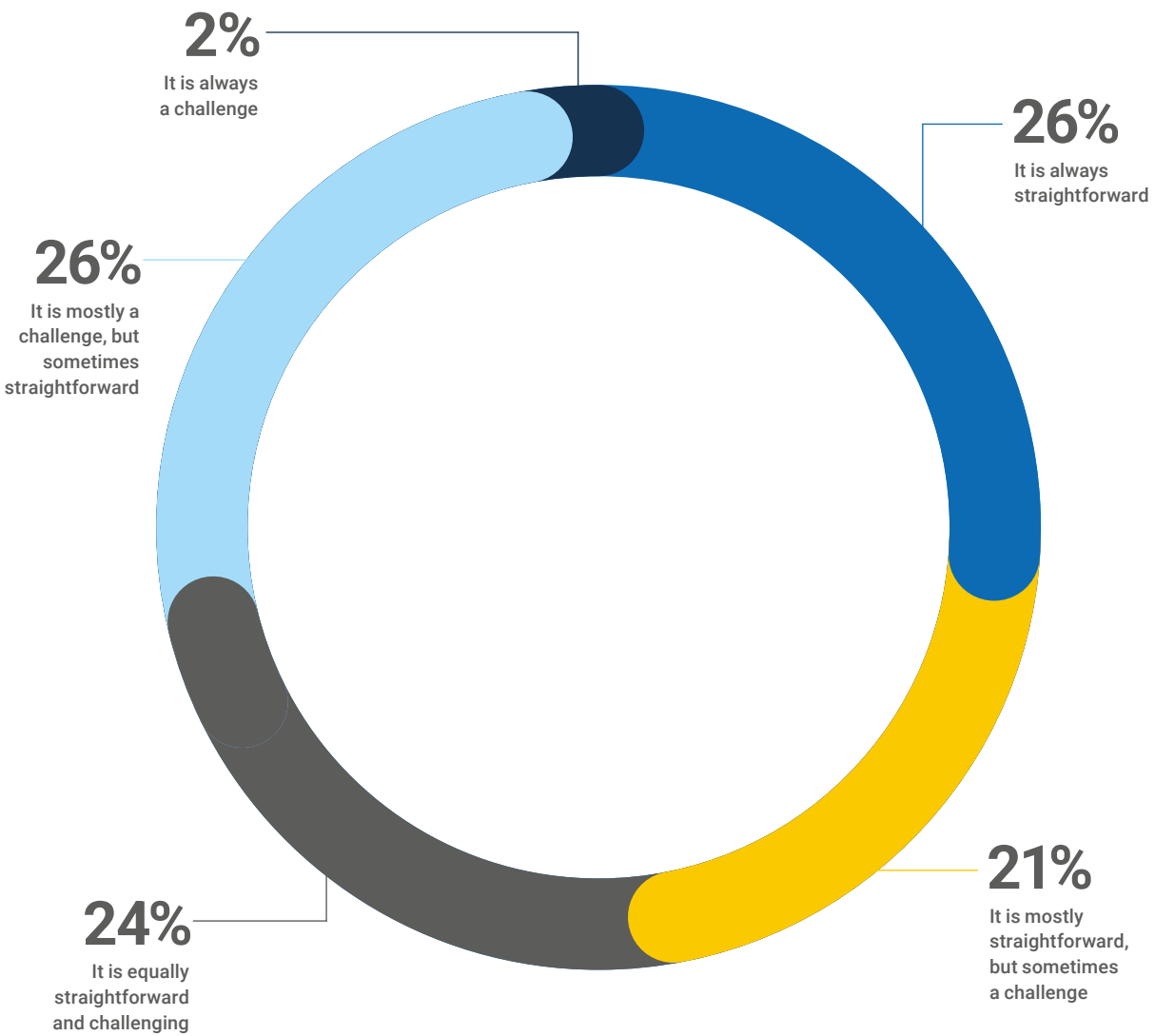

The report shows that organisations consider data theft as the most significant insider threat, with nearly 20% of respondents identifying it as a major issue. This is not surprising, as the unauthorised access, mishandling or copying of sensitive customer data can be a serious risk for companies, leading to reputational damage and regulatory violations.

While financial theft, such as embezzlement or fraudulent transactions, is a concern for the industry, it is notable that it ranks below data theft in prevalence. This may indicate that financial institutions have historically placed a stronger emphasis on protecting their assets, though the risk of financially motivated insider threats should not be underestimated.

Other prevalent threat types, such as unauthorised access, negligence, and policy violations, demonstrate the diverse nature of insider risks faced by the industry. These threats can not only enable direct financial or data loss but also serve as gateways for more sophisticated attacks, potentially exploited by external threat actors through social engineering or vectors such as business email compromise (BEC) and authorised push payment (APP) fraud.

To address this multifaceted challenge, financial institutions must adopt a holistic approach to insider threat management. This should include a combination of robust access controls, advanced user behaviour analytics, comprehensive employee training programs, and clear incident response plans. By addressing the full spectrum of insider threat vectors, organisations can better protect their assets, reputation, and overall security posture.

## **6.** How straightforward is it for your organisation to find evidence when there is suspicious insider threat activity? [select one answer]




While 25% of respondents report that finding evidence is straightforward, it is concerning that a combined 71% of organisations stated that the process involves some form of a challenge. This suggests that many financial services organisations still struggle with the process of collecting, analysing and presenting evidence of suspicious insider activities. This is a recurring issue that links back to earlier in the survey.

While suspicions of insider fraud frequently arise, proving such cases can be challenging due to insufficient evidence. For example, searching through and analysing logs to expose insider threats and compile evidence on complex fraud schemes often lack context and is overwhelmingly time-consuming. This difficulty often leads to insider fraud being less visible, under-reported, or entirely unreported. Consequently, it is mistakenly perceived as a lower risk; organisations operate under the assumption that they are aware of potential threats when, in reality, they may be overlooking significant risks due to the lack of visibility into these covert activities.

To address these challenges, financial institutions should invest in developing standardised investigation protocols and equipping their teams with dedicated case management systems and evidence-based forensic analysis tools. These capabilities can streamline the evidence gathering process, improve cross-departmental collaboration, and ensure that critical information is captured and presented in a clear, actionable manner.

Additionally, organisations should consider providing specialised training to their compliance, HR, and security personnel on best practices for insider threat investigations. By building internal expertise and enhancing the organisation's overall investigative capabilities, financial institutions can more effectively uncover and respond to suspicious insider activities.

## 7. The UK's upcoming 'Failure to Prevent Fraud' law penalises organisations that fail to prevent employee fraud benefiting the organisation. How do you anticipate this new legislation (expected sometime in 2H 2024 or 1H 2025) will change how your organisation prioritises insider threat detection and prevention? [select the most appropriate answer]


The responses to this question are evenly distributed, with 29% of respondents stating that they would not change their approach despite the new law coming into force. This is a concerning finding, as organisations should be expected to have reasonable fraud prevention procedures in place, despite the wait for official guidance and firms that choose not to prioritise compliance will face significant penalties and potential reputational damage.

One possible explanation for this lack of concern is that these organisations may already have robust insider threat management programmes in place and feel confident in their ability to meet the new regulatory requirements. While this may be the case, it is also possible that some respondents are underestimating the potential impact of the law and the need to re-evaluate their overall approach to insider threat detection and prevention.

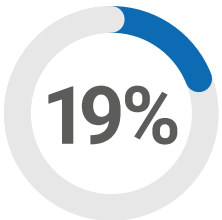
The decision not to prioritise the law – consciously or not – could also be due to an internal shift in focus towards employee training schemes and awareness programmes, as outlined in the results of question 10.

Regardless of their current state of affairs, some 47% of respondents are planning to prioritise further implementations to better understand and manage fraud risks reflecting a robust commitment to address fraud risks for better outcomes. This indicates organisations are currently in search of implementing more robust risk management programmes, practices, and systems.

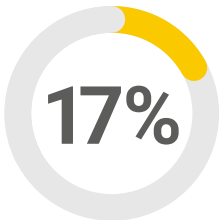
All financial institutions should undertake a comprehensive review of their existing policies, controls, and response procedures. This should include conducting gap assessments to identify areas that require strengthening, updating internal policies and training programs to address the new legal requirements, and implementing advanced monitoring and analytics solutions to enhance their ability to detect and respond to suspicious activities.

By proactively addressing the implications of the "Failure to Prevent Fraud" law, organisations can not only avoid potentially severe penalties but also strengthen their overall resilience against insider threats, ultimately protecting their assets, reputation, and customer trust.

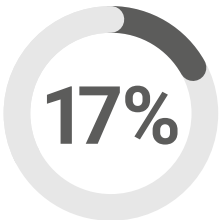
## **8.** What is your organisation's primary concern regarding privacy in the context of insider threat monitoring? [select the most appropriate answer]



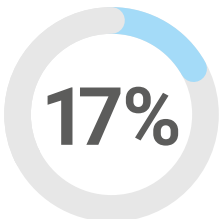

Ensuring that monitoring activities are proportionate and justified (avoiding excessive monitoring)




Employee privacy concerns around monitoring activities that aren't security-related (e.g., personal browsing history, emails, messages)




Ensuring a culture of trust within the organisation




Transparency about employee monitoring practices and the use of collected data


Legal compliance with employee privacy regulations (e.g., GDPR, CCPA)


Balancing employee privacy with organisational monitoring needs

The survey results demonstrate that financial institutions are actively considering privacy concerns in the context of insider threat monitoring, with a slight majority of respondents (19%) emphasising the need to ensure that monitoring activities are "proportionate and justified" and avoid excessive monitoring.

This emphasis on proportionality reflects the critical balance that organisations must strike between effective monitoring and respecting employee privacy. Overly intrusive or disproportionate monitoring practices can not only erode trust and morale within the workforce but also expose the organisation to potential legal and reputational risks.

To address this challenge, our report financial institutions must implement monitoring solutions and practices that prioritise data minimisation, such as network-based monitoring and the use of pseudonymization techniques. By collecting and processing only the essential information required for security purposes, organisations can meet their insider threat detection and prevention objectives while minimizing the impact on employee privacy.

Equally important is the need for transparency and clear communication around monitoring practices. Organisations should develop and clearly articulate their policies regarding employee monitoring, explaining the purpose, scope, and safeguards in place to protect personal information. By engaging employees and fostering a culture of trust, financial institutions can alleviate concerns and ensure that their insider threat management efforts are perceived as necessary and justified.

## 9. How well do you think your organisation's risk management strategies effectively address the potential overlap and interconnectedness between insider fraud and external fraud incidents? [select the most appropriate answer]

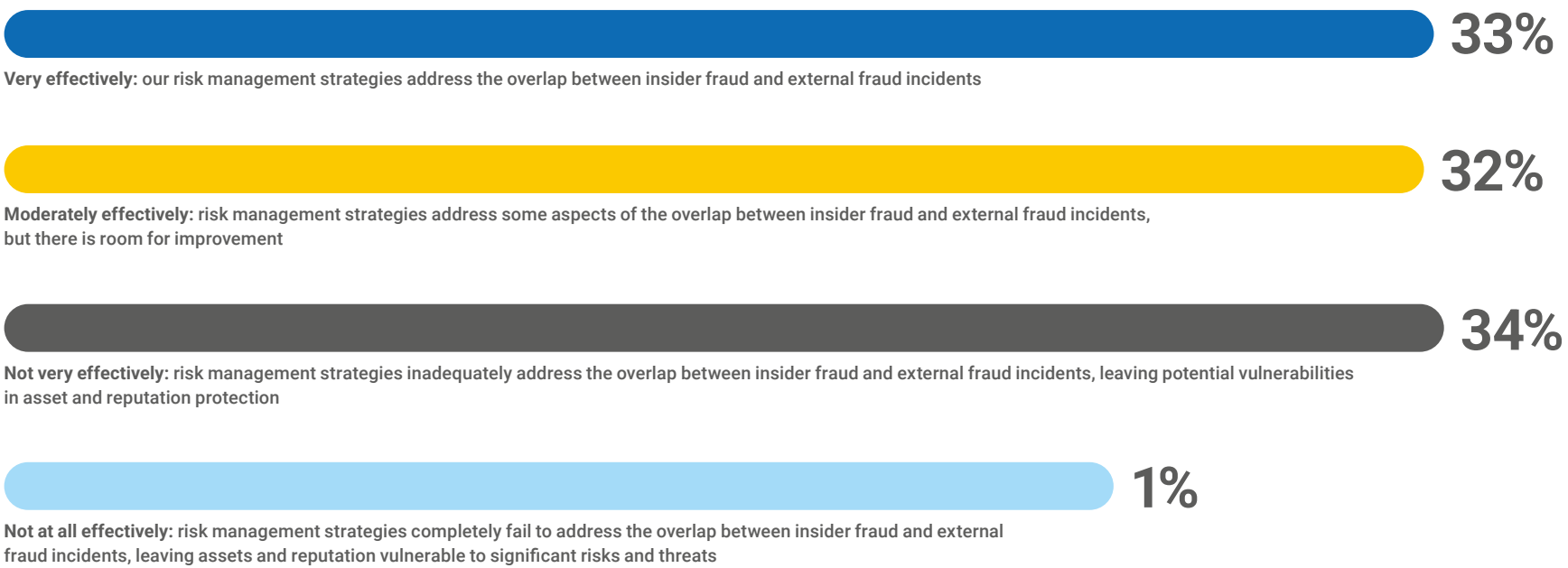
While the majority of respondents (65%) report that their risk management strategies are very or moderately effective in addressing the overlap between insider and external fraud, it is concerning that 35% of organisations are still struggling with their level of risk management, suggesting further improvement is still needed to combat insider threats effectively.

The inability to effectively manage the inter-connectedness between insider and external fraud threats can leave financial institutions vulnerable to significant risks. Insider threats can be exploited by external actors through techniques like business email compromise or social engineering, while external threats may also be enabled or amplified by malicious insiders with access to sensitive information and systems.

As emphasised in responses to question 2, financial institutions need to invest in integrated monitoring solutions and threat intelligence sharing capabilities to enhance their overall security posture. These can capture user behaviour in real-time across systems and services such as multi-app monitoring from all channels, a great benefit in the case of potential overlaps and interconnectedness between internal and external fraud incidents.

Being able to capture user behaviour in real-time across systems is of great help as external frauds can be more visible to detect, while internal fraud can be more subtle and difficult to identify.

Additionally, financial institutions should establish cross-functional teams and incident response protocols that bring together specialists from areas like compliance, fraud, cybersecurity, and risk management. By fostering collaboration and coordinating their efforts, these teams can more effectively mitigate the complex, interconnected risks posed by both insider and external threats.



## **10.** Which of the following is the top priority for your organisation's insider threat management strategy over the next 12 months? [select one option]

Responses were evenly distributed and demonstrate a range of views, indicating that financial services professionals have multiple priorities to further improve their management threat strategies.

Over a fifth of respondents (21%) identified the introduction or enhancement of employee training and awareness programs as their top priority for insider threat management over the next 12 months. This emphasis on human-centric can teach staff how to detect red flags and be empowered to assess risks and create a more vigilant and engaged workforce that serves as an additional layer of defence.

Any employee training initiatives should be closely integrated with other components of the insider threat management strategy, such as the implementation of advanced monitoring technologies, the enhancement of data quality and accessibility, and the promotion of ethical behaviour through policy updates and leadership initiatives. By aligning these various workstreams, financial institutions can create a comprehensive, multi-pronged approach to addressing the insider threat landscape.

The figures also indicate that organisations are looking at more sophisticated systems that can improve data quality and reducing silos (16% of respondents), suggesting that a holistic approach that further enhances collaboration across departments would boost their approach to mitigate insider fraud risk.

Some 17% of respondents reported addressing privacy concerns while enhancing insider threat detection is considered a priority, suggesting that respondents are actively considering privacy concerns in the context of insider threat monitoring, considering systems that can solve legal and ethical complications and seamlessly implement data protection regulations.

# Conclusion

Internal fraud incidents are now a serious threat for financial institutions (FIs).

The report shows FIs are aware of the dangers posed by several insider fraud threats, including unauthorised access to specific areas, financial theft, policy violations and data theft.

To further strengthen their defences, many FIs are managing insider risk by implementing monitoring technologies, which help monitor employee digital actions and communications within the organisation. Consequently, they are actively considering privacy concerns, prioritising legal and ethical complications alongside data protection regulations.

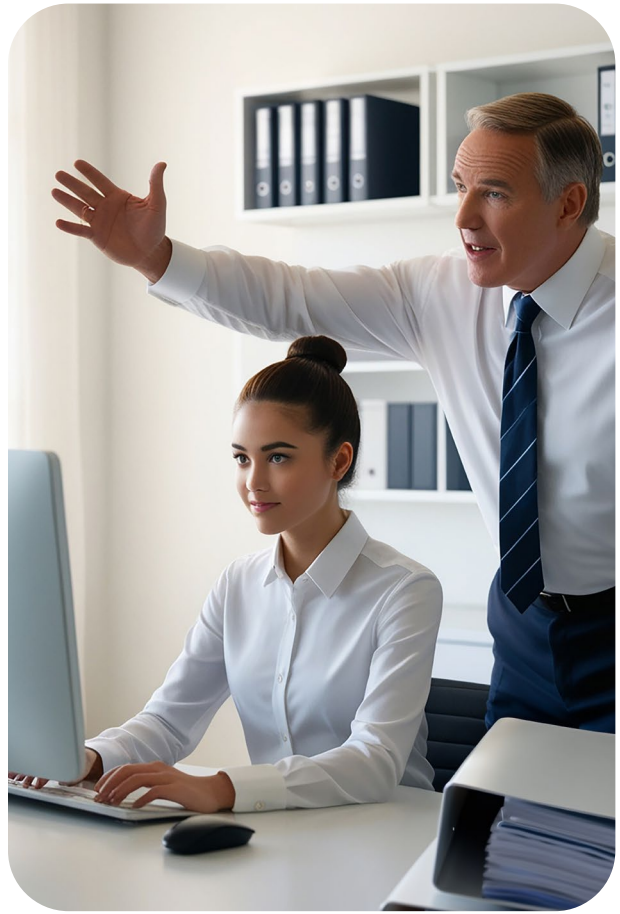
Despite active measures to shield against insider threats, more than 70% of respondents find evidence gathering challenging, and 35% struggle with risk management, indicating a need for further improvements. Organisations should implement new measures and strengthen existing ones. Although many FIs feel confident in their current safeguards, preparedness can always be enhanced through increased staff training, collaboration with internal and external stakeholders, and the implementation of suitable monitoring technologies.

Organisations need to put new measures in place while strengthening the previous ones. While many FIs are confident that they are in safe hands when it comes to insider fraud, preparedness can always be improved by increasing staff training while collaborating with internal stakeholders and external organisations and implementing suitable monitoring technologies.

In light of the ongoing unsettled economic climate throughout the UK and Europe coupled with new impending regulations soon taking place FIs must not underestimate the rising risk of insider fraud. Proactively addressing insider fraud through continuous monitoring and regular updates to security protocols can significantly reduce the risk of incidents. Leveraging advanced monitoring technologies can provide deeper insights into potential threats and enhance the accuracy of fraud detection. It's also crucial that these technologies present evidence immediately, rather than taking a long time to complete the analysis. A holistic strategy that integrates technological solutions with human-centric approaches, such as employee training and ethical culture promotion, is essential for comprehensive fraud prevention.

Collaboration with industry peers and participation in threat intelligence sharing networks can provide valuable insights and strengthen overall security posture. Staying ahead of regulatory changes and ensuring compliance with new laws, such as the UK's 'Failure to Prevent Fraud' legislation, will be crucial for maintaining trust and avoiding penalties. Continuous improvement of fraud prevention measures, informed by regular assessments and feedback, will help FIs stay resilient against evolving threats.

To be best prepared, FIs should continue to invest in the latest technologies and ensure their personnel are aware of the threats and ramifications of insider fraud.



## About Bottomline

**Bottomline helps businesses transform the way they pay and get paid.**

A global leader in business payments and cash management, Bottomline's secure, comprehensive solutions modernize payments for businesses and financial institutions globally. With **over 35 years** of experience, moving **more than $10 trillion** in payments annually, Bottomline is committed to driving impactful results for customers by reimagining business payments and delivering solutions that add to the bottom line.

FStech In collaboration with Bottomline™