opentext™

Smarter cybersecurity for Financial Services

The importance of cyber resilience in safeguarding your organization and customers

In 2020, the Financial Stability Board (FSB) warned that "a major cyber incident, if not properly contained, could seriously disrupt financial systems, including critical financial infrastructure, leading to broader financial stability implications."[2]

Industry backdrop

Financial institutions (FIs) aid businesses and are key contributors to community efforts to grow and evolve. However, their importance makes them a prime target for bad actors. They need to be properly protected, with evolving cybersecurity practices to address the financial industry's unique challenges, including the omnichannel role they play for their customers, employees, and other entities globally.

This paper explores how cybersecurity approaches are evolving to identify and protect FIs against threats to their data, applications, and systems. In the process, FIs reduce risk, preserve trust, and enhance operational resilience.

As of 2023, the average cost of a data breach in the financial industry worldwide was $5.9 million US.[1]

Cyber resilience as a core business competency

Financial Services as an industry is in the throes of digital transformation, creating opportunities for the next generation of innovations. At the same time, it's never been more critical to protect and defend an institution's most valuable data and assets, requiring a radical approach to deliver true 360-degree visibility.

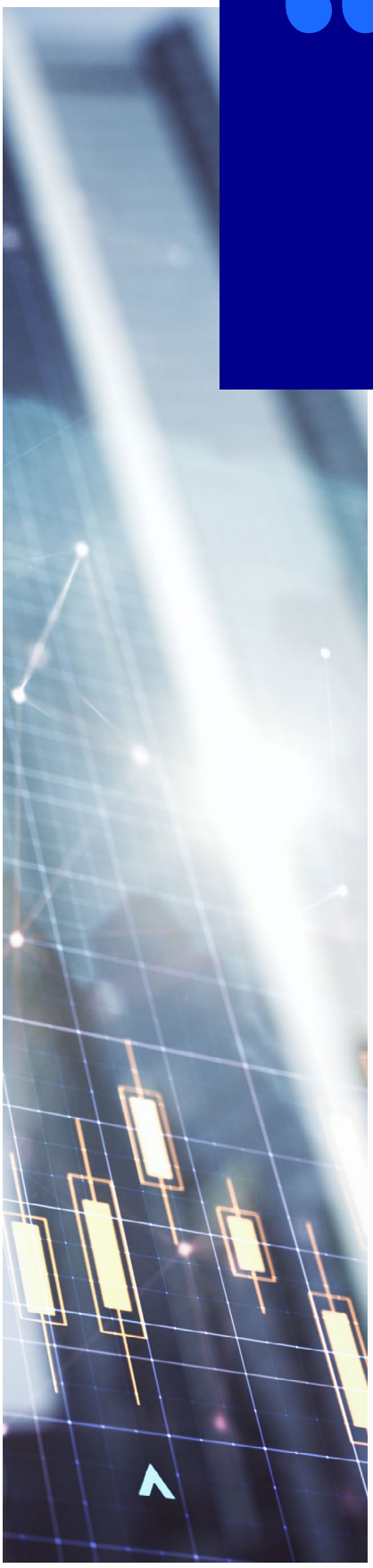
This approach focuses on the importance of the NIST Cybersecurity Framework's five functions: IDENTIFY - PROTECT - DETECT - RESPOND - RECOVER. However, it then goes a step further—embracing cyber resilience as a core business competency. This overarching discipline helps organizations ANTICIPATE - WITHSTAND - RECOVER - EVOLVE, protecting data to support customers, employees, and investors, regardless of cyber challenges.

Enhancing trust and security every step of the way

A holistic approach to cybersecurity and cyber resilience requires addressing the three pillars central to every Financial Services organization: identity and access points, data, and applications. The universal questions when assessing cybersecurity measures are: "Who has access to what when? How was access granted and for how long?" Understanding who touches data, what data is involved, from which point to which point, and the associated rights and privileges is fundamental to building cyber resilience and smarter protection.

1 Statista, Global Cost per Data Breach On Average, October 2023

2 Financial Stability Board, Effective Practices for Cyber Incident Response, October 2020



> **"We have introduced a best practice deep defense framework, including dynamic code scanning and intrusion testing, supported by documentation and training. Fortify on Demand has been fully integrated in the effort to improve the quality and, more specifically, the security of the applications we deliver to the business."**
>
> – Xavier Pernot
> IS Security Specialist, Generali France

The same is valid when it comes to data usage. Information discovery should be the first phase of the cyber resilience journey, with a focus on comprehending how data is used, by whom, for how long, and for what purpose. This requirement is captured in legislation and regulations around the world, such as the GDPR and other country- and region-specific privacy laws. However, it also provides financial institutions with a competitive advantage by reinforcing that data management is paramount.

Once the information they hold is properly discovered and understood, FIs must deploy a robust, comprehensive information management strategy. They should enhance security and trust for international transactions, credit card data, investments from customers and other financial exchanges with improved information control, encryption, tokenization, monitoring, and governance.

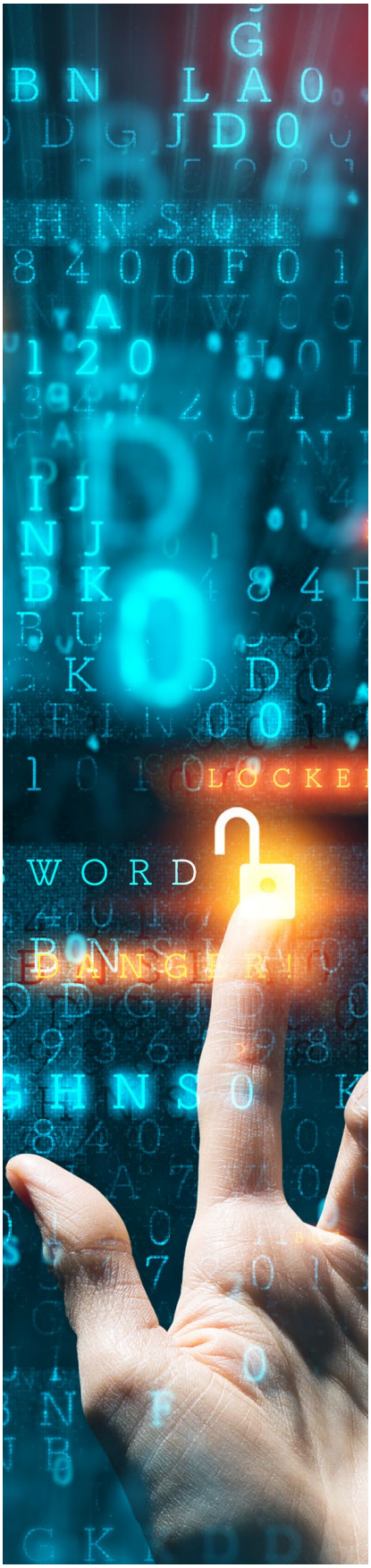
In the triad of identity, data and applications, boosting application security is imperative when hosting data, either in cloud or off cloud. A sound risk mitigation strategy must build resilience in the code of customer-facing applications. Gaps, bugs, and vulnerabilities that could be exploited must be eliminated, enhancing code security across both internal and external development processes.

Holistic and systematic threat intelligence

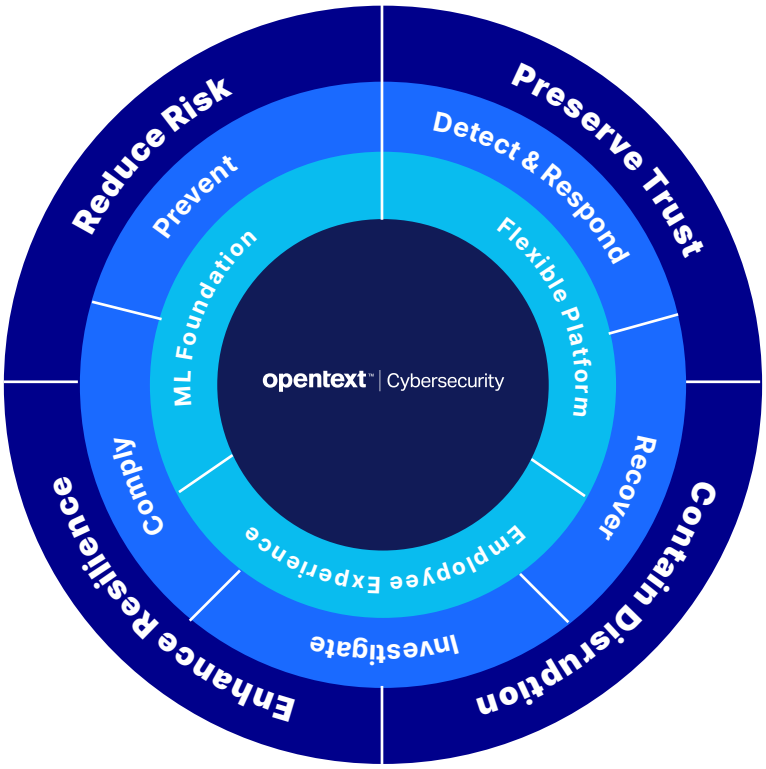
Our comprehensive approach to cybersecurity and cyber resilience is trusted by global financial institutions, with 95 percent of Fortune 500 companies relying on OpenText for information management. Our deep understanding of cybersecurity ecosystems allows organizations to take a systematic approach to protecting valuable and sensitive information.

OpenText uses proven processes, best practices, and frameworks to gather threat intelligence, metrics, and indicators to reduce the exposure factor (EF). We empower organizations to take a holistic security approach, where the sum is greater than the parts, with cybersecurity strategy and tactics delivering complete customer-focused, process-driven protection and defense.

In the challenging and changing Financial Services environment, we understand how change is tied to threat intelligence and how to address the three Vs of change: velocity, variety, and volume. In the world of Security Operations, it is imperative to use real-time data for both internal and external threats as well as leverage machine learning and AI to boost threat detection rates and identify patterns of behavior. OpenText solutions are backed by 25 years of incident response expertise, with a cybersecurity portfolio designed to reduce risk, preserve trust, contain disruption, and enhance resilience.



OpenText is trusted by governments and organizations around the world in their journeys to adapt and comply with information security, regulatory, and industry standards while navigating ever-expanding attack surfaces and security threats. We deeply understand initiatives like NIS2 (Network and Information Security 2) in Europe, and the mandated risk-mitigation approaches needed to protect the morale and security posture of a country by protecting finance systems.



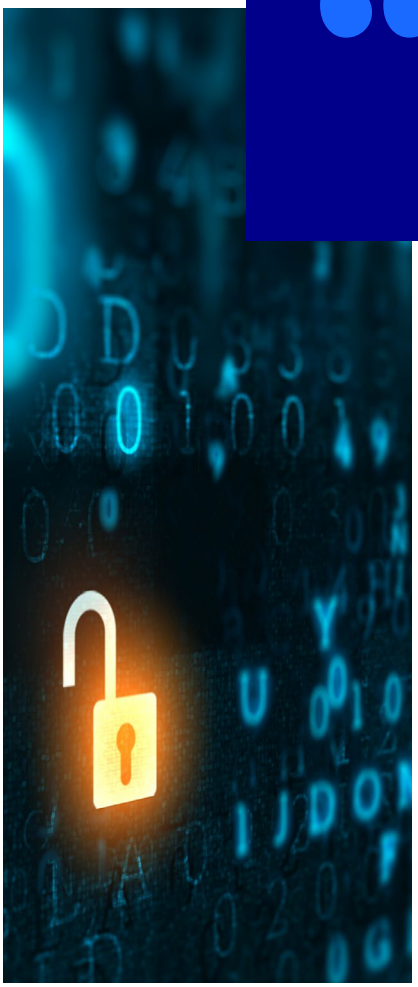
Compliance with NIST2 and other regulations requires the right combination of talent and technologies, including Identity and Access Management, Application Security, Data Privacy and Protection (encryption, tokenization, information discovery, and data governance), and Security Operations.

Building digital trust

Digital transformation continues to broaden operations for financial institutions, with omnichannel banking requiring new levels of digital trust. While trust is subjective in nature, demonstrating a solid cybersecurity approach and a commitment to maintaining digital trust, in addition to delivering innovative, reliable services, helps strengthen confidence among customers, clients, employees, and partners.

OpenText helps organizations build and maintain digital trust with a holistic, consistent, comprehensive, and end-to-end security approach across four pillars: Identity and Access Management, Security Operations, Data Privacy and Protection, and Application Security. AI and machine learning advancements are integrated into our solutions to increase security intelligence in the digital age.

opentext™



> **"By consolidating duplicate events and eliminating false positives with ArcSight SOAR, we have cut down the number of daily alerts to our SOC team by 90%."**
>
> – Emrecan Batar
> Information Security Senior Specialist, Odeabank

Our holistic approach to cyber resilience ensures interoperability with existing applications and environments—from the endpoint to the cloud, from the application to the network, and from data to information. As a result, we leave no system, platform, or application behind, providing the next generation of cybersecurity innovations to keep your organization safe and secure.

Proposed next steps

Together, let's outline a vision and identify opportunities to quickly improve your cybersecurity key performance indicators. Below are suggested next steps to ensure your cybersecurity journey is in lock step with your information management journey.

- **Introductory meeting.** Bring together your OpenText Global Account Director or Senior Account Representative with your organization's Account Business Unit CISO, VP of Security Operations, VP of Emergency Operations & Incident Management, VP of Security, and/or other security and risk management positions.
- **Joint roadmap exchange.** Hold a one-half- to full-day- long information exchange with information security and risk management leaders and OpenText to learn about your cybersecurity initiatives, current approaches, and obstacles. The team will then share cybersecurity technologies and best practices to support those initiatives.
- **Business Value Consulting workshop.** The OpenText Business Value Consulting team engages with information security teams to better understand the current state of information security business processes and to quantify the business impact of OpenText cybersecurity solutions.

Monica Hovsepian

Global Senior Industry Strategist, Financial Services

Mhovsepi@opentext.com

LinkedIn: Monica Hovsepian