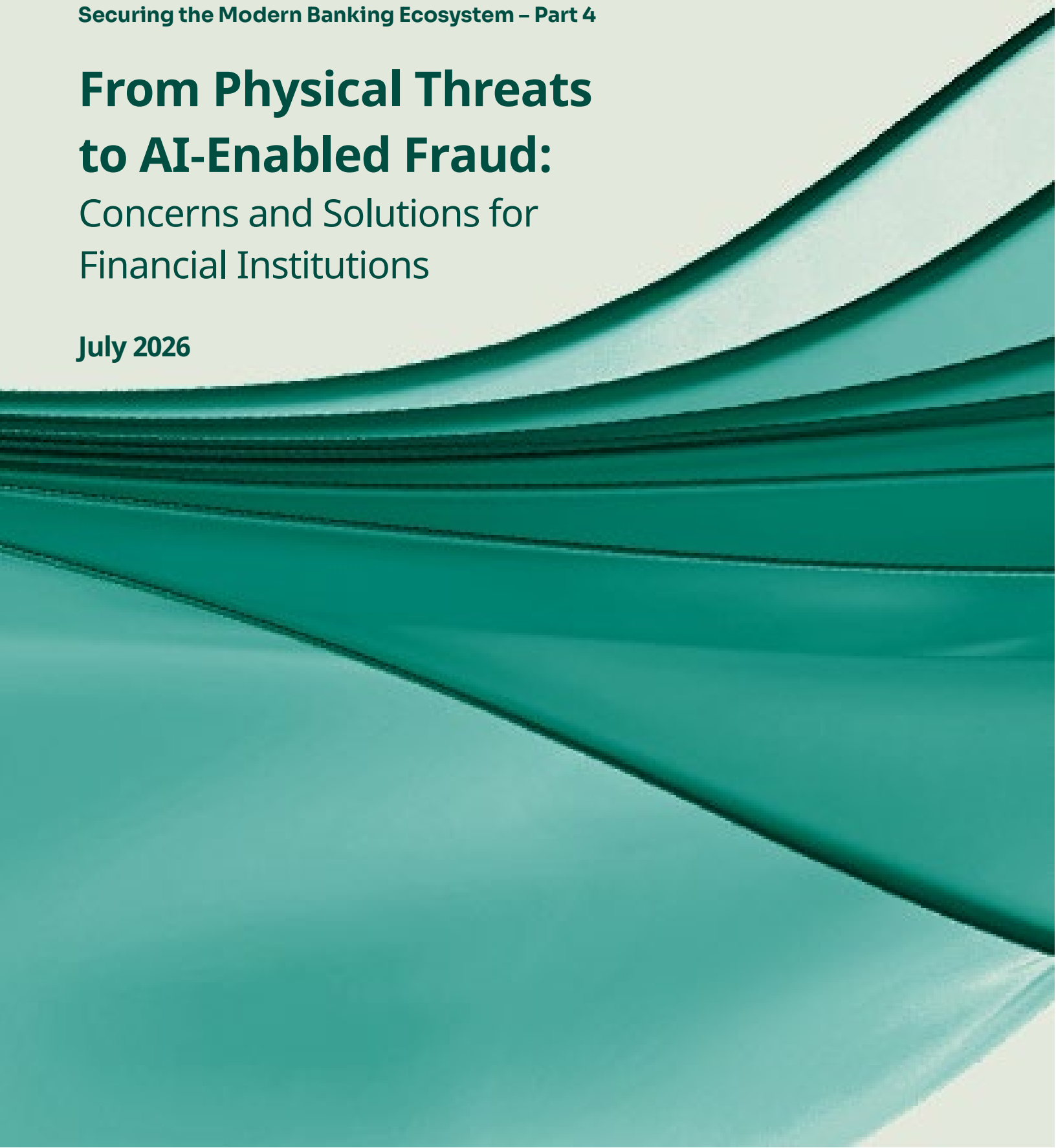


Securing the Modern Banking Ecosystem – Part 4

From Physical Threats to AI-Enabled Fraud:

Concerns and Solutions for
Financial Institutions

July 2026

A large, abstract graphic on the right side of the page. It features several overlapping, wavy, curved bands in various shades of teal and blue, creating a sense of depth and movement. The bands curve upwards from the bottom left towards the top right.

From Physical Threats to AI-Enabled Fraud:
Concerns and Solutions for Financial Institutions

Table of contents

Executive summary 2

Risk management 3

Governance & human behavior..... 7

Final summary 11

Executive summary

Banks and ATM deployers face a convergence of physical crime, AI-driven social engineering, supply-chain fragility, as well as governance and behavioral gaps. The security landscape for Financial Institutions remains volatile and at times challenging.

In March, NCR Atleos and Trellix joined forces to host our first security summit at Abertay University Cyber Quarter in Dundee. By bringing together industry security experts, Financial Institutions and experts in cyber and fraud academia we collectively asked questions and discussed real-time challenges on how to stay ahead of fraud and cyber-attacks both aimed at the banking industry and beyond. We highlighted reporting frictions (e.g., data-sharing concerns under GDPR), over-reliance on reactive controls, and complex incidents that can often stretch resources for lengthy periods of time.

This white paper is one of four produced which outlines the key outputs from eight concern areas and the discussions that followed along with some key conclusions.

As the final white paper in the series, it spotlights risk management and the impact of human behavior and security.

Trust & Threats The Shift in Physical Attacks Responsible Finance	Operational Resilience Disaster Recovery Supply Chain Security
Securing Tomorrow AI-Driven Phishing & Social Engineering Evolving Attack Vectors	Covert & Coercive Risk Management Governance & Human Behavior

Risk management

The role of cross-functional security governance

Effective ATM logical security cannot operate in isolation. The team quickly identified that within any organization there should be a cross-functional security council: a team of experts from multiple areas of a business that meet regularly to monitor emerging threats, analyze customer-facing issues, and coordinate defensive actions.

This multi-disciplinary approach provides key advantages:

- **Shared situational awareness:** Logical and physical security teams can compare patterns in any malware attempts, man-in-the-middle attacks, physical tampering to help understand attacker behavior holistically.
- **Prioritization of mitigations:** By aligning across domains, the organization can assess which threats require immediate intervention and what should be incorporated into longer-term product strategy.
- **Faster response cycles:** The council functions as a decision-making forum that can halt releases, trigger escalation to senior leadership, or coordinate remediation plans.

This approach emphasizes that ATM security is not strictly a technical function; it requires an organizational structure capable of absorbing and acting on diverse threat signals.

Current state of logical security: predominantly reactive

Developers and security specialists note that many security controls occur after code is produced, including vulnerability scans, dependency checks, and compliance reviews. These checks may identify previously unknown risks, especially from third-party or open-source libraries introduced during development.



Key observations:

- **Security checks:** Addressing security late in the cycle creates scramble periods where teams rush to fix issues before release.
- **Dependency risks are unpredictable:** For example, a library that appeared safe earlier in the year may later be found to contain critical vulnerabilities.
- **Time allocation for remediation is inconsistent:** While mechanisms exist to delay releases, they are not universally understood or used by all developers.

This reactive posture increases the risk of vulnerabilities entering production and highlights the need to integrate security earlier in the engineering lifecycle.

Moving toward shift-left security

Although an organization aspires to more proactive security, it was highlighted that implementing true “shift-left” practices remains challenging. Developers report that:

- **Requirements often lack security clarity,** making it difficult to anticipate risks before implementation.
- **Agile ten-day sprint cycles encourage incremental release readiness,** yet don’t always leave room for deeper security assessment.
- **Unstructured reliance on open-source components** means teams may lack visibility into versions, vulnerabilities, or long-term maintenance concerns.

To move toward a shift-left model, the security function must provide:

- Dev Early-stage threat modeling
- Mandatory secure coding standards
- Integrated dependency intelligence and automated scanning
- Security-specific acceptance criteria for each sprint

This ensures security is not a final gate but a built-in expectation throughout development.

Enhancing transparency and breaking down silos

One of the strongest developer-driven recommendations is the need to break down silos, particularly around:

- Understanding the provenance and security history of open-source libraries
- Collaborating across teams to validate assumptions
- Making hidden risks visible earlier in the lifecycle

Developers expressed interest in:

- Having more time to investigate library versions and known issues
- Better mechanisms to share information on approved dependencies

- Greater participation in upstream open-source communities, both to contribute and to understand evolving risks

This shift would encourage a culture where security is a shared responsibility rather than a downstream checkpoint.

Continuous monitoring: a necessity for ATM logical security

During the summit, it was emphasized that ATM security is never a “one-and-done” exercise. Threats evolve constantly, and even well-vetted components can become vulnerable as new attack techniques emerge.

For ATM environments, where systems often remain in the field for many years, continuous monitoring and regular revalidation are essential. This includes:

- Automated vulnerability scanning
- Runtime integrity validation
- Behavioral monitoring for anomalies
- Continuous review of threat intelligence

Logical security must therefore be treated as a lifecycle activity spanning development, deployment, and in-field operation.



In conclusion

ATM logical security is evolving in response to increasingly sophisticated threats, growing software complexity, and the expanding use of third-party and open-source components. The insights from the discussion reinforce that while strong technical capabilities exist, the organization's most significant opportunities lie in earlier integration of security, greater cross-functional transparency, and continuous oversight across the full software lifecycle.

Equally important is maintaining and strengthening cross-functional governance structures such as forming a security council, which play a critical role in unifying physical, logical, fraud, and operational security perspectives. This collaborative model ensures the organization can anticipate threats, prioritize risks, and respond swiftly when vulnerabilities are identified.

Finally, as the threat landscape continues to evolve, ATM logical security must operate as a lifecycle discipline rather than a milestone. Continuous scanning, monitoring, threat intelligence, and revalidation are essential to maintaining long-term system integrity, especially in environments where software and hardware remain deployed for many years.

Together, these practices support a more resilient ATM ecosystem, one capable of defending against modern threats, reducing operational risk, and aligning security more closely with product development and organizational strategy.



Governance & human behavior



In a landscape where individuals are often portrayed as the weakest link in security, the team adopted a different perspective by challenging that humans are, in fact, essential to sustaining strong security foundations within the broader ecosystem. Without human judgment, analysis, and decision making, business requirements cannot be effectively translated into the security policies that underpin today's FinTech operations.

It is business leaders, through a top-down approach, who establish the standards that guide organizational behavior. Key insights from the discussions underscored culture as the central element in fostering secure practices:

- **Employee integrity:** Employees generally act with good intentions but may, knowingly or unknowingly, engage in improper actions. Creating an environment where individuals can report concerns with integrity—without fear of reprisal—is essential to enabling transparent and responsible behavior.
- **Leadership beyond the C-suite:** Employees are more inclined to trust and follow the guidance of the managers they interact with daily rather than C-level executives who may operate remotely or from different offices altogether.
- **Security vs. speed:** In environments characterized by continuous deployment and rapid delivery cycles, convenience often outweighs the time required to fully understand organizational policies. It highlights the need for cultural reinforcement to ensure security is an instinctive priority, not a secondary hurdle.
- **Shared accountability:** While leadership sets the tone for a secure culture, every employee shares responsibility for upholding the organization's security posture through their daily actions and decisions.

The discussion emphasized that a strong security culture relies on employee integrity, everyday leadership influence, and balancing rapid delivery pressures with adherence to organizational policies.

Policy creation

Governance is a continually evolving landscape; policies cannot be written once and left unchanged for years. As technologies, legal requirements, and industry standards shift, internal governance must remain responsive and adaptable.

Key observations within the team included:

- **Knowledge gap:** Although governance is a critical component of business operations, there is a shortage of professionals with the expertise to craft clearly defined, high-quality policies. As a result, organizations often purchase prewritten policies or rely on automated tools, such as AI-based generators, to create them.
- **Insufficient time:** With new advancements emerging at an increasingly rapid pace, governance functions often struggle to keep up. This lag can result in significant gaps—sometimes spanning years—before updated approaches are implemented to maintain security.
- **Hidden policy content:** Essential information that employees need is frequently buried within lengthy policy documents. Important guidance may appear 20+ pages into a document, written in dense language that is difficult for employees to interpret or act on.

“The human factor is real, people need to be able to follow guidance easily.”

Jason Daniels

ATM & Cash Services Nationwide Building Society



Overall, the team concluded that effective policy creation requires specialized expertise, timely updates, and accessible content to ensure governance keeps pace with organizational needs and evolving security demands.

Insider threats

Another critical element discussed was insider threats. Even within organizations that foster strong security cultures, insider threats remain an inherent risk. The team identified several key areas of concern:

- **Accidental data disclosure:** Even well-trained and compliant employees can unintentionally expose sensitive information through simple mistakes or oversight.
- **Disgruntled employees:** Individuals who become dissatisfied or resentful may engage in malicious behavior, intentionally assisting attackers or bypassing established security controls.
- **Coercion:** Any employee may be vulnerable to bribery, intimidation, or blackmail, potentially compelling them to act on behalf of criminal groups.

While even the most robust policies cannot fully prevent insider threats, they play a critical role in establishing accountability and enabling the collection of evidence necessary for potential legal action. However, by the time such measures come into effect, reputational damage may already have occurred, often with consequences that extend far beyond financial loss.

Building a human-centric security future

Although humans are often characterized as the weakest link in security, the team's discussions demonstrated that people are, in fact, central to addressing the challenges identified. Effective solutions arise from designing security practices around human behavior rather than solely around systems, with the following recommendations emerging:

- **Create concise accessible policies:** Develop shorter, clearer policy documents that present essential information upfront, rather than burying critical guidance deep within lengthy text.
- **Empower team leaders to set the standard:** Focus on immediate managers as key drivers of security culture. Employees place greater trust in the leaders they interact with daily, making a solely top-down, level-driven approach less effective.
- **Maintain clearly documented decision evidence:** Ensure that the rationale behind security decisions is well defined and recorded, enabling transparent reference and supporting continuous improvement efforts.



In conclusion

People—not systems—sit at the heart of every effective security strategy. While technology, governance frameworks, and formal controls provide essential structure, it is human judgment, accountability, and culture that ultimately determine how securely an organization operates. Strengthening security, therefore, requires more than updating tools or drafting new policies; it demands designing processes that reflect how people work, lead, and make decisions.

By recognizing the realities of human behavior, both its strengths and risks, a clear path forward has been identified; grounded in clarity, trust, and shared responsibility. Shorter and more accessible policies, empowered frontline leaders, and transparent decision-making processes form the foundation of a more human-centered security model. At the same time, acknowledging insider threats underscores the importance of vigilance, accountability, and cultural resilience.

Taken together, these insights point toward a security future built not around viewing humans as liabilities, but as essential partners. By aligning governance, leadership, and policy design with the way people actually think and act, organizations can create security practices that are not only stronger, but sustainable, adaptable, and truly embedded into everyday operations.



Final summary

This white paper highlights how financial institutions are facing a rapid convergence of physical ATM attacks, AI-enabled social engineering, and growing governance and human-behavior challenges, all intensified by regulatory and intelligence-sharing barriers. It argues that rising threat sophistication demands a shift toward ecosystem-wide collaboration, earlier security integration, and human-centered governance to build long-term resilience. Ultimately, securing the modern banking landscape requires coordinated action across technology, regulation, and culture.

Thank you to everyone who took part in the cyber summit sessions, for their willingness to participate, contribute, and collaborate so openly throughout the discussions.

