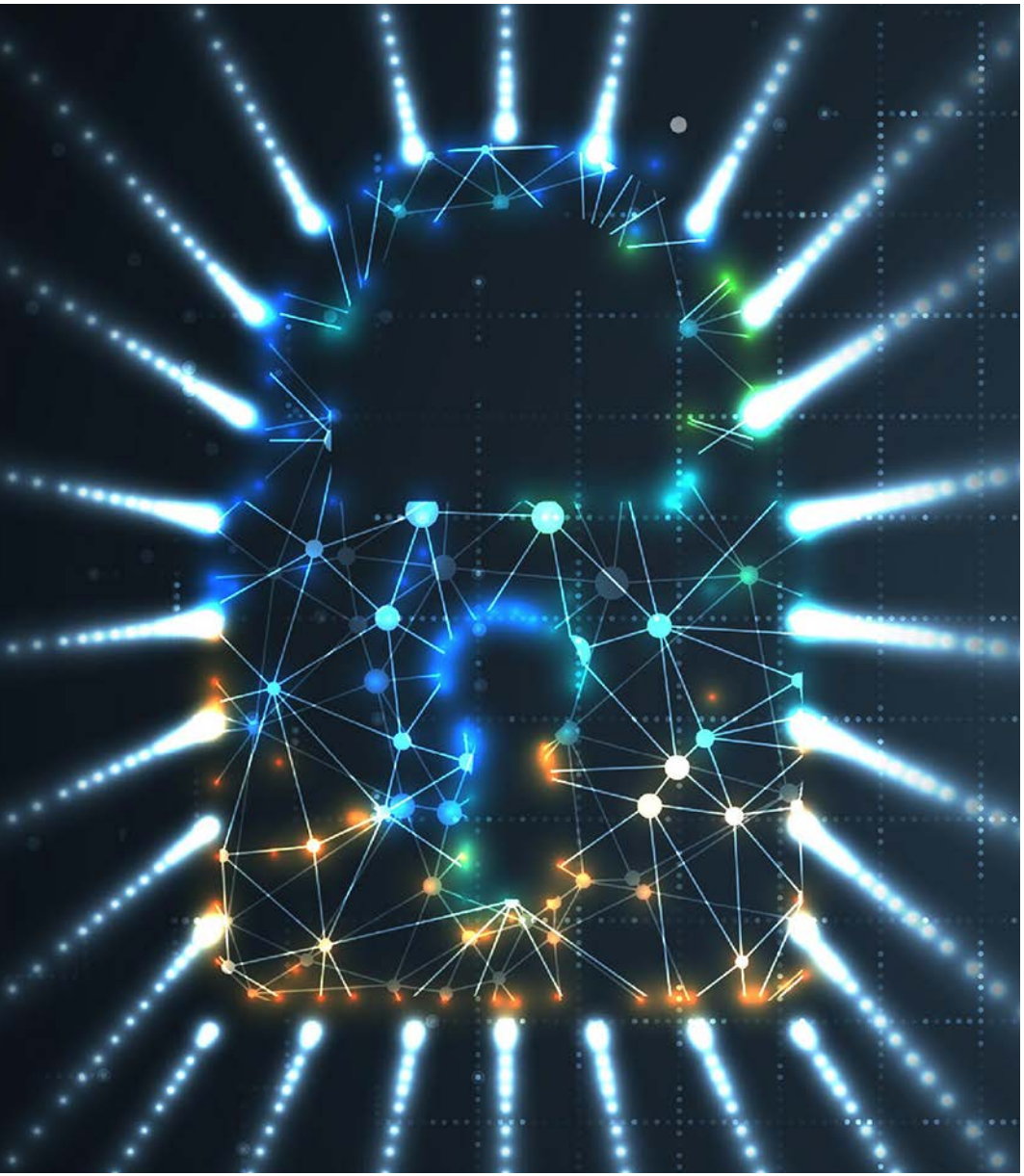
FINTECH FUTURES | REPORTS

Dataminr®

Business resilience and continuity in financial services



Introduction

From cyberattacks and economic shifts to geopolitical events and supply chain disruptions, security leaders in the financial services industry are facing a growing number of risks and, as such, must contend with a threat landscape that is ever more complex and unpredictable.

This puts increasing pressure on security leaders to ensure they have 24/7 visibility of such risks so they can protect their customers, employees, and assets.

This report considers the heightened increase in threats for financial services firms, how shifting business models (including open banking) are bringing additional security considerations, and how to establish a rapid and robust response to risks with access to the right tools, such as real-time data.

Heightened threats

Threats against financial services companies are undoubtedly increasing, in terms of their diversity, frequency, and severity, including cyberattacks, supply chain disruptions, and geopolitical tensions like the Ukraine-Russian war. Financial services companies are particularly exposed to these threats given their size and makeup; many are global and have both online and in-person customer interactions.

They are also a top target for cyberattacks, which are being carried out by increasingly more sophisticated players, including those sponsored by nation states and advanced persistent threat (APT) actors. Potential cyber risks include complex phishing schemes, ransomware, and distributed denial-of-service (DDoS) attacks. For ransomware, for instance, the financial services industry has seen a surge in attacks in the past few years, according to cybersecurity provider, SOCRadar.

> *The sophistication and scope of ransomware attacks targeting banks have grown alarmingly in recent years.*
>
> *SOCRadar*

In a threat analysis post published on July 12, 2023, it said the trend started in the first half of 2021; in the first half of 2023, ransomware attacks exceeded 2022's total.

According to SOCRadar, it is not only the frequency of attacks that is increasing. "The sophistication and scope of ransomware attacks targeting banks have grown alarmingly in recent years. From small community banks to global financial companies, no institution is immune to the risks posed by these insidious cyberattacks."

Banks' physical branch networks and digital channels are exposed to cybercrime, as are the external networks that underpin the industry as a whole, including ATM networks, domestic and international payment and messaging networks, and settlement systems.

Financial services companies are often required to open their systems to partners – including fintechs – to offer new products. These integrations are imposed by regulation, as embodied within open banking. However, increased openness means more points of potential attack. As the points of vulnerability increase, so too do the associated risks.

This can be seen in multiple successful attacks on crypto wallets, for instance. Customers are also vulnerable through standard digital interactions. In late 2021, around 790 banking customers of Singapore-based bank OCBC were targeted in a phishing scam resulting in a loss of at least $13.7 million.

A survey of 51 countries by the International Monetary Fund (IMF), published in March 2023, found that among emerging market and developing economies, most financial supervisors have not introduced cybersecurity regulations or built resources to enforce them. This included the central banks or supervisory authorities, with 56% lacking a national cyber strategy for the financial sector.

The mix of threats includes geopolitical unrest, of which the war in Ukraine is the most high-profile current example. What do such conflicts mean for businesses? What's the impact on the safety of their staff and supply chains? Their reputation, share price, and expansion plans?

In parallel, new business models, increasing volumes of data, complex value chains and growing regulatory challenges are placing more demands on the way that financial institutions go about managing operational risk.

42% of the central banks or supervisory authorities lack a dedicated cybersecurity or technology risk-management regulation.

64% do not mandate testing and exercising cyber security measures or provide further guidance.

54% lack a dedicated cyber incident reporting regime.

48% do not have cybercrime regulations.

Banks are continuing to face calls for fair and responsible banking practices. For example, in March 2022, the US Consumer Financial Protection Bureau (CFPB) broadened the focus of its Unfair, Deceptive, or Abusive Acts or Practices (UDAAP) to include anti-discrimination in consumer finance. Regulatory bodies have made it clear that this is only the first of many moves towards greater economic inclusion; therefore, organisations should take heed.

Doing so effectively while keeping pace with an ever-evolving risk landscape is a necessity.

How to respond to today's threats

An essential part of establishing a rapid and robust response to today's threats is to streamline collaboration, response protocols and critical information flows. The aim is to create real-time command and control to mitigate all types of risk and high-impact events.

Failure to do so can result in financial institutions being unable to maintain business operations when a major disruption or crisis occurs. As such, firms are shifting from subjective control assessments and increasingly adopting data-driven risk measurement and real-time detection technology and tools.

Increasingly, financial institutions are also taking an enterprise-wide, collaborative view and approach to managing risks, built on an understanding of where the risks intersect across the organisation, rather than viewing risks in isolation and managing them individually.

This includes consideration of third-party risks. Often in financial services, the corporate security teams responsible for business resilience and continuity can be small, with a number of security functions outsourced to third parties. Examples of common areas of outsourcing are security monitoring, incident response, security testing, and training. Firms need to ensure that their businesses are adequately secure when there is this sort of reliance. Those third parties themselves are exposed to all or many of the same types of operational risks.

Financial services companies must deepen their understanding of risk and ensure resilience. Waiting for regulators to appropriately identify and address new risks will leave banks at a competitive disadvantage. Ongoing awareness and assessments of a range of risks should drive proactive, not reactive, regulatory resilience across banks' global operations.

Firms need to identify critical business services and functions and, having done so, prioritize recovery and determine the necessary recovery strategies and resources. It is through identifying and planning for a variety of potential future scenarios that a firm becomes proactive when a crisis hits.

Part of the preparation will be to establish a service recovery time objective (SRTO) for each critical business service. This is vital for resource prioritization and decision making.

The exercise should include identifying and mapping end-to-end dependencies, including people (inside and outside the organisation, working on- and off-premise), processes, technology, and other critical resources.

> *"Firms need to identify critical business services and functions and, having done so, prioritize recovery and determine the necessary recovery strategies and resources."*

> *The team should then follow the crisis management plan that has been created and rehearsed for such scenarios. The goal is not to go off course or try to invent responses ad-hoc.*

Where is risk concentrated? Focus is likely to be needed where there is a concentration of people, technology and/or other necessary resources in a single country or region.

What to do when a crisis hits

Today's threats are becoming more extreme and diverse. The implications of these two forces create heightened risk, but deep domain knowledge, best practices and technology can help organizations better manage those risks.

The crisis response needs to be as efficient and optimized as possible. That means it should be tested and everyone should be familiar with it. Ideally, when activated, it can be smoothly and consistently followed.

If an event looks like it could turn into a crisis, then the security team needs to be put on standby as soon as possible. This is the first point where the benefits of early warnings and real-time alerts can become apparent.

The team should then follow the crisis management plan that has been created and rehearsed for such scenarios. The goal is not to go off course or try to invent responses ad-hoc.

A crucial way to exert team discipline is to hold meetings with all stakeholders as soon as possible. Those meetings themselves should reflect the overall ethos of having clear objectives that are then adhered to.

> *No crises will ever be exactly the same so conduct regular post-event evaluations. Review past incidents, refine response strategies and optimize your workflows for future risks.*

Set your strategic intent, articulate the goals, and ensure alignment within the team. This should be formally established and relayed via the communication channels. This should guide decision making and prioritization.

In terms of prioritization, not all tasks are equal. Identify the most important areas to focus on right now. But consider that primary efforts – unlike strategic intent – are likely to change in terms of priority and focus as the crisis evolves.

Ensure clarity of roles and responsibilities. If you have multiple global, regional and/or local security teams then it is extremely important that every team member knows their own responsibilities.

Have the courage to make timely decisions. The worst decision is to make no decision at all. Security and risk leaders will be required to make well-informed decisions in the absence of certainty.

And stay true to your company's values in your crisis response. For example, if you are positioned as a leader in customer service, make sure all your crisis responses reflect this.

No crises will ever be exactly the same so conduct regular post-event evaluations. Review past incidents, refine response strategies and optimize your workflows for future risks.

Here, we have explored ways financial services firms can ensure they are well prepared to mitigate and withstand a wide range of risks, disruptions and crises - allowing them to strengthen overall business resilience.

CASE STUDY 1
A global international bank

Find out why this global bank – with tens of thousands of employees in offices across five continents – turned to Dataminr when it realised it needed to expand the capabilities of its global security operations centre (SOC).

Read on to learn more

CASE STUDY 2
Deutsche Börse

Learn how Dataminr's real-time alerting solution, Dataminr Pulse for Corporate Security, became a "game changer" for Deutsche Börse's physical security team and the four ways its usage paid off:

1. Improved the capacity of its security operation
2. Ensured it stayed ahead of high-impact global events
3. Built credibility and trust among its senior leadership
4. Strengthened cross-functional collaboration and support

Read on to learn more

About Dataminr

Dataminr is recognised as one of the world's leading AI businesses.

The company's clients are the first to know about high-impact events and emerging risks so they can mitigate and manage crises more effectively.

Dataminr solutions are relied on 24/7 by hundreds of clients in over 100 countries across six continents to help them solve real-world problems.

Dataminr is one of New York's top private technology companies, with over 800 employees across eight global offices.

About
FINTECH FUTURES

Worldwide fintech news, intelligence & analysis

FF 40YEARS
Leading fintech media coverage

Celebrating **40 years of excellence**, FinTech Futures stands as the leading source of cutting-edge insights and resources for the global fintech sector. Our reputable platform serves industry professionals across various areas, including **FinTech**, **BankingTech**, **PayTech**, **RegTech**, **WealthTech** and **LendTech**.

Adopting a digital-first approach, we provide comprehensive coverage to keep readers informed and empowered to make knowledgeable decisions. Our extensive portfolio comprises Banking Technology magazine, daily newsletters, an intelligence library, **Banking Tech Awards**, **Banking Tech Awards USA**, **PayTech Awards** and the popular **What the Fintech? podcast** with over 1,000 listeners per episode.

Join our dedicated global community of **100k+ monthly visitors** and **25k newsletter subscribers** as we shape the future of banking, payments, and fintech together. Access a wealth of resources, including **reports**, **white papers**, **e-books**, **industry surveys**, **webinars** and more – all available for free. Our refreshed **website**, enhanced user experience and expanded digital channels offer an integrated platform for multimedia content and in-depth intelligence resources.

Explore advertising, brand awareness, thought leadership, and lead generation opportunities through our suite of products and services. Experience our commitment to digital excellence and adaptability in the ever-changing landscape. Trust FinTech Futures as your catalyst for change and growth in the banking, payments, and fintech industries, delivering well-researched, quality content to our global community.

Contact us

Sam Hutton
Head of Sales
sam.hutton@fintechfutures.com
+44 208 052 0434

Kate Stevenson
Business Development Manager
kate.stevenson@fintechfutures.com
+44 782 593 0099

Download our media kit here