Mighty Guides

Sponsored by

Trustwave®

7 Experts on Building and Maintaining Cyber Resilience

How Financial Services Firms Can Manage Risk and Sustainably Scale

Table of Contents

Introduction

The number of ransomware attacks increased tenfold over last year, and attacks like SolarWinds and Kaseya illustrated the devastating and widespread impacts of supply chain attacks on organizations of all sizes. At the same time, financial services firms are faced with another challenge—there is no playbook for navigating the scope of the digital transformations they are currently experiencing. To survive this moment, financial services companies must ensure their cyber resilience.

Financial firms are no strangers to security matters, having developed a level of security maturity that is higher than one might typically find in other sectors. They know, better than most, that resilience is the key to addressing increasingly complex threats and creating a secure foundation for sustainable, long-term growth. As their needs change, so, too, must the strategies they deploy to maintain their resilience.

This ebook explains what cyber resilience is and why it matters to financial services companies today. It also outlines the unique challenges that financial firms face in becoming resilient, discusses how they can develop effective strategies for doing so, and covers how a managed services provider can help financial services accelerate the process of building cyber resilience.

All the best,
David Rogelberg
Editor,
Mighty Guides Inc.

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

Foreword

Playing defense is a tough job, no doubt about it. With cybercrime exponentially rising and financial services being one of the most highly targeted verticals, the industry must establish stringent protocols, practices, and solutions.

Financial services organizations are no strangers to being targeted by bad actors. The lack of a standard security blueprint coupled with the ever-changing threat landscape and technology evolution can make establishing and maintaining a proactive security posture challenging and costly.

Identifying the right partner to support your organization's security goals is a critical decision. Your partner needs to understand and work with you to achieve your business goals while helping to optimize existing resources and future investments in security technology.

In this guide, we explore best practices and strategies to build and maintain long-term resilience. We also discuss the importance of rapid detection, response, and recovery from threats.

The diligent efforts of several financial industry experts, leaders in the cybersecurity space, and research into modern attack trends came together to make this guide possible. I encourage you to leverage the collected expertise to tackle your security challenges head-on.

Regards,
Steve Baer,
Field Chief Technology Officer,
Trustwave

Trustwave®

TRUSTWAVE MANAGED DETECTION & RESPONSE

INFINITELY BETTER MDR

Your security tools. Our detection and response platform and relentless experts. Integrated with out-of-box rules and up-to-the-minute threat intelligence to detect faster and respond better with automation and orchestration.

Infinite vigilance, 24x7, against cyberthreats around the globe.

www.trustwave.com

Meet Our Experts

Kory Daniels
Global Director of Threat Detection and Response Consulting, Trustwave

Spencer Ingram
Senior VP of Operations, Trustwave

Steve Baer
Field CTO, Trustwave and Trustwave Government Solutions

Erica Wilson
VP of Global Security and Privacy Risk Management, RGA

Muhammad Maad
CISO, Faysal Bank Limited

Satyajeet Rattan
VP of Cybersecurity Architecture and Engineering, Synchrony

Erik Blomberg
VP, CISO Svenska Handelsbanken

Chapter One

What Cyber Resilience Is and Why It's Essential

The need for cyber resilience has never been greater than it is today, particularly in the financial sector. Verizon's 2021 Data Breach Investigations Report shows that the financial industry still faces an onslaught of attacks from credentials and phishing to ransomware. What's more, this industry is still heavily reliant on external parties for breach discovery—whether it's via bad actors making themselves known (38% of the incidents) or notification from monitoring services (36% of incidents).

As the SolarWinds hack of 2020 made abundantly clear, financial firms must also prioritize supply chain attacks. According to the 2021 Network Security Report from Trustwave, a suspected nation-state-level cyberattack targeting SolarWinds's Orion network monitoring tool distributed malware to approximately 18,000 SolarWinds customers. The consequences were devastating, with grave implications for corporate security and national security alike.

Financial services firms must be vigilant in maintaining their cyber resilience to combat these threats. According to Spencer Ingram, Senior Vice President of Operations at Trustwave, "You should assume a threat actor is already in your environment and 'living off the land.' Proactive threat hunting supplements and reinforces existing controls and detections using the latest tactics, techniques, and procedures (TTP)." These capabilities better position financial services organizations to stay ahead of current and future threats.

Then there's the issue of scalability. Financial services companies must also maintain cyber resilience at scale as the threat landscape continues to evolve at breakneck speed.

"Cyber resilience is the business technology imperative that not only complements cybersecurity but also enables the business to operate in a manageable manner. It should be phrased as 'a way of doing business' and 'preparation for hostile activity.'"

Satyajeet Rattan
Vice President of Cybersecurity Architecture and Engineering, Synchrony

Doing so will help them better respond to unexpected events, like sudden shifts in the market or weather-related emergencies. Ultimately, resilience will help financial services firms maintain their competitive position in an uncertain world.

> **"A defender's job is extremely difficult; they need to be 'right' 100% of the time, the attacker only needs to be 'right' once."**

Spencer Ingram
Senior Vice President of Operations, Trustwave

To accomplish cyber resiliency goals, financial companies must first understand what cyber resilience means and how it determines their viability over the long term. Cyber resilience is the organizational capability to:

1. Rapidly detect threats

Financial services firms often don't even know they've been breached until it's too late. A malicious actor may make themselves known, or monitoring services may alert them to a potential incident—but the damage has already been done. By reducing the mean time to detect critical threats, financial services firms can respond more quickly and mitigate any potential impacts on digital assets or the company's reputation.

2. Rapidly respond to threats

A rapid response is essential for cyber resilience. Accordingly, financial services firms must identify the right strategies for reducing their mean time to respond to threats. This involves increasing the fidelity or expanding the breadth of their responses to certain threats by leveraging a combination of threat intelligence, tooling, and operational enhancements. For example, extended detection and response (XDR) delivers data visibility across networks, clouds, and endpoints. It also applies automation and analytics to enhance protection across both endpoints

"Cyber resilience is having the resources and capabilities to address cybersecurity threats as part of normal operations. The success criteria consist of the ability to identify, protect, detect, respond, and recover from cyberattacks with the least amount of disruption to business operations."

Erica Wilson
Vice President of Global Security and Privacy Risk Management, RGA

and environments. Security information event management (SIEM), meanwhile, provides the ability to easily cut through the noise and quickly respond to emerging threats. Additionally, a comprehensive incident response plan mitigates the impact of an attack.

3. Quickly recover from an incident

When a cyberattack arrives in full force, the consequences grow more severe by the minute. An organization's risk from a breach can include everything from the exposure of highly sensitive data and asset loss to accruing large fines and penalties. Arguably even more damaging is the potential loss of customer trust or the devaluation of their brand to maintaining business continuity. This level of resilience can minimize or avert financial losses, reduce or avoid legal or regulatory penalties, and potentially even safeguard a company's competitive market position.

4. Shift from a reactive stance to a proactive posture

Financial services enterprises cannot afford to maintain a reactive response model of security. A proactive posture allows organizations to prevent major data breaches and security incidents before they happen. One effective way to transition toward this posture is to adopt predictive analytics with high fidelity threat intelligence, which identifies hidden attackers in the environment and open threat vectors to identify hidden attackers in the environment as well as open threat vectors that can lead to a breach.

As the Biden Administration's recent executive order on cybersecurity states, companies must adopt a zero trust architecture security model that assumes a breach is likely or has already occurred. This approach decreases the default emphasis on constantly searching for the next attack and focuses the business on the most present and urgent risks to manage.

5. Mature into a stable and sustainable company

Without stability or sustainability, cyber resilience will remain elusive. A financial services company must be able to scale for growth, either geographically expanding and developing new lines of businesses or pursuing mergers and acquisitions while simultaneously remaining agile and keeping a close eye on evolving threats..

"Cyber resilience is the ability to respond to threats and events from while ensuring that the services and products remain available and operational for internal and external customers."

Muhammad Maad
Chief Information Security Officer,
Faysal Bank Limited

Key Points

- Cyber resilience has never been more critical than it is today, especially in the financial sector.
- Financial services organizations must also maintain their cyber resilience at scale in the face of increasingly sophisticated threats.
- Cyber resilience is the organizational capability to rapidly detect, respond to, and quickly recover from an incident. Shifting from a reactive stance to a proactive, stable and consistently maturing posture are vital components of a cyber resilient organization.

"Cyber resilience is an essential component of our overall operational resilience. It is mainly aimed at withstanding external cyber threats, including supply chains and insider threats."

Erik Bromberg
Vice President, Chief Information Security Officer,
Svenska Handelsbanken

Chapter Two

Cyber Resilience Challenges Facing Financial Services Firms

Cyber attackers, including financially motivated groups and nation-state actors, continue targeting financial services firms in large numbers. The connection financial institutions have to wealth—and the global economy—makes them perpetual high-value prey for malicious actors.

As businesses continue their digital transformation, the role of the financial services sector has also evolved in both the global supply chain and various third-party partnerships. Financial services companies have capital, of course, but they also possess valuable consumer data and intellectual property that cyber attackers can sell on the dark web.

> **"The financial industry has always been considered the most lucrative target. As a result, financial services have also been the most frequently attacked over the past 20 years."**
>
> 
>
> **Kory Daniels**
> Global Director of Threat Detection and Response Consulting, Trustwave

"The economy is becoming more and more digitized, especially in the Nordic countries, where cash is rare in the day-to-day economy. Therefore, cyber (security) resilience is vital. If the digital economy is severely interrupted by cyberattacks, it will immediately have huge impacts on society."

Erik Blomberg
Vice President,
Chief Information Security Officer,
Svenska Handelsbanken

The substantial bounty a financial services firm potentially offers make it both an appealing target as well as an attractive vector from a malicious actor's perspective. Rather than simply attacking a financial services firm, for example, a bad actor could potentially use a financial services firm as a means to target—or gain entry into—an entirely different organization.

Instead of just attacking a financial services firm, a bad actor may also use the financial company to target a high net worth individual or a corporate client. If a cyber criminal is able to penetrate a financial services firm's cyber defenses using a supply chain attack, for example, they may be able to access lucrative personally identifiable information (PII) or client data ranging from credit card numbers to estates or titles and beyond. From there, the cyber attacker can use that valuable information to steal funds, commit identity theft, or simply sell it to the highest bidder.

Financial services firms' cyber defense strategies and operations are critical to effectively minimize the increased risks to both their business operations and their reputations. They require cost-effective and sustainable solutions to build and maintain cyber resilience at scale. For a real example of a financial organization needing increased security after a recent merger left them with exponentially more attack surface to cover, view our case study, Banking on Trust.

"The reality of FinTech speed and innovation, coupled with threat trends (including source, motivation and modus operandi, supply chain complexity, and reliance), creates a complex mix that requires not just a cybersecurity lens but a well-defined cyber resilience glue."

Satyajeet Rattan
Vice President of Cybersecurity Architecture and Engineering, Synchrony

> You need to proactively test and validate your documented response playbooks as well as have an incident commander identified. When an incident occurs, muscle memory should take over, providing confidence to act decisively and preventing paralysis and panic. Be sure to engage nontechnical stakeholders in these playbooks.

Spencer Ingram
Senior Vice President of Operations, Trustwave

Key Points

- Financial services firms' access to high-stakes data, currency, and the global economy make them a unique target.
- Cyber attackers see financial companies not just as appealing targets, but attractive vectors too.
- Financial firms' cyber defense strategies and operations are critical for effectively minimizing increased risks.

"Financial services companies offering their products and services with resilience will gain customer trust and increased market share."

Muhammad Maad
Chief Information Security Officer,
Faysal Bank Limited

Chapter Three

Strategies for Building and Maintaining Cyber Resilience

To determine the right strategies for building and maintaining cyber resilience, financial services firms should ask themselves the following questions:

1. Have we achieved an acceptable level of resilience with respect to our organizational risk? If so, how do we know this?

Cyber resilience can look slightly different for each financial services company depending on its business model, the threat environment in which it operates, and its future plans for expansion. That said, there are a few high-level questions that most financial firms will find useful in determining whether they have achieved an acceptable level of resilience relative to their organizational risk. Is the organization able to reduce its mean time to detect and respond to relevant threats? Can it quickly recover from an incident? And, perhaps most importantly, has it made the transition from a reactive stance to a proactive posture?

2. How confident are we in the people, processes, and technology (PPT) needed to achieve the level of resilience we require?

This is a critical question for a CIO or CISO to consider. A financial services firm's people, processes, and technology are essential to the success and viability of a company's operating model. As the business grows and new threats emerge, the PPT become even more critical still. If there are weaknesses or areas for improvement in any of these PPT categories, the organization should begin identifying the relevant gaps as well as the appropriate measures for filling them.

"The impacts of remote work, sophisticated phishing schemes, challenges with addressing ransomware, and increased attacks on cloud services are top of mind for many organizations."

Erica Wilson
Vice President of Global Security and Privacy Risk Management, RGA

3. How will we achieve a scalable and agile cyber resilient operating model? What competencies, process improvements, and technologies will we need to continually scale and adapt in the future?

Once the company has established its current level of resilience and determined what their goal is, they must then create a scalable plan to achieve their desired level of resiliency. This can involve several elements along the people, processes, and technologies continuum. For example, a plan could include security awareness education, improved digital forensics and response capabilities, or specific managed security technologies that establish a strong first line of defense.

> **"Who watches the watchers? Partner with trusted third parties that use the right tools to find flaws, misconfigurations, and weaknesses."**
>
> 
>
> **Steve Baer**
> Field Chief Technology Officer, Trustwave and Trustwave Government Solutions

Attaining the level of resilience required can be a heavy lift both in terms of human resources as well as budgetary investments. This is especially true if the company is in the middle of digital transformation initiatives that result in its security and IT teams juggling multiple priorities. In circumstances such as these, financial firms may benefit from working with a managed services provider that provides the full spectrum of expertise and experience required—from high-level strategy down to day-to-day operations—to reach their desired level of resilience. A trusted partner can not only help firms build and maintain resilience but also accelerate their ability to do so.

"The threat landscape is and will become even more challenging. Security is competing with (prioritized against) digitalization/business investment to push the business forward."

Erik Blomberg
Vice President,
Chief Information Security Officer,
Svenska Handelsbanken

Key Points

- Cyber resilience can look different for each financial services company.
- Financial services firms must consider how confident they are in the people, processes, and technology (PPT) that are necessary to achieve the level of resilience they require.
- Ultimately, financial firms must transition toward a scalable and agile cyber resilient operating model if they are to meet the challenges ahead.

"There are four challenges when dealing with cybersecurity: balancing tactical and strategic focus; shifting culturally; acknowledging third-party ecosystems and dependencies; and adjusting and adapting to a continuously changing threat

Satyajeet Rattan
Vice President of Cybersecurity Architecture and Engineering, Synchrony

Chapter Four

How the Right Managed Services Partner Can Help

A strategic partnership accelerates the transition to cyber resilience. An experienced partner can help a financial services company identify the right strategies to build resilience and successfully execute them. With this in mind, consider the difference between a vendor and a partner and when it's advantageous to work with one versus the other.

A vendor can implement a technology solution or carry out specific cybersecurity functions on a transactional basis. A true managed services partner, however, can provide a financial services firm with strategic guidance and expertise as the company's requirements become more sophisticated and the threat environment becomes more complex. A financial company that establishes strong and effective working relationships with the right partner early on will also find itself in a better position to quickly recover from an incident and maintain the business continuity it needs to remain competitive.

"Bring in accelerators to minimize financial risk—individuals who've gone and done this across the industry, in organizations both big and small. That way, you can ensure the best financial return."

Kory Daniels
Global Director of Threat Detection and Response Consulting, Trustwave

"A managed services partner can be a great benefit. Having experienced, dedicated resources that are essentially an extension of an organization's cyber workforce is a winning strategy."

Erica Wilson
Vice President of Global Security and Privacy Risk Management, RGA

To fully leverage all the benefits that a strategic partnership can provide, financial companies must find the right partner for their needs. A valued and adaptable managed services partner:

1. Enables financial services firms to reduce their vendor footprint, optimize expenditures, and reduce complexity.

This can help financial companies optimize their return on investment, reduce their total cost of ownership, and gain valuable budget flexibility that they can then use to make strategic investments as needed. Streamlining the complexity associated with maintaining multiple vendor relationships also allows financial firms to become more organizationally agile.

2. Understands financial services companies' unique requirements and challenges.

A managed services partner should be able to bring deep, sector-specific expertise to bear on a financial services company's behalf. Since the financial sector has already reached a high level of maturity compared to other verticals, it's critical to have a partner that possesses a full range of mature service capabilities and expertise. A true partner can properly advise on the strategies for resilience that are best suited to the organization's unique needs.

3. Provides expert guidance on higher level strategic issues and serves as an accelerator for becoming more resilient.

If a financial company has ambitious goals for digitally transforming and expanding their global footprint, for example, it is essential to quickly build and maintain the level of resilience that makes this possible. Accordingly, financial services firms must also consider the speed at which they can realistically become cyber resilient. A valued and adaptable managed services partner accelerates this process by augmenting a firm's capabilities wherever they are needed, helping the company confidently manage the risks it faces as it transitions toward a proactive posture.

"We have just seen a cyberattack having global implications on an MSP (Kaseya). You really need to pick your MSPs with care and a long-term view, and select those who take security seriously."

Erik Blomberg
Vice President,
Chief Information Security Officer,
Svenska Handelsbanken

4. Helps financial services firms maintain resilience in an agile way as they scale for growth and the threat landscape continues to dynamically change.

Agility is central to maintaining cyber resilience, especially as a financial services firm grows. A managed services partner with a flexible portfolio can be of strategic value in this area, particularly in the context of a long-term relationship, delivering everything from specific services like digital forensics and incident response capabilities to custom advisory and consulting services that help the company maintain its resilience in a quickly evolving landscape.

"MSPs have abundant and qualified technical resources. They are more likely to acquire, train, and retain qualified resources than financial services companies."

Muhammad Maad
Chief Information Security Officer,
Faysal Bank Limited

“Managed services providers should leverage your technology with their research and prevention/detection capabilities to maximize your investments.”

Steve Baer
Field Chief Technology Officer,
Trustwave and Trustwave Government Solutions

Key Points

- A strategic partner can serve as an accelerator for developing cyber resilience.
- This partner can also help a financial services firm maintain cyber resilience as the company's requirements become more sophisticated and the threat environment becomes more complex.
- A managed services partner with a flexible portfolio can be of particular value in these cases, delivering a full range of services and capabilities that help the company maintain its resilience in a quickly evolving landscape.

"The unique value provided by an MSP is the expert capability in specific services and tools that would not be possible for individual financial services companies to attain. MSPs can deliver an end-to-end solution for their clients, which would be a challenge if they attempted it in-house."

Muhammad Maad
Chief Information Security Officer,
Faysal Bank Limited

Learn More About Our Experts

Kory Daniels, Global Director of Threat Detection and Response Consulting, Trustwave

Kory is an innovator and leader in cyber threat detection program transformation. Over the past fifteen years, Kory has overseen and supported the evolving requirements in helping organizations define, measure, and accelerate achieving their security maturity targets with fast growing midmarket firms to F500 global enterprises.

Spencer Ingram, Senior Vice President, Operations, Trustwave

Spencer Ingram, Senior Vice President, Operations, drives strategy for Trustwave customer experience and systems and processes that support the overall global business. He previously served in managed security services (MSS) leadership positions at IBM and Secureworks, where he led global teams across security engineering, operations and security information and event management (SIEM). He also worked in service desk and vulnerability management to provide service delivery to thousands of global clients, representing hundreds of millions in annualized subscription revenue.

Steve Baer, Field Chief Technology Officer for the Americas, Trustwave & Trustwave Government Solutions

Steven Baer is the Field CTO for the Americas at Trustwave & Trustwave Government Solutions. Known as just “Baer” to most, he has been in the InfoSec industry for more than twenty years, starting out in banking and ecommerce and then moving on to specialized technologies at RSA, Trustwave, and Dell-SecureWorks. He has also played pivotal leadership roles as virtual CISOs and executive sponsors and is an active participant in Infragard, The Chicago FBI Citizen’s Academy, and on the Steering Committee for the U.S. Secret Service Chicago Electronic Crimes Task Force.

Erica Wilson, Vice President, Global Security and Privacy Risk Management, RGA

Erica Wilson has more than twenty years of IT experience. She has worked in various industries including manufacturing, higher education, financial services, and most recently reinsurance. She has served in all capacities of security, including the role of Chief Information Security Officer. Erica is currently the VP of Global Security and Privacy Risk Management for RGA. In this role, she serves as a key advisor for the organization regarding technology risks and leads a dynamic team of professionals who ensure security and privacy issues are effectively addressed and managed.

Muhammad Maad, Chief Information Security Officer, Faysal Bank Limited

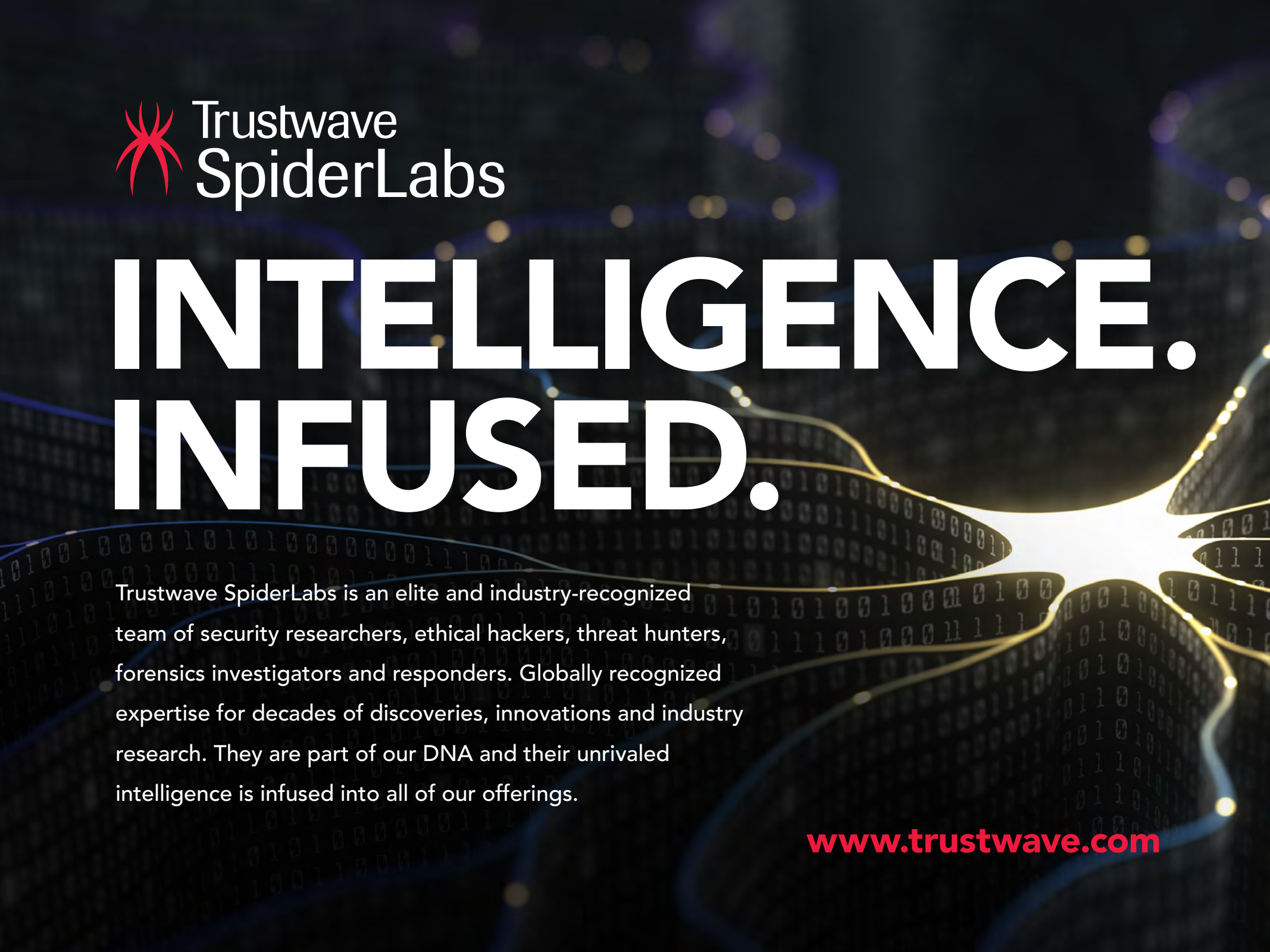
Maad is the Chief Information Security Officer (CISO) at Faysal Bank Limited. He has almost thirty years of experience within information technology, information security, and technology advisory services. Earlier in his career, he held positions as Executive Director – IT Advisory for Ernst & Young, Chief Information Officer for ZTBL, and Head of IT for HSBC Pakistan.

Satyajeet Rattan, Vice President, Cybersecurity Architecture & Engineering, Synchrony

Satyajeet Rattan brings over two decades of diverse technology experience spanning multiple industry verticals with deep expertise across technology infrastructure, enterprise architecture, and cybersecurity domains. In his current role as VP of Information Security Architecture at Synchrony, he is focused on protecting the organization and its customers from the ever-changing risks and threats in the always-connected world.

Erik Blomberg, Vice President and Chief Information Security Officer, Svenska Handelsbanken

Erik Blomberg is the Senior Vice President and CISO of Svenska Handelsbanken. He is an experienced leader who specializes in enterprise risk management, business alignment, international coordination, and security governance. Erik has worked more than twenty years in different management positions in Handelsbanken IT, most recently as head of UK IT, before being appointed CISO close to six years ago. Erik has his master's degree in computer science and worked as a consultant at Capgemini before joining Handelsbanken.


Trustwave
SpiderLabs
INTELLIGENCE.
INFUSED.
Trustwave SpiderLabs is an elite and industry-recognized team of security researchers, ethical hackers, threat hunters, forensics investigators and responders. Globally recognized expertise for decades of discoveries, innovations and industry research. They are part of our DNA and their unrivaled intelligence is infused into all of our offerings.
www.trustwave.com