

CENTRAL BANK OF EGYPT
Egyptian Banking Institute



62.432

البنك المركزي المصري
المعهد المصرفي المصري

35.715

85.204

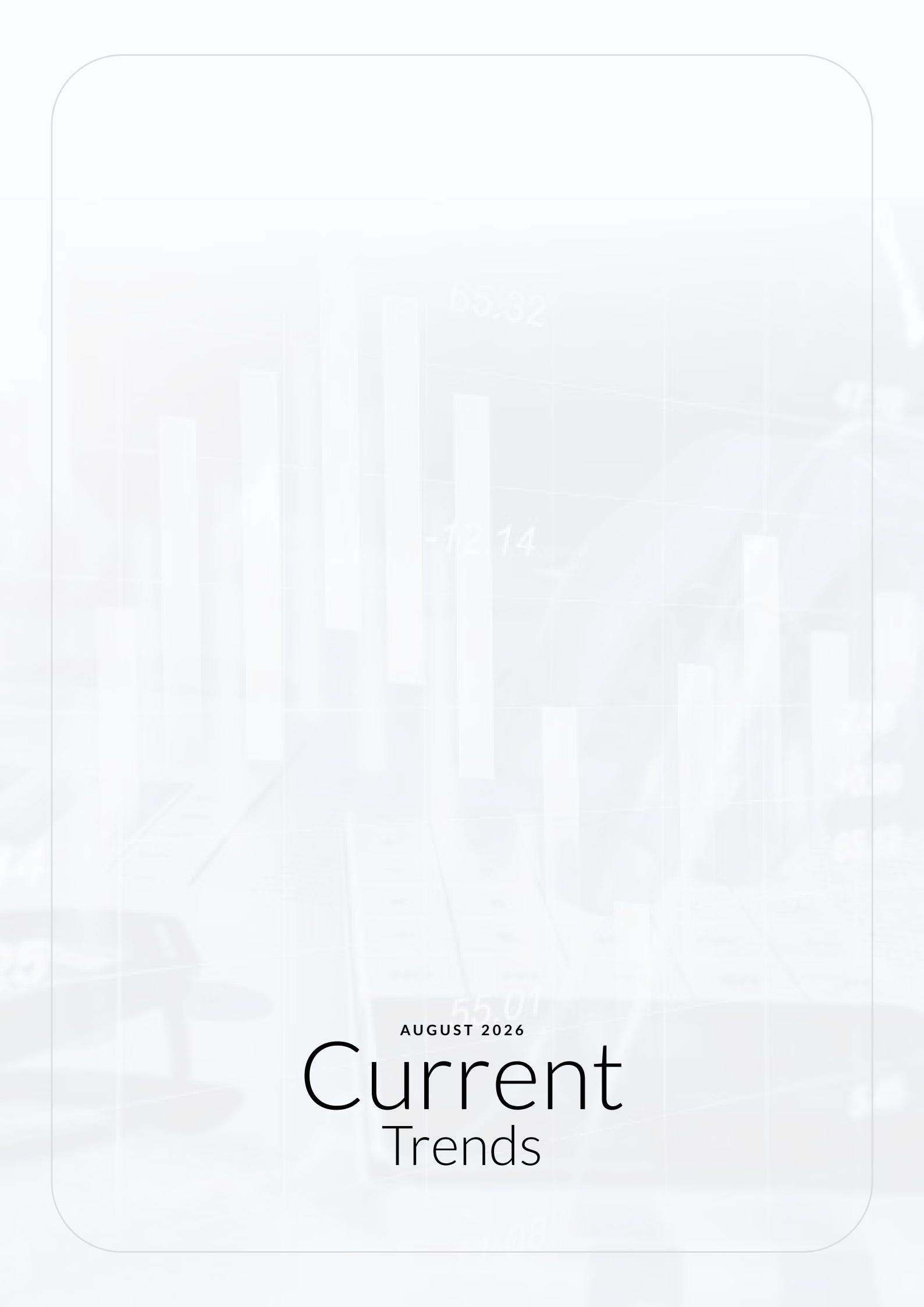
35.254

AUGUST 2026

Cyber Resilience in the AI Era

Current Trend

12.751



AUGUST 2026

Current Trends

Background

Financial institutions are increasingly transitioning to a hyper-connected, real-time payments digital ecosystem through the rapid advances of cloud computing, open banking and real-time payment, while this evolving landscape has also created new and unprecedented cyber threats. In this new paradigm, traditional perimeter defenses are no longer enough, and banks must shift their focus to cyber-resilience, taking the approach of operating, surviving and quickly recovering from attacks that are always going to happen. In this landscape, generative AI is a double-edged sword for both security teams and malicious actors, dramatically improving their capabilities. On the defense front, machine learning algorithms help Security Operations Centers identify sophisticated fraud patterns, automate basic threat hunting, and react to incidents. On the other hand, cybercriminals use automated tools to craft extremely believable phishing attacks, produce a variety of advanced malware at scale, and develop deepfakes that could defeat biometrics. In addition to traditional risks, banks are now facing new threats such as data poisoning, prompt injection, and model extraction, among others, to their proprietary AI infrastructure.

Concept and Definition

According to IBM Cyber resilience is an organization's ability to prevent, withstand and recover from cybersecurity incidents.

Cyber resilience is different from traditional cybersecurity, which is mainly about cyber defense, cyber resilience is not just about cyber defense but about ensuring the continuity of vital banking services when security measures are breached.

As AI is increasingly used in fraud prevention, customer service, payment processing, credit evaluation, and cybersecurity, banks must not only guard their digital systems but also safeguard their AI models from various forms of attacks, including prompt injection, model manipulation, data poisoning, and adversarial attacks. Modern cyber resilience is, therefore, a one-stop solution where cybersecurity and operational resilience, AI governance, business continuity and regulatory compliance are all woven together into a single strategy.

Cybersecurity vs Cyber Resilience

No matter how strong cybersecurity defenses are, there is no guarantee that an attack will never succeed. Cyber resilience is about being able to bounce back when the inevitable happens – a breach – and still run your business. It reduces the losses, builds trust of stakeholders and contributes to the sustainable survival of the organization. It improves cyber protection by providing strategies that are not only preventive, but also recovery and business continuity strategies.

Aspect	Cybersecurity	Cyber Resilience
Focus	Prevention – Defense against attacks, strong defenses around systems and data	Running operations and getting back on the business quickly after an attack, so that systems can recover.
Proactive vs. Reactive	Primary proactive approach, looking to prevent breaches and attacks before they occur.	Involves both proactive and reactive components. It anticipates incidents, reacts to them and recovers from them.
Short-term Goal	Often deals with the short-term objective of averting short-term threats and breaches.	Focuses on the long term recovery, adaptability and continuous operations even during a cyberattack.
Long-term Goal	Build a robust defense that prevents unauthorized access and protects critical systems.	Ensure rapid recovery and minimal disruption, even when attackers manage to breach defenses.

Benefits

1. Protection of AI Models as Core Institutional Assets

Cyber resilience ensures the bank's own AI models, used for credit decisions, fraud scoring, and customer interactions, are treated as protected assets, guarded against tampering, data poisoning, theft, or manipulation, rather than left exposed as unmonitored components of the technology stack.

2. A Responsible Governed AI Model

Cyber resilience embeds AI governance into the institution's risk structure, ensuring every AI system in use has clear ownership, oversight, and accountability. This gives the bank a defensible, auditable record of how its AI systems are managed.

3. Protection Against AI-Enabled Fraud

Fraud in the AI era increasingly relies on deepfakes, synthetic identities, and automated impersonation, cyber resilience gives the bank a standing capacity to withstand and recover from these attack types as they evolve, rather than depending on any single detection method staying ahead of attackers indefinitely.

4. Reduced Institutional Exposure to Third-Party AI Dependencies

Cyber resilience goes beyond the bank's own systems to cover external AI providers and platforms that the bank uses, so that a compromise or failure somewhere outside the bank's system does not quietly negatively impact the bank's operations or decision making.

Challenges

5. Faster Detection and Containment of AI Threats

With the power of cyber resilience, banks can have the ability to receive, store and analyse billions of security events, and detect suspicious activity across an attack surface that AI has made much bigger and faster moving. This reduces the time between starting an attack and the bank holding it, which means that the attack can do less harm before it can be controlled.

6. Sustained Operational Continuity Through Disruption

Cyber resilience helps in the event of a cyber incident, which allows the bank to respond rapidly, prioritize the most important threats, and restore core services with minimal downtimes. The result is the institution can continue to run instead of being forced to shut down a long time while incident response catches up.

7. A Sustainable Security Operations Function

Cyber resilience helps the bank's security teams stay updated with more alerts every day by providing a structured ability to first prioritize, investigate, and respond to the most serious alerts and to keep the Security Operations Centers (SOCs) effective rather than overwhelmed by the volume of alerts.

8. Stronger Customer and Institutional Trust

Cyber resilience secures customer confidence in the bank's ability to keep their money and information secure, which can be more easily compromised, and even more valuable, in an AI-driven world.

1. AI-Powered Cyberattacks

Generative AI enables cybercriminals to generate more convincing phishing emails, malicious code, automated discovery of vulnerabilities, and deepfake impersonations, making attacks more scalable and harder to detect.

2. Adversarial Attacks on AI Models

AI systems can be exploited by attacking them, either by poisoning the data, injecting prompts, generating adversarial examples, or evading the model to make false decisions or misclassify threats.

3. Legacy Banking Infrastructure

While many banks are still running legacy systems not originally built to handle the pace of attacks or integrate with modern security automation, this exposes them to greater operational risks.

4. Third Party Risk and Supply Chain Risk

Cloud vendors, fintech firms, AI companies, and external APIs are becoming more vital to banks. One financial institution's cyber incident can impact many other institutions at once, resulting in systemic risk.

| Practices

5. Skills Shortage

The evolving sophistication of AI-driven cybersecurity demands skilled individuals who have a strong background in AI, cloud security, cyber threat intelligence, and operational resilience. There are still many financial institutions experiencing a shortage of these specialized skills.

6. Increasing Regulatory Expectations

Regulations on AI governance, compliance with cybersecurity requirements, privacy rules, operational resilience and model risk management increase the complexity of governance within the banking sector.

HSBC

By partnering with Google Cloud to co-develop its Dynamic Risk Assessment system, HSBC successfully transformed its transaction monitoring infrastructure to achieve robust cyber resilience and proactive financial crime defense. Facing the immense operational challenge of analyzing 980 million monthly transactions across millions of accounts, the bank deployed adaptive machine learning models that continuously learn emerging fraud tactics while operating under a strict Responsible AI framework that prioritizes transparency and customer protection. The implementation yielded dramatic operational gains: HSBC increased its detection of complex financial, cut false-positive alerts by 60%, and compressed deep transaction analysis timelines from several weeks to just a few days.

For more details check this link: <https://www.hsbc.com/news-and-views/ai-views/hsbc-views/harnessing-the-power-of-ai-to-fight-financial-crime>

BNP Paribas

BNP Paribas Corporate and Institutional Banking successfully deployed a dual cybersecurity strategy to safely scale autonomous AI across its operations, supporting employees on its internal AI platform. The bank established a "Trust for AI" governance model that assigns strict digital identities, clear access boundaries, and real-time monitoring to AI tools while keeping humans in charge of final decisions. To safeguard its data, the bank hosts sensitive workloads on its own internal servers while maintaining a flexible, multi-model network with external tech partners. By using AI to speed up threat detection and automated code repair, while simultaneously applying strict guardrails to protect the AI tools themselves, the bank created a safe, resilient model for running autonomous systems in global finance.

For more details check this link: <https://cib.bnpparibas/we-govern-what-we-build-cybersecurity-in-the-age-of-agentic-ai/>

Mastercard

Mastercard's Decision Intelligence Pro platform demonstrates how financial institutions can leverage generative AI and network-wide behavioral analytics to counter the surge in AI-fueled payment fraud—including synthetic identity schemes and real-time impersonation scams—while significantly boosting approval rates for genuine transactions. By analyzing a huge amount of data points across interconnected payment networks in seconds, Mastercard enables banks to move away from rigid, rule-based systems toward real-time contextual decision making.

For more details check this link: <https://www.mastercard.com/global/en/news-and-trends/Insights/2026/ai-is-helping-banks-save-millions-by-transforming-payment-fraud-prevention.html>

PayPal

PayPal enhanced its fraud prevention system by combining graph database technology with H2O Driverless AI to detect complex buyer-seller collusion networks across millions of accounts. By mapping shared IP addresses and account connections into a network graph and processing the data through automated machine learning, the system created new predictive features that outperformed a decade of expert-engineered rules.

For more details check this link: <https://h2o.ai/content/dam/h2o/en/marketing/documents/2020/01/PayPal-Customer-Case-Study-rnd2-1.pdf>

Honeywell

Honeywell expanded its Operational Technology Cybersecurity Suite to protect critical infrastructure across manufacturing, energy, and industrial sectors from sophisticated cyber threats. The portfolio features the artificial intelligence powered Cyber Proactive Defense platform, which uses real time analytics to correlate system alerts and stop threats before they cause operational downtime. Additionally, Cyber Governance Risk and Compliance leverages machine learning to automate compliance reporting and evidence collection, significantly reducing administrative workloads.

For more details check this link: <https://www.honeywell.com/us/en/news/press-releases/2026/06/honeywell-strengthens-ot-cybersecurity-suite-for-resilience-against-next-generation-of-industrial-cyber-threats>

August 2026

Current Trends

HOTLINE
15200
One number to better serve you!

Headquarters – Nasr City
22 A, Dr. Anwar El Mofty St., Tiba 2000
P.O.Box: 8164 Nasr City, Cairo, Egypt

www.ebi.gov.eg



Like us on
facebook.com/EgyptianBankingInstitute



Follow us on
twitter.com/EBItweets



Join us on
linkedin.com/company/egyptian-banking-institute



Watch us on
YouTube Channel: Egyptian Banking Institute (EBI)