How To Protect Your Financial Services Company From Insider Threats
52% of organizations doubt their ability to detect a data breach through internal monitoring.¹
Insider Threats Are Gaining Traction

More than ever, employees or past employees are using their privileges and knowledge of company networks and internal workings to gain unauthorized access to sensitive financial and customer data for personal gain. With breaches making news headlines, financial services firms are continuously seeking new ways to protect their organization from insider threats.

How can financial services firms assure protection of their assets from the inside-out?
Understanding the Risks

This chapter will highlight some of the risks posed by insider threats to the financial sector. These are the most common vulnerabilities.
Risk 1: Fraud

Fraud incidents, both online and offline, have increased by more than 130% during the past year.²

Risk 2: Disclosure of Information

Customer data and their account information including social security numbers has been leaked from internal and externally-based cyberattacks.
Risk 3: Loss of Money

Among financial services firms, banks lost $16.8 billion to cybercriminals in 2017.⁴

Risk 4: Loss of Intellectual Property

Intellectual property can constitute more than 80% of a single company’s value today.³
Risk 5: Reputational Damage

It's been reported that about 20% of consumers will leave credit card companies or banks that have experienced a breach while they were customers.  

Risk 6: Destruction of Hardware

Clearly document asset inventory and properly dispose of old equipment to avoid exploitation.
Risk 7: Disruption of Critical Infrastructure

Disruptions to financial services capabilities, especially communication and payment systems, could dramatically affect global exchange processes and economic activity. 🔗
Learning From Past Financial Cyberattacks

Points of vulnerability from banking online, doing taxes online, and transferring money online all widen the attack surface for hackers. Some of the globe’s most notable threats making news headlines are helping all finance cyber professionals understand the severity of them.
Equifax Breach Impacts Over 147 Million Americans

Probably one of the most famous cyberattacks, Equifax’s failure to keep its computer systems up-to-date prompted the exposure of sensitive personal information of more than 147 million Americans in 2017.

The breach lasted from mid-May through July. The hackers accessed people’s names, social security numbers, birth dates, addresses and, in some instances, driver’s license numbers. They also stole credit card numbers from about 209,000 people and dispute documents with personal identifying information from about 182,000 people. And they grabbed personal information of people in the UK and Canada too.⁷
In 2014, JPMorgan Chase made headlines when a former employee was arrested for stealing customer data and attempting to sell it to an undercover informant for tens of thousands of dollars.

The JP Morgan data breach is considered one of the most serious intrusions into an American corporation’s information system and one of the largest data breaches in history.
Barclays Bank Customers at Risk After Data on USB Drive Exposed

Criminals gained access to a Barclays Bank USB flash drive filled with the personal details of more than 13,000 customers. The flash drive was reported to belong to a group of customers linked to Barclays Financial Planning business.
Chapter 3

Protect Your Organization from Insider Threats

Circadence empowers financial services organizations to increase their cyber security readiness levels through gamified, persistent training. Today’s approach to cybercrime needs to be proactive and preventative, not reactive. The following recommendations are just a few ways you can begin to adopt and embrace a more holistic approach that safeguards the organization at all levels.
Make insider threat awareness part of employee training

Make learning about cybersecurity attacks and mitigation strategies fun for everyone in the financial services organization from the end user to the internal staff. If well-informed employees are controlling the technologies used to monitor attacks, the better off they will be at preventing them from occurring on the inside.

While it may seem impossible to get all staff on board, tools like inCyrt™ can help train cyber and non-cyber professionals with fundamental competencies to stay safe while working.
Monitor all endpoint access

Regularly review whether employees still require remote access and/or a mobile device to do their jobs or if other means can be employed. Ensure that all remote access is terminated when an employee leaves the organization.
Continue to enforce policies and controls

Security software apps each have their own management policy and configuration requirements. Work with your HR team to implement company-wide policies for any/all employees engaging with an IT environment. General data protection, third-party access, user monitoring, and password management policies are a few to consider.
Recognize phishing attacks

Protecting your customers may seem like a no-brainer but it continues to remain a blind spot in the industry. Cyber professionals need to be able to identify when a hacker is targeting their customers with phishing scams and mitigate them. With mobile banking an ever-prevalent mechanism for financial management, teams need to identify malicious mobile apps and social media attacks before they cause damage. Gamified cyber training platforms like Project Ares® can teach individuals the latest methods and ways to prevent attacks.
Summing It Up

We understand budgets are tight and resources scarce, but your cyber security teams are, in many ways, your company’s immune system, and without the proper training to ensure their “health,” companies should expect severe losses.

It won’t be easy, but the long-term benefits will bring forth immediate value when overall business risk is managed, thanks to smart decision-making to train cyber teams on cloud-based, gamified, cyber range platforms.

Enable your cyber teams and they will thank you for it.
We’re Ready To Help Financial Services Firms Stay Protected

For a full in-depth overview and demonstration of how Circadence’s next generation learning and assessment solutions can amplify human cyber security defenses against existing and emerging threats, reach out to us.

Contact us

303-413-8800
Circadence® Corporation is a market leader in next generation cyber security readiness and training.

**Flagship Products**

**PROJECT ARES**
Gamified cyber learning platform leveraging Artificial Intelligence.

**ORION**
Custom cyber battle room builder for authentic practice and skills development.

**CyRaas**
Hyper-scalable, Cloud-based cyber range in a private, secure environment running on Microsoft Azure.
Award-Winning Cyber Readiness Solutions

4 https://bankinnovation.net/2018/05/cybersecurity-still-keeps-bank-execs-up-at-night/