Digital Transformation
NETWORK
A Business Software Alliance Initiative

AI in Cybersecurity for Financial Services

AI Strengthening Financial Cybsersecurity

Perhaps no greater task exists for financial institutions than the need to protect assets. Worldwide, they are taking advantage of digital transformation tools to offer customers convenience, flexibility, and innovation. Simultaneously, cybercriminals are developing new ways to attack banks, insurers, and peer institutions through their digital vulnerabilities, including within their artificial intelligence (AI) infrastructure.

AI has therefore become a critical tool for Information Technology (IT) security teams. It helps avoid and path vulnerabilities, expedite threat detection, and automate timely incident responses. This is particularly relevant for the financial sector, where breaching customer data enables criminals to access funds and steal assets.

The costs are real. At US$5.56 million, financial services recorded the second highest average breach cost among industries, after healthcare, in IBM's 2025 Cost of a Data Breach Report.[1] Companies that invest in AI and machine learning (ML), and take a DevSecOps (development, security, and operations) approach are more secure when cybercriminals strike. And companies that adopt AI-enabled modern backup and recovery solutions can turn cyber incidents into challenges they are prepared to meet.

BSA member Palo Alto Networks uses "continuous discovery" to help companies across America stay ahead of their adversaries: the company blocks up to 30.9 billion cyberattacks each day.

This report explores three areas where AI is at the forefront of cybersecurity for financial services:

SECTION 1
AI Fortifies the Fortress: How AI-driven Security Operations Centre modernization is changing the game for the industry's IT security departments.

SECTION 2
AI and Cybersecurity in the Quantum Era: A look at how AI defends against AI-based attacks and look ahead to the quantum computing era.

SECTION 3
AI Versus Social Engineering: AI's power to tackle identity theft, phishing, and similar types of fraud.

"This would not be possible without AI," Wendi Whitmore, Chief Security Intelligence Officer at Palo Alto Networks, explained in a recent testimony[2] before Congress' Committee on Financial Services. "With financial institutions sitting at the center of the digital economy, the imperative for the sector should be clear: simultaneously embrace AI for cybersecurity, and cybersecurity for AI."

AI for cybersecurity refers to the use of AI systems to enhance an organization's overall security posture, while AI security is about protecting AI systems. "Maintaining trust has never been more challenging," according to EY.[3] Public officials expect financial institutions to enhance privacy protections for customers, who in turn expect their confidential information to be held securely.

This report explores three areas where AI is at the forefront of cybersecurity for financial services. First, how AI-driven Security Operations Centre (SOC) modernization is changing the game for the industry's IT security departments. Second, we dive into how AI defends against AI-based attacks and look ahead to the quantum computing era. Third, we discuss AI's power to tackle identity theft, phishing, and similar types of fraud.

SECTION 1
AI Fortifies the Fortress

Financial institutions face a daunting challenge: cybersecurity complexity. As noted in IBM's "Capturing the Cybersecurity Dividend in Banking,"[4] complexity is not just an IT issue—it is "eating bank profits." Building out IT and cybersecurity systems over decades has created a tangled web that has obscured risk and driven up costs for financial institutions around the globe.

IBM's research with 1,000 executives across 21 industries and 18 countries (including 140 in banking) reveals a stark reality: banks juggle an average of 114 different security solutions from 42 vendors. This fragmented approach not only frustrates security professionals but also hinders overall effectiveness.

For many financial services providers, platformitization, along with bringing systems together into a single cloud-based, AI-powered, Security Operations Centre (SOC) has been a game-changer. A SOC boosted by AI can detect and respond to threats faster, reduce alert fatigue for humans, and thwart attacks before they even happen. Companies that leverage AI-powered SOCs have an edge over both their competitors and cybercriminals.

AI-powered SOCs can also provide great visibility about what they are doing to protect customers' assets, while ensuring data privacy and security—something appreciated by IT teams, C-suite members, and external regulators.

DX AT WORK

paloalto NETWORKS

Freezing Out Cyberattacks at Glacier Bancorp

Glacier Bancorp, Inc. provides commercial banking services through 227 banking offices in the western United States. Because customer trust is paramount, Glacier Bancorp chose to replace its legacy antivirus solution with **Palo Alto Networks**' Cortex XDR,[5] an AI-powered detection and response app that natively integrates network, endpoint, and cloud data to stop sophisticated attacks.

Cortex XDR transformed visibility and protection, decreasing mean time to respond (MTTR) by 80%. The AI in XDR slashed false positives by 50% and clearly explains to security teams what threats are being detected. Protection was so comprehensive that penetration tests conducted by an external vendor failed.

“Very often by the time I wake up, [Cortex XDR] has already identified the zero day, updated our firewall, and is blocking the traffic,” says Sam Mauch, CISO, Glacier Bancorp. “We’re protected before we even know about it, and we’re not scrambling to get it fixed.”

DX AT WORK

IBM

From 700 to 20 Daily Security Incidents, via AI

Based in Rawalpindi, Pakistan, Askari Bank has hundreds of branches across the country. In 2021, Pakistan’s government brought in new cybersecurity rules to bring the country’s banks up to speed on a largely neglected area. Askari Bank wanted a great solution for threat detection, so the SOC team turned to **IBM** Security QRadar[6] security information and event management (SIEM), a AI-backed product that aggregates logs from various sources within a single repository.

Although stopping threats from becoming security breaches is the ultimate measure of success for a SOC, the efficiency with which it does so is also key. Through QRadar SIEM’s ability to weed out false positives, Askari Bank’s SOC has reduced the number of security incidents from roughly 700 per day to fewer than 20.

DX AT WORK

elastic

Elastic Gives Personal Capital Flexibility

With more than 3.3 million users and $22.7 billion in assets under management in the United States, Personal Capital is one of the country's leading wealth management and financial advice organizations. Personal Capital's Security Team wanted to protect the company against cyberthreats, so they turned to the **Elastic** Security solution[7] for the data management and security analysis capabilities the solution offers, including endpoint and cloud security monitoring.

The deployment of Elastic Security has dramatically decreased the MTTR to potential attacks and gave Personal Capital more flexible control over the security data lifecycle. "One of the greatest strengths of Elastic Security is its flexibility," says Maxime Rousseau, Chief Information Security Officer at Personal Capital. "We now have a unified approach to our security data and can detect issues quickly as well as meet the data conservation requirements of financial regulators."

SECTION 2

AI and Cybersecurity in the Quantum Era

AI is rewriting the rules of competition and reframing geopolitics, all while quantum breakthroughs loom on the horizon. Although the rapid deployment of AI has benefited the financial services sector, to deliver value, companies must also ensure their systems are secure and resilient.

Unlike traditional exploits that target software vulnerabilities, AI-specific attacks can manipulate the very foundation of how an AI system learns and operates. These attacks are not just about breaching a network but can also be about corrupting the AI's probabilistic logic itself. AI security therefore encompasses strategies, tools, and practices aimed at safeguarding AI models, data, and algorithms from threats.

To help all organizations, including those in the financial sector, the National Institute of Standards and Technology (NIST) is organizing the Cybersecurity Framework Profile for Artificial Intelligence—known as the "Cyber AI Profile"—to provide guidelines for managing cybersecurity risk related to AI systems as well as identifying opportunities for using AI to enhance cybersecurity capabilities.

Along with this work, BSA and its members have emphasized that the best cybersecurity includes a focus on resilience with the goal of being able to respond to the attack, and recover to a clean and trusted state.

Quantum computing (QC) promises incredible opportunities for the financial sector, but will also introduce an entirely new class of complex security risks. Quantum computers will soon be able to crack widely used public-key encryption. The BSA is therefore calling for quick adoption of Post-Quantum Cryptography (PQC)—encryption algorithms designed to be resilient to QC-powered attacks.

AI has a huge role to play in this solution. “Automated risk assessment, cryptographic inventory mapping and migration planning can significantly reduce the cost and complexity associated with post-quantum transitions,” wrote Neuracraft CEO Anshuman Yadav for the World Economic Forum.[8] Adopting PQC will help protect financial institutions and their customers from the next wave of attacks in the QC era.

DX AT WORK

EY IBM

Reducing Risk in Rio

At Banco do Brasil, scaling AI means more than deploying models. With more than 80 million customers and hundreds of AI use cases, the stakes are high. Financial institutions operate in high-stakes environments where the cost of failure is measured in lost trust, regulatory penalties, and reputational damage.

To address these challenges, Banco do Brasil collaborated with **EY** and **IBM** to co-develop a governance-first AI strategy designed to scale with confidence.[9] Integrated dashboards and automated risk assessments now provide continuous visibility into potential exposures. When model metrics breach thresholds, alerts are triggered instantly. This approach enables teams to detect risks early, take corrective action and ensure compliance in real time.

DX AT WORK

rubrik

Compliance 101 in the 305

A South Florida staple since 1926, Grove Bank & Trust is the oldest continuously operating bank in Miami Dade County. They faced issues with backups and therefore regulatory compliance; they turned to **Rubrik**, which offers AI-based solutions[10] to achieve business resilience against cyberattacks, malicious insiders, and operational disruptions.

“Rubrik helped solve our backup issues and gave us confidence that we’re set up for success going forward,” said Grove Bank’s CIO Sergio Garcia. With Rubrik’s 24/7 automated and reliable backups, Garcia and his team slept soundly despite the risk of hurricanes, as well as benefiting from increased security and compliance. “With Rubrik we have documentation to show the regulators everything they need to certify our compliance,” adds Garcia.

DX AT WORK

Ahead of the Curve on Quantum

IBM Guardium Quantum Safe[11] is software that helps companies protect encrypted data from the potential risk of future cyberattacks driven by bad actors who gain access to cryptographically relevant quantum computers. IBM Guardium Quantum Safe builds upon expertise from IBM Research—including IBM's PQC algorithms—and IBM Consulting.

"Generative AI and quantum computing provide immense opportunities, but they also bring new risks," says Akiba Saeedi, Vice President, IBM Security Product Management. "During this transformative time, organizations need to improve their crypto-agility and carefully monitor their AI models, training data, and usage. IBM Guardium Data Security Center—with its AI Security, Quantum Safe, and other integrated capabilities—provides comprehensive risk visibility."

DX AT WORK

Microsoft

Italian Flair, Powered by AI

Italy's Intesa Sanpaolo Group is a top European banking group with an unwavering commitment to leading-edge security in the face of a rapidly evolving attack landscape. When they wanted to upgrade their aging on-premises SIEM, they decided to take advantage of the AI-enhanced threat-finding capabilities of Microsoft Sentinel,[12] now enhanced by Microsoft Copilot for Security.

"Visibility is our most effective weapon against cyber 'unknown unknowns,'" says Matteo Feraboli, Group Senior Director of Cybersecurity and Anti-Fraud at Intesa Sanpaolo Group. "We adopted Microsoft Sentinel so that we could detect threats and anomalous behavior faster and more effectively than ever before."

SECTION 3

AI Versus Social Engineering

From small-scale criminal actors to nation-state backed organizations, AI is increasingly being employed in cyberattacks against financial services businesses. Criminals increasingly use social engineering[13] to manipulate people into sharing sensitive information, sending money to criminals or compromising their organizational security.

The Association for Financial Markets in Europe (AFME) and PWC UK work recently published their report AI's Impact on the Evolving Cyber Threat Landscape for Capital Markets.[14] AI empowers cyberattackers, making incursions faster, harder to detect, and more intense.

"The motivations and methods behind AI powered attacks remain familiar, but the speed and volume at which they occur have intensified exponentially," they wrote. AI-generated voices and videos can be used to impersonate customers or trusted individuals at the bank itself. AI makes phishing attempts more convincing, especially in unfamiliar languages. And AI can trick staff into following fake but plausible internal processes.

Firms can use AI-enabled security products to counter these new threats at scale. They can triage alerts by correlating threat intelligence and surfacing related activity. GenAI can create rapid incident summaries so teams can get started faster, guide investigations, and automate routine response tasks like containment and remediation. Additionally, genAI supports proactive threat hunting by suggesting queries that uncover lateral movement or privilege escalation.

DX AT WORK

OpenAI

ChatGPT Spots Fraudsters for Stripe

Stripe powers the payments of small and large businesses across the internet, expanding the digital payments universe and growing the GDP of the internet. Earlier this year, Stripe asked 100 employees to do something highly unusual: stop their day jobs and instead, dream up features and functionality for the payment platform using the newest generation of **OpenAI**'s language learning model, GPT-4.[15]

Stripe maintains a robust community on forums like Discord. However, bad actors can use these spaces to try to get critical information from community members or gain credibility with Stripe's community team.

Just by analyzing the syntax of posts in Discord, GPT-4 has been flagging accounts where Stripe's fraud team should follow up and be sure it isn't actually a fraudster trying to join in. GPT-4 can help scan inbound communications, identifying coordinated activity from malicious actors.

DX AT WORK

A Peachy Cybersecurity Setup

Georgia Banking Company (GBC) serves customers in six Metro Atlanta locations, combining the services offered by large national banks with the personalized attention of a community bank. An ambitious IT overhaul was a vital part of its ambitious goal to transition from a $600 million bank focused on mortgage warehouse lending to a $5 billion community bank focused on consumer and commercial services.

They decided to migrate to **Microsoft** Azure,[16] improve GBC's internal productivity solutions with Microsoft 365, and protect everything with Microsoft Security solutions. With an infrastructure no longer bound by physical perimeters, identity was GBC's top priority. "The attack surface is much greater than ever before because malicious actors can strike from anywhere in the world," explains Neil Natic, Chief Information Officer. "I honestly believe that the visibility possible with Microsoft 365 E5 is a must for any organization, regardless of size."

With Privileged Identity Management in Microsoft Entra, the bank can provide access to resources based on role and take access management well beyond the standard username and password. "The additional layer that we implemented both prevents accidental deletion and stops malicious actors from deleting backups in order to install ransomware," explains Natic.

DX AT WORK

okta paloalto® NETWORKS

Twice as Nice: A New Partnership for Identity Verification

Verifying who accesses data and from what device is an essential part of data protection. **Okta** and **Palo Alto Networks** are partnering to deliver a unified security architecture, enabling customers to automate threat response, secure application access on any device, and reduce security roadblocks.

"AI is supercharging attacks on user credentials, requiring a 'fight AI with AI' approach that brings identity directly into an organization's security infrastructure for a real-time and unified response," said Stephen Lee, Vice President of Technology Partnerships at Okta. Their joint AI-powered platforms will "prevent risks of siloed tools, providing nearly 2000 joint customers with a comprehensive view of their security posture, context-aware access controls, and secure authentication to stay ahead of today's threats."

DX AT WORK

okta workday.

Don’t Trust Me, I’m a Doctor

ProAssurance Group is an industry-leading specialty insurer with extensive expertise in healthcare professional liability. They know that data protection starts with identity and access management (IAM). The team started by integrating **Okta** with **Workday** to establish a single source of truth for all user identities. Everything is automatically synchronized by Okta across ProAssurance’s ecosystem of applications.[17]

With unified identity in place, new users are automatically enrolled in Multi-Factor Authentication (MFA) solutions like Okta Verify. Although certain applications require MFA every single time, Okta enables dynamic policies that reduce “MFA fatigue.” As long as users are authenticating from a trusted device and haven’t experienced significant changes in their network or location, they can continue working without disruption.

“It’s rare from a security standpoint to find a solution that’s easier for the user and it’s more secure,” says Robert Gwaltney, their Vice President for Information Security. “Those two things do not meet often, but Okta makes it possible.”

DX AT WORK

Cybersecure by the Sea at Coastal Community Bank

Coastal Community Bank was founded in Washington state in 1997 as a traditional brick-and-mortar bank, and grew over the years. In 2018, the bank’s leadership broadened their vision and long-term growth objectives. They use **Microsoft** Azure and seamlessly integrated the Databricks Data Intelligence Platform, which provided resiliency and tooling to cost-effectively deal with both data and schema at scale. Their use of Databricks has also helped them achieve unprecedented time to value. “We’ve done two years’ worth of work here in nine months,” says Curt Queyrouze, President at Coastal.

Barb MacLean, Senior Vice President and Head of Technology Operations and Implementation, believes AI has the potential to improve the system as a whole, for everyone. “How do we move beyond the minimum regulatory requirements on paper around something like anti-money laundering and truly reduce the impact of bad actors in the financial system?” By using a strong data foundation, Maclean can envision big things for her team. “Technologies like generative AI open up self-serve capabilities to so many business groups,” she says.

DX AT WORK

Cisco/Mystery Bank

A financial institution was experiencing a surge in sophisticated phishing attempts targeting its employees, potentially exposing sensitive customer data and financial systems to risk. The bank deployed **Cisco** XDR to leverage agentic AI to verify threats and execute tailored investigation plans and used AI-driven prioritization to help boost the effectiveness of security operations teams. By enabling these protections, the institution received integrated security across the network, endpoints, email, and cloud environments, thereby enabling comprehensive visibility and automated response capabilities.

This implementation improved the security posture against phishing and other cyber threats and helped to streamline compliance processes, positioning the bank at the forefront of financial cybersecurity.

Conclusion: AI Keeps Finances Safer, Worldwide

The digital transformation has revolutionized financial services, with customers enjoying an unprecedented level of convenience. At the same time, in the hands of bad actors, new technologies can equate to new threats. BSA supports NIST's work on the Cyber AI Profile and recognizes the need to manage cybersecurity risk related to AI systems. AI has potential to keeps banks, their customers, and their assets better protected in the decades ahead.

Endnotes

[1] IBM, *Cost of a Data Breach Report 2025: The AI Oversight Gap*, https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91.

[2] *Written Testimony of: Wendi Whitmore Chief Security Intelligence Officer Palo Alto Networks Before the: Committee on Financial Services*, December 10, 2025, https://docs.house.gov/meetings/BA/BA00/20251210/118735/HHRG-119-BA00-Wstate-WhitmoreW-20251210.pdf.

[3] Cybersecurity Services, EY.com, https://www.ey.com/en_gl/industries/financial-services/cybersecurity-services.

[4] IBM, “Capturing the Cybersecurity Dividend in Banking,” https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/banking-unified-cybersecurity-platform.

[5] Palo Alto Networks, Glacier Bancorp Hardens Security Without Breaking the Bank, https://www.paloaltonetworks.com/customers/glacier-bancorp-hardens-security-without-breaking-the-bank.

[6] IBM, Leaning on Automation and Analytics to Keep Cyberthreats at Bay 24x7, https://www.ibm.com/case-studies/askari-bank.

[7] Elastic, Personal Capital Protects Its Wealth Management Systems and Customers from Cyberattacks with Elastic Security, https://www.elastic.co/customers/personal-capital.

[8] World Economic Forum, “The Quantum Divide: How to Prevent a Two-Tier Global Financial System,” January 30, 2026, https://www.weforum.org/stories/2026/01/quantum-divide-two-tier-global-financial-system/.

[9] IBM, “Trust by Design: Embedding Governance into AI at Banco do Brasil,” October 24, 2025, https://www.ibm.com/new/product-blog/trust-by-design-embedding-governance-into-ai-at-banco-do-brasil.

[10] Rubrik, “Grove Bank & Trust is Hurricane-Ready with Rubrik,” https://www.rubrik.com/collections/financial-services#c_4.

[11] IBM, “IBM Advances Secure AI, Quantum Safe Technology with IBM Guardium Data Security Center,” October 22, 2024, https://newsroom.ibm.com/2024-10-22-ibm-advances-secure-ai-quantum-safe-technology-with-ibm-guardium-data-security-center.

[12] Microsoft, “Intesa Sanpaolo Accrues Big Cybersecurity Dividends With Microsoft Sentinel, Copilot for Security,” September 25, 2024, https://www.microsoft.com/en/customers/story/18745-intesa-sanpaolo-group-microsoft-copilot-for-security.

[13] IBM, “What Is Social Engineering?” https://www.ibm.com/think/topics/social-engineering.

[14] AFME, *AI’s Impact on the Evolving Cyber Threat Landscape for Capital Markets*, November 2025, https://www.afme.eu/media/ciapalr3/ai-and-the-evolving-threat-landscape-for-big-banks-afme-and-pwc_.pdf.

[15] OpenAI, “API Stripe,” https://openai.com/index/stripe/.

[16] Microsoft, “Georgia Banking Company Turbocharges Growth With Cloud Adoption and Microsoft Security,” https://www.microsoft.com/en/customers/story/1601845516735103955-georgia-banking-company-banking-microsoft-security-solutions.

[17] Okta, “ProAssurance Implements an Identity Security Fabric Using the Okta Platform,” https://www.okta.com/customers/proassurance/.

Sign up for BSA updates
dtninfo@bsa.org

The Digital Transformation Network (DTN), an initiative of the Business Software Alliance, brings together cross-sector business and technology leaders for constructive dialogue and information exchange in the areas of government regulation, public policy, and impacts to society associated with software-enabled digital transformation. Participants represent market leaders experiencing digital transformation across advanced manufacturing, automotive, consumer goods, energy, financial services, healthcare, retail, media, and telecommunications industries.

IN PARTNERSHIP WITH

Business
Software
Alliance

GLOBAL DATA
ALLIANCE

software.org
BSA Foundation

www.dxnetwork.org