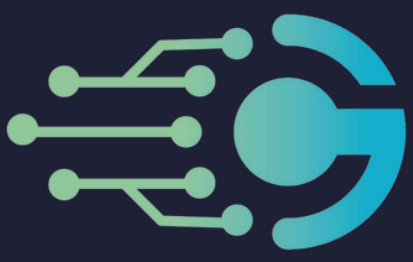
GUIDE

How to Minimise Insider Cyber Security Threats in Your Financial Services Firm



Chapman Technology Partners

Why Insider Threats Are Inevitable for Financial Firms Without the Right Safeguards

80% of cyber incidents involve human error or negligence.

For firms handling sensitive financial data, insider threats aren't just possible—they're inevitable without the right safeguards.

From disgruntled employees to accidental data leaks, insider threats pose a unique risk. Unlike external hackers, insiders already have access. That means damage can be done quickly, quietly, and at scale.

But the good news? These threats can be dramatically reduced with the right strategy.

Over 30% of UK businesses experienced insider-related cyber incidents last year

Source: UK Government Cyber Security Breaches Survey 2024

Only 17% of UK SMEs have an insider threat management strategy in place

Source: Hiscox Cyber Readiness Report 2023

1. 74% of data breaches involve a human element

Source: Source: Verizon Data Breach Investigations Report 2024

1. Define What 'Insider Threat' Means in Your Business

Start by identifying who your insiders are.

This could include:

- Current employees
- Contractors
- Third-party vendors
- Ex-employees with lingering access

And it's not just malicious intent to consider. Accidental insider breaches—such as staff clicking phishing links or sharing credentials—can be just as damaging.

---

2. Apply the Principle of Least Privilege

Give employees only the access they need to do their job, nothing more.

This limits the potential damage if an account is compromised or misused. For example:

- A paraplanner doesn't need admin access to CRM settings.
- An accounts assistant shouldn't access full client portfolios.

Regularly audit permissions to ensure access levels remain appropriate as roles evolve.

3. Implement User Activity Monitoring

Monitoring doesn't mean spying—it's about transparency and protection.

Use tools that log user activity on systems and flag unusual behaviour. For instance:

- Downloading large volumes of data
- Logging in at odd hours
- Accessing client records outside of job responsibilities

Modern platforms allow for automated alerts and real-time response, which is vital in preventing a small incident from escalating.

---

4. Train Staff in Security Awareness

Employees are your first line of defence, but only if they're equipped.

Regular cyber security training should cover:

- Phishing recognition
- Password best practices
- Reporting suspicious activity

Make it sector-specific. For example, highlight risks associated with transferring client funds, compliance breaches, or mishandling regulated data.

Training should be **ongoing**, not one-off. Cyber threats evolve, and your team's knowledge needs to evolve with them.

5. Build a Culture of Security

A strong security culture encourages employees to take ownership and responsibility.

Foster open communication so staff feel safe to report mistakes or suspicious behaviour without fear of blame. Encourage senior leaders to model good security practices.

Security shouldn't be an IT issue, it's an organisational value

---

6. Revoke Access Immediately When Staff Leave

One of the most overlooked insider risks is the ex-employee with active credentials.

Always:

- Disable user accounts on or before their leaving date
- Recover all devices
- Reassign shared access credentials (like software logins)
-

Failure to do this leaves a dangerous backdoor open, especially if the departure wasn't amicable.

7. Use Multi-Factor Authentication (MFA) Everywhere

If a password gets leaked, MFA can stop it being exploited.

Enable MFA across all critical systems—especially:

- Email platforms
- CRM and client data portals
- Cloud storage and backup tools

MFA is one of the simplest and most effective ways to protect against both insider and external threats.

---

8. Have a Clear Insider Threat Response Plan

Even with defences in place, incidents can happen.

Create a plan that includes:

- Detection and logging protocols
- Communication procedures
- Legal and compliance steps
- Incident response team responsibilities

Test your response plan regularly, especially if you're FCA-regulated or subject to financial data protection requirements.

Final Thoughts

Insider threats aren't just an IT issue. They're a business risk with legal, reputational, and financial consequences, particularly for firms in the financial services sector.

By combining technology, policies, and training, your firm can significantly reduce its exposure to insider threats, whether they're accidental or intentional.

Next Step: Book a cyber security audit tailored to financial services

At Chapman Technology Partners, we specialise in helping regulated firms protect their data and reputation through cyber-first IT support.

Book your free 15 minute intro call here and let's make sure your IT is working for you, not against you.

www.chapmantechnologypartners.co.uk

Chapman Technology Partners

Strategic IT, Cyber Security & AI Solutions
for Regulated Industries

Strawberry Fields Digital Hub,
Chorley, PR7 1PS

greg@ctpartners.co.uk
01257 542388

CYBER ESSENTIALS CERTIFIED