Cyber Shielding in Finance: Protecting Trust in a Constantly Risky Environment

Effective strategies to prevent fraud, safeguard digital identity, and ensure regulatory compliance.

Executive Summary

The financial industry is one of the most heavily regulated sectors and also one of the most exposed to cyber threats. The growth of digital channels, the adoption of fintech platforms, and the pressure to deliver agile and seamless customer experiences have significantly expanded the attack surface. Automated fraud, identity theft, ransomware, and data breaches are just a few examples of the risks evolving alongside financial innovation.
This white paper provides a detailed analysis of recent threats and common attack vectors, offering insight into the primary cybersecurity challenges faced by banks, brokerages, and fintech companies. The focus is on the operational, reputational, and regulatory impact of these risks. It also presents practical recommendations and specialized technological solutions tailored for the financial sector, including managed detection and response (M/XDR), external threat intelligence (M/ETI), and continuous security awareness training (M/AT).

More than just informing, this paper outlines a clear path forward from a reactive stance to a proactive cyber resilience strategy. Our aim is to provide a strategic guide that empowers financial organizations to strengthen their security posture, ensure regulatory compliance, and preserve customer trust in a high-risk environment.
The financial industry does not just manage money. It manages trust. And in an environment where digital threats grow more frequent and sophisticated, that trust is constantly under attack.

Table of Contents

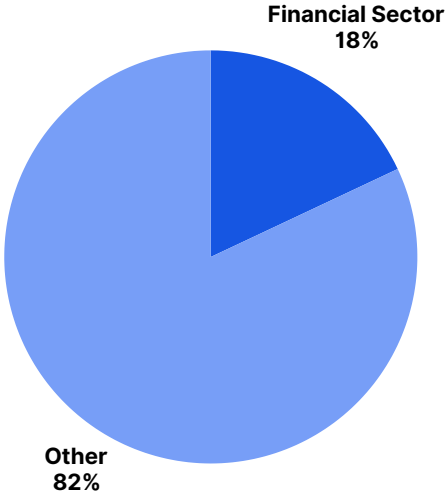
- Introduction 4
- Cybersecurity Challenges and Risks in the Financial Sector 5
- Impacts of a Cyberattack on Financial Institutions 7
- Applicable Regulations 8
- Practical Recommendations and Protection Strategies 9
- Case Study 10
- Key Benefits and ROI 12
- Strategic Conclusion 13

Introduction

Digital transformation has redefined the financial ecosystem. Traditional banks, brokerage firms and fintech companies now compete and in many cases collaborate in an environment where technology drives innovation, efficiency and reach.

However, this evolution has also amplified vulnerabilities. It is no longer just a challenge for fintechs. Banks face the task of modernizing their services on top of legacy infrastructures. Both banks and brokerage firms operate under increasing regulatory pressure and are exposed to risks targeting their digital and investment platforms.

In this new landscape, cybersecurity becomes a critical capability for sustaining trust in the financial system.



According to IBM Security's 2024 report, the financial sector was the second most targeted industry worldwide, accounting for 18 percent of all reported incidents. In Latin America, digital fraud and phishing are the most common threats, with particular emphasis on mobile platforms and real-time payment systems.

This scenario demands a renewed view of cybersecurity, not just as a technical issue but as a critical business function. Institutions must adopt a proactive approach that considers both the increasing sophistication of attacks and compliance with local and international regulations.

The purpose of this document is to provide visibility to leaders, decision-makers, and key players in the financial sector regarding the main current cybersecurity risks. It offers a comprehensive view of the threat landscape, its potential consequences, and the strategies available to strengthen organizational protection.

Why It Matters: Cybersecurity Challenges and Risks in the Financial Sector

The financial sector faces threats that combine high frequency, technical sophistication, and severe consequences. Among the main challenges are:

Automated Fraud and Identity Theft

Attackers use bots and algorithms to impersonate identities, open fraudulent accounts, or carry out unauthorized transactions. This type of fraud is growing especially within fintech platforms, where processes are highly automated. In banks and brokerage firms, these practices also appear in unauthorized SPEI transfers, point-of-sale transactions, ATM withdrawals, or identity theft on investment platforms. In addition to direct financial fraud, these activities degrade the accuracy of scoring models and generate operational noise that affects business decision-making.

Phishing and Account Compromise

Phishing remains one of the most effective techniques for stealing credentials and now appears in multiple forms. These range from targeted campaigns (spear phishing) against executives and privileged staff, to large-scale SMS-based attacks (smishing) and extortion tactics aimed directly at end users. In the financial sector, these attacks are often directed at banking executives or brokerage agents, with the goal of exploiting privileged access to internal systems such as core banking platforms or trading environments. A single compromised access point can escalate to impact high-value accounts or sensitive customer data.

Attacks on APIs and Open Architectures

The adoption of open architectures, such as Open Banking, introduces new attack surfaces. Poorly secured APIs can be exploited to extract data or manipulate operations. Innovation without proper controls can become an entry point for cybercriminals. While common among fintechs, these vulnerabilities also affect banks that integrate third-party solutions or enable connectivity with Open Banking ecosystems.

Ransomware and Denial of Service

Although less frequent, ransomware in the financial sector has a critical impact, causing operational shutdowns, data loss, and extortion with potential regulatory consequences. DDoS attacks also aim to disrupt key services. These incidents can lead to multimillion-dollar losses, regulatory sanctions, and immediate damage to customer trust. Banks face risks in critical systems such as ATMs, SWIFT, or online banking services, where any disruption directly affects both operations and customer perception.

Reputational and Legal Impact

Beyond technical damage, a security incident can lead to customer distrust, regulatory investigations, fines, or even the loss of operating licenses. In a sector built on trust, response time and transparency during an incident are critical. Such events can jeopardize partnerships, trigger penalties, and endanger business continuity. In traditional financial institutions, these incidents may also lead to regulatory audits or strain relationships with international organizations.

Risks in Critical Infrastructure and Legacy Systems

Many banking institutions still rely on legacy systems (core banking platforms, ATMs, SWIFT integrations) that do not always receive frequent security patches or updates. While these platforms are often robust, they were designed before the current era of cyber threats and can serve as entry points for advanced attackers.

Impacts of a Cyberattack on Financial Institutions

A security breach in the financial sector can trigger immediate and devastating effects across various areas of the business. Below are the main consequences an organization may face following a cyber incident:

Operational: Disruption of critical services such as SPEI transfers, trading platforms, or account access. A cyberattack can paralyze key systems for hours or even days, directly impacting banking operations and the customer experience.

Reputational: A visible incident can erode the trust of customers, investors, and strategic partners. In a competitive environment, the loss of credibility can be more costly than the attack itself.

Financial: Direct losses from fraud, costs associated with system recovery, hiring of forensic experts, compensation to affected customers, and payment of regulatory fines.

Legal: The exposure of personal or financial customer data can trigger regulatory investigations, class-action lawsuits, and severe penalties. Non-compliance with regulations such as CNBV provisions, the Fintech Law, PCI DSS, or international frameworks like GDPR may result in financial fines, operational restrictions, or even loss of licenses.

Applicable Regulations

Regulatory compliance is a core pillar in the operation of any financial institution. Cybersecurity regulations aim to ensure data protection, service continuity, and the prevention of financial crime. Among the main regulatory frameworks applicable in the Latin American context are the following. The obligations vary depending on the type of institution but are strictly enforced for both banks and brokerage firms supervised by the CNBV, as well as for fintech companies that are regulated or in the process of obtaining a license.

Law to Regulate Financial Technology Institutions (Fintech Law – Mexico)

Requires fintech companies to establish robust controls for information protection, technological risk management, and business continuity planning.

PCI DSS Standard

Mandatory for any organization that processes, stores, or transmits payment card data. Requires encryption, continuous monitoring, and vulnerability management.

ISO/IEC 27001

Although not mandatory, it is a widely adopted standard for information security management and is valued as an indicator of organizational maturity by auditors and partners. It is also key for accessing complementary certifications or participating in tenders with specific security requirements.

CNBV Provisions

For regulated institutions, the National Banking and Securities Commission requires specific information security policies and procedures, periodic audits, and incident response plans.

International Regulations

For institutions that handle international user data or operate outside of LATAM, regulatory frameworks such as the GDPR (personal data protection) or U.S. cybersecurity regulations must also be considered. These are increasingly used as global benchmarks for best practices, especially by institutions with operations or clients outside Latin America.

This is particularly relevant for many fintechs and banks with clients in the United States or Europe, as they do fall under these regulations. Non-compliance can result in financial penalties, regulatory restrictions, or a loss of credibility with customers and investors.

Practical Recommendations and Protection Strategies

Given the environment described, financial organizations must adopt a proactive and adaptable defense posture. Below are key strategies based on industry best practices, along with Banyax's managed solutions.

Continuous Threat Visibility and Detection

Implement advanced monitoring solutions such as Banyax's **M/XDR (Managed Extended Detection and Response)**. This reduces detection times from hours to minutes, allowing attacks to be contained before they escalate.

Staff Awareness

Human behavior remains the most vulnerable link. Banyax's **M/AT (Managed Awareness Training)** module provides regular training sessions, phishing simulations, and metrics to track improvements in security culture.

External Threat Intelligence

Banyax's **M/ETI (Managed External Threat Intelligence)** service analyzes open sources, the deep and dark web, and underground forums to anticipate threats before they compromise key assets. It includes monitoring for exposed credentials, executive impersonation protection, domain abuse detection, malware identification in external environments, and brand reputation surveillance on hidden platforms. The **M/ETI (Managed External Threat Intelligence)** service draws from both open and closed sources, enabling action before malicious actors can compromise critical assets or damage the brand.

Comprehensive Incident Management

Have clear protocols and trained personnel ready to respond to incidents. Banyax's **24x7x365** model provides operational support and specialized guidance throughout the entire incident lifecycle, reducing uncertainty during critical moments and accelerating operational recovery with expert backing.

Integration with Compliance

All Banyax solutions are designed to align with regulations such as PCI DSS, ISO/IEC 27001, and local regulatory requirements, making it easier to support audits, document evidence, and maintain continuous compliance without friction.

Case Study

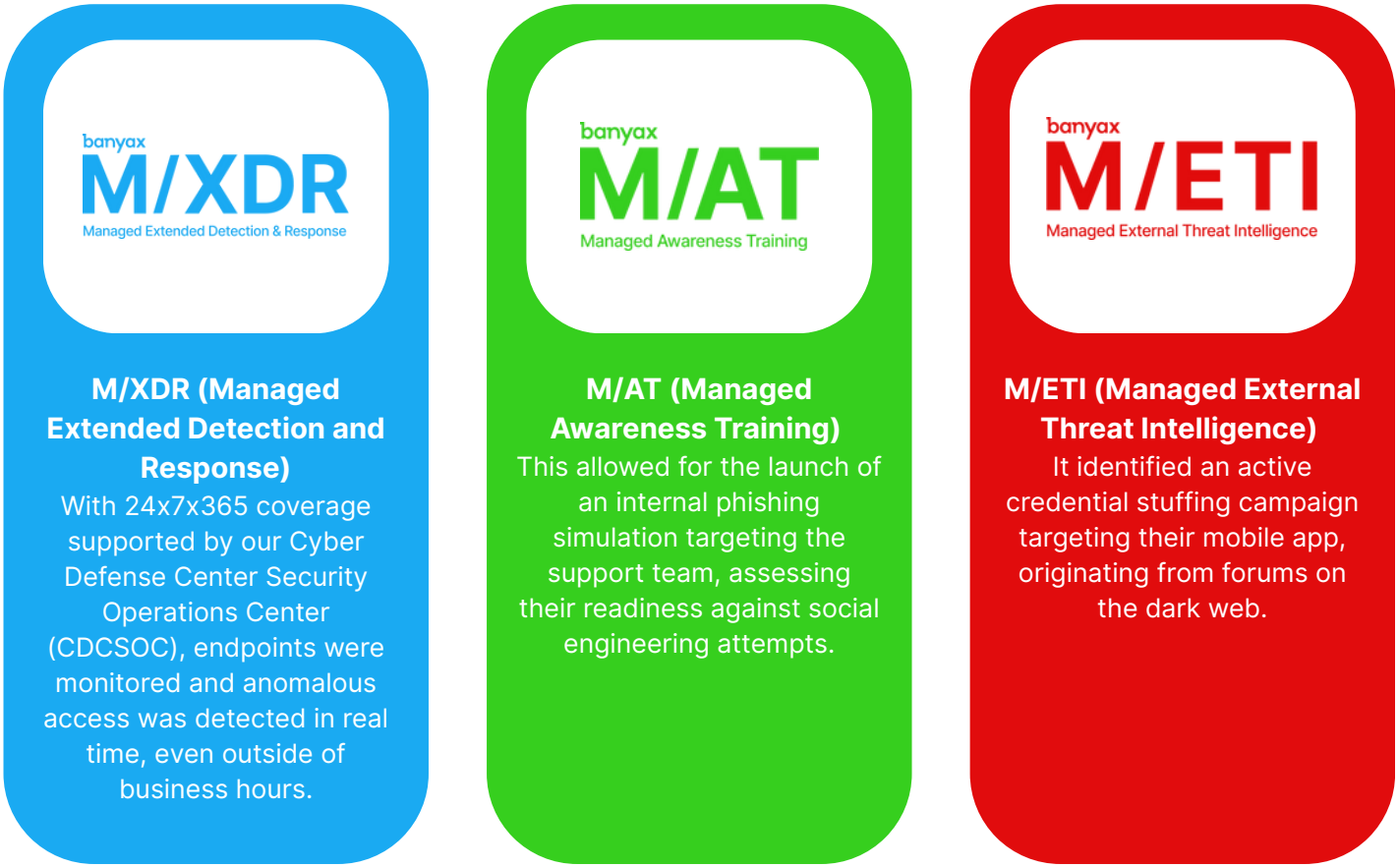
Context

A fintech specializing in digital investments detected an unusual pattern: thousands of new registrations on its platform using seemingly legitimate data, but with no subsequent activity. At the same time, the support team began receiving complaints from users about unrecognized transactions in their accounts.

What initially seemed like a minor anomaly soon revealed signs of a possible automated campaign targeting access to real customer accounts. A fintech focused on digital investments detected unusual behavior: thousands of registrations with seemingly valid data but no further interaction. At the same time, the support team reported a spike in complaints about unrecognized transactions in customer accounts.

Action

The organization activated Banyax support for an immediate and coordinated response. Three key services were prioritized for implementation:



The company implemented Banyax services, prioritizing:

banyax M/XDR Managed Extended Detection & Response

M/XDR (Managed Extended Detection and Response)
To monitor in real time and detect anomalous behavior across endpoints and access points.

banyax M/ETI Managed External Threat Intelligence

M/ETI(Managed External Threat Intelligence)
Which identified an active credential stuffing campaign targeting their mobile app.

banyax M/AT Managed Awareness Training

M/AT (Managed Awareness Training)
A targeted phishing simulation was implemented to train and evaluate the support team.

Result

14,000 automated access attempts were identified and blocked within 48 hours.

The early detection rate of suspicious access **increased by 63%.**

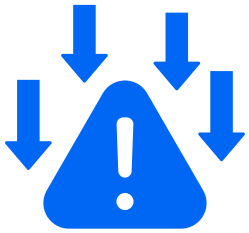
The average incident response time was reduced from **6 hours to under 45 minutes.**

The company avoided a massive data breach and submitted its compliance report to the **CNBV without any findings.**

The combination of intelligence, continuous detection, and specialized operational support prevented a public crisis, protected the institution's reputation, and strengthened regulatory trust. Speed made the difference, but strategy sustained it. A comprehensive strategy of detection, intelligence, and training not only stopped the attack but also prevented a public incident, safeguarded the company's reputation, and reinforced the confidence of the regulator. Acting in time made all the difference.

Key Benefits and ROI

The adoption of managed cybersecurity solutions delivers measurable benefits that strengthen both the operations and market positioning of financial organizations:



Reduced Risk and Exposure

- Significant reduction in critical incidents during the first months of implementation, enabled by continuous monitoring, advanced detection, and automated response.
- Protection against targeted campaigns and emerging threats through contextualized intelligence.

Operational Cost Optimization

- Reduction of expenses related to monitoring personnel and incident management through Banyax's 24x7x365 model.
- Cost optimization in monitoring and response infrastructure by migrating to a managed model (M/XDR), eliminating the need for investments in hardware, specialized personnel, and individual tools.

Improved Regulatory Compliance

- Automated reports aligned with CNBV, PCI DSS, and ISO/IEC 27001 requirements.
- Ease of both internal and external audits.

Strengthened Customer Trust

- Increased user retention by reducing fraud incidents.
- Enhanced image as a secure, prepared, and transparent institution.

Each of these benefits translates into tangible returns that go beyond loss prevention: they reinforce business continuity and enhance competitive positioning in a highly regulated and competitive environment.

Strategic Conclusion

Cybersecurity in the financial sector is no longer an isolated technical function, but a critical organizational capability that directly impacts operations, reputation, and regulatory compliance. While attacks have become more sophisticated, so have the solutions available to face them with intelligence, speed, and precision.

This document has outlined the main risks faced by banks, brokerage firms, and fintech companies, as well as the opportunities to strengthen their defenses through practical strategies and specialized technology.

With its focus on human behavior as the root of risk and its modular portfolio of managed services, Banyax positions itself as a strategic ally to face these challenges with vision and effectiveness.

In an environment where trust is the most valuable asset, financial institutions ranging from nationally operating banks to brokerage firms and emerging fintechs must make cybersecurity a strategic pillar.

Adopting an active defense posture not only mitigates threats but also builds confidence among customers, investors, and regulators. **Banyax** supports you on this path with solutions designed to protect what matters most: your organization's continuity, reputation, and trust.

Investing in digital protection today is securing your future tomorrow.

The impact of an attack can be immediate, but reputation is built over the long term.

Would you like to learn how Banyax can strengthen your organization's security posture?

Schedule your personalized Banyax demo today and discover why your organization needs a partner that turns cybersecurity into a strategic advantage.

Contact us at:
contacto@banyax.com
www.banyax.com

IBM Security. (2024). X-Force Threat Intelligence Index 2024. IBM Corporation. https://www.ibm.com/reports/threat-intelligence

PCI Security Standards Council. (2022). Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures, v4.0. PCI SSC. https://www.pcisecuritystandards.org/document_library

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. https://www.iso.org/standard/27001

Congreso de los Estados Unidos Mexicanos. (2018). Ley para Regular las Instituciones de Tecnología Financiera. Diario Oficial de la Federación. https://www.dof.gob.mx/nota_detalle.php?codigo=5518653&fecha=09/03/2018

Comisión Nacional Bancaria y de Valores. (2023). Disposiciones de carácter general aplicables a las instituciones de crédito en materia de seguridad de la información. CNBV. https://www.cnbv.gob.mx

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj