proofpoint.

Managing Insider Threats in Financial Services

Protect Sensitive Data and Safeguard Your Brand

24% of all security breaches occur at financial institutions. And more than half the attacks on these companies come from insiders.[1]

Introduction

Financial services firms are usually among the first to adopt new cybersecurity tools. But despite that investment, the sector still accounts for almost a quarter of all security breaches. And insiders contribute to more than half of these incidents.

As part of their job, workers in this critical sector have access to digital money flow and valuable customer data. This access makes them an inherent risk factor for your business—and lucrative targets for bad actors.

Some insiders are malicious. Many are just careless. And others are compromised by outside attackers who gain access to sensitive data, systems and resources. It's no wonder that insider threats are such a challenging threat vector.

This e-book looks at insider threat management from the perspective of the financial services industry. Drawing from real-life examples in insurance, banking and wealth management, it discusses the challenges of managing these threats. And it shows how Proofpoint can help you identify, investigate and respond to insider incidents quickly and efficiently.

[1] Verizon Data Breach Investigations Report. 2017

SECTION 1

Insider Threats in Today's Dynamic Financial Services Sector

Since 2018, the financial services industry has seen a 20.3% increase in insider threats.[2]

Every business must protect confidential information. That includes safeguarding customer information, corporate data and intellectual property. This mandate may be even more critical for banking, lending, investment management and insurance industries.

Like other industries, the finance sector is moving towards distributed workforces. And it relies more and more on cloud-based applications. These converging trends make managing insider threats even more challenging.

IT infrastructure is now shared by a wider range of users. In a typical enterprise, contractors, service providers, service partners and remote employees may have access. Suddenly, defining an "insider" isn't so simple.

Defining what constitutes a "threat" isn't much simpler. Insider threat management isn't just about rooting out malicious users. It's also about identifying and managing threats from negligent and compromised users.

[2] Ponemon Institute. 2020 Cost of Insider Threat Global Report.

SECTION 2

The Who and What of Insider Risk

Insider risk should be a major focus of any digital-driven businesses. For financial services firms, it's especially critical.

But where should they start? The first step in building a technology-enabled insider threat programme is to understand the *who* and the *what* of insider risk:

- Whom should we be concerned with?
- What should we be protecting?

Who should you be concerned about?

Managing insider risks starts with deciding which of your users pose the biggest risks of insider breach. Every company and use case is unique. But here are some common categories of users to consider:

Non-employee users. Disaggregated, dynamic supply chains and service chains are common in financial services. Often, contractors, service providers, consultants and partners share IT infrastructure with employees. Any of them can pose a potential risk.

Privileged-access users. Some workers need access to protected infrastructure and information. Examples include:

- IT administrators
- Help desk employees
- Call centre associates
- Financial administrators

High-risk employees. Some users may be deemed a high risk by HR based on factors such as:

- Behaviour
- Job changes
- Performance or disciplinary issues
- Flight risk

Employees affected by mergers and acquisitions. The financial services sector is one of constant change. Companies routinely merge, acquire and divest. A firm's authorised user bases may shrink or swell quickly. These changes cause stress on the organisation and can lead to data breaches.

Remote workers. A far greater portion of the global workforce is now working remotely. Working outside of protected network perimeters can increase the risk of insider breaches.

It's not just about malicious users

The term "insider threat" is commonly associated with users who show malicious intent. They may be motivated by financial gain, revenge or foreign allegiances. But negligent or compromised users are actually a much more common cause of insider breaches.

Negligent users are those acting outside of sanctioned processes. They unwittingly expose your infrastructure or data and increase risk.

Compromised users are those under the influence of outside attackers. Some are socially engineered to send data. Others have simply lost control of their account.

In any case, negligent and compromised users are usually your biggest insider risk.

What should you be protecting?

Like most companies, financial services firms rely on highly secure digital transactions. They also depend on the integrity of employee and customer-facing IT infrastructure. Here are some of their highest-priority concerns:

Protecting sensitive data. Financial services firms manage large volumes of personally identifiable information (PII). They include payment card industry (PCI) and personal health information (PHI) data. PII is highly valuable to fraudsters and often the main target of data breaches.

Compliance. The financial services sector is subject to a wide range of regulations and compliance mandates. These rules govern how firms protect data, information and the integrity of their processes. Compliance gaps and data breaches can be costly.

Financial fraud. Financial services firms manage large volumes of transactions and raw capital. Fraudsters exploit workers and use their insider access to steal cash through a wide range of schemes.

Service disruption. Financial services firms rely on IT infrastructure to support customer and employee-facing services. Attackers with insider access can damage or disrupt your systems. Downtime can mean lost revenue, opportunity and trust.

Protecting proprietary information. Many investment firms rely on proprietary information or trading algorithms to maintain a competitive edge. Their success hinges on keeping that data secure.

Brand damage. Financial services build brands on trust—from customers, trading partners and regulators. When security breaches occur, especially when caused by insiders, this trust is violated. That hurts your brand.

SECTION 3

How Insider Threat Management Technology Can Help

Insider threat management helps security teams get a handle on this unique threat vector.

It combines elements of data loss prevention (DLP) and user behaviour analytics (UBA) to help reduce risk in three key ways:

Identifying user risk

ITM solutions enable security teams to quickly detect potential security breaches. The most effective tools help you tell the difference between false positives and insider activity that requires follow-up. This requires knowing the full context around user activity and data movement—especially for users deemed high risk.

Protect from data loss

Most financial firms have data they need to protect—exclusive algorithms, trade secrets, PII and more. No financial service firm wants this data to improperly leave its environment. Quickly identifying and stopping data leakage is a core function of a modern ITM solution.

Accelerate incident response

The cost of insider threats hinges on the time it takes to respond to an incident. Modern ITM systems can help security teams do this as much as 10 times faster. With the right ITM solution, work that might have taken days or weeks can be wrapped up in minutes. Faster investigations lead to shorter mean time to resolution.

SECTION 4 – Proofpoint ITM in Action

Real-World Customer Scenarios

Global insurance broker – Greater visibility into distributed worker activity

The challenge

A global insurance brokerage was looking to protect customers' claims data.

To do that, its security team needed greater visibility into potential insider-led data breaches. The company could monitor its highly distributed workforce through a cloud-based application. But reviewing the app's activity logs—and reverse-engineering what happened—took a lot of time and work. At the same time, data-protection laws only increased concerns about data collected and managed through the app.

The solution

The brokerage needed an insider threat management tool to proactively safeguard confidential data everywhere it lives and moves—especially on remote endpoints. It sought greater visibility into how users interacted with the data and into their activities on endpoints. It needed a solution that could proactively identify high-risk behaviour, send compliance alerts and make audits easier for compliance teams.

The result

With ITM, the company can now:

- Detect risky movement of claims data files from corporate apps, on servers and out of endpoints.
- Educate and warn users of out-of-policy behaviour in real time.
- Correlate irrefutable evidence on the "who, what, when, where, why and how" when investigating an alert. Screen captures of endpoint activity provide context of what happened before and after a violation. That insight helps determine whether the act was negligent, malicious or the result of an external compromise.
- Retain a detailed audit trail of employee and third-party activity to meet financial compliance mandates.

Independent wealth management firm – Safeguarding clients' trust and assets

The challenge

Independent wealth management firms are charged with keeping clients' sensitive and private information safe. Success depends on trust.

As part of their day-to-day jobs, the firm's workforce handles private client data every day. For the company insiders include not just fund managers, administrators and other employees but also third-party contractors. The firm faced constant threats—cyber crime, corporate and state-sponsored espionage, monetary fraud and more.

The solution

The firm needed a robust security system that protects them from the risks of cyber crime and monetary fraud. The security team needed an easier way to monitor potentially risky activity across the company. That included distributed users and third parties.

The result

ITM helped the company:

- Simplify acceptable-use and compliance policies.
- Automatically detect risky movement of sensitive and confidential information in real time.
- Streamline incident investigations by correlating all data movement and user activity in real time. Screen captures of endpoint activity provided irrefutable evidence of what the user did.
- Retain a detailed audit trail of user activity to meet financial compliance mandates.

Regional bank – Protecting from insider threats at financial call centres

The challenge

A regional bank needed to keep its call centres secure in a new era of remote work.

Its workforce touched bank member data on every call. The security team needed to continue monitoring insider activity and responding to potential incidents even while employees worked from home. The bank was especially concerned about high-risk employees with access to valuable private information that could be stolen, leaked or altered. The team also needed to identify, collect and share forensic data when responding to an incident.

The solution

The security team sought out a solution to detect anomalous behaviour in real time. But it had to enhance data collection and oversight in a work-from-home world without hurting productivity and customer service.

The result

ITM helped the call centre solve its insider threat challenges by:

- Making users more resilient. ITM raised security awareness with real-world insider threat scenarios. It also helped the bank clarify corporate data policies.
- Deploying lightweight, user-mode endpoint collectors. This approach kept users productive by not slowing down their devices.
- Detecting risky user behaviour and data movement in real time.
- Collaborating with HR, legal, compliance and IT teams. The teams worked together to agree on user and file data collection, behavioural detection needs and incident-response workflows.
- Speeding up investigations. ITM provided contextual intelligence on the user, easier evidence gathering and smoother collaboration between teams.

Conclusions and Recommendations

Why Proofpoint: Best Practices ITM from a Trusted Advisor

Every day, your IT and security teams work hard to work identify, detect and respond to cyber threats. Proofpoint Insider Threat Management (ITM) can help. ITM protects you from data loss, disruption and other damage caused by your users and attackers who compromise them.

Our award-winning solution has helped more than 1,200 leading companies in more than 100 countries:

- Shorten mean-time-to-detect (MTTD) potential risks to sensitive and confidential information from insider threats.
- Reduce breach frequency, severity and cost with shorter mean-time-to-respond (MTTR) to incidents.
- Make security teams more productive with lower costs. With Proofpoint, you can consolidate multiple technologies (such as user-based analytics and endpoint DLP) into a single ITM platform.

Here's how we support you:

- We'll work with you on a proof of concept that helps you visualise your ITM programme.
- We can help you design and build out your internal threat management programme. We can break your projects into manageable bites and prioritise based on high-risk behaviours. The proof of concept helps you visualise your ITM programme. And our ITM Jump Start Services let you realise fast time to value.
- We help you build user resilience with Proofpoint Security Awareness Training.

Our goal is the same as yours: protecting valuable business assets and the people who produce them.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

0512-002-01-01 10/21