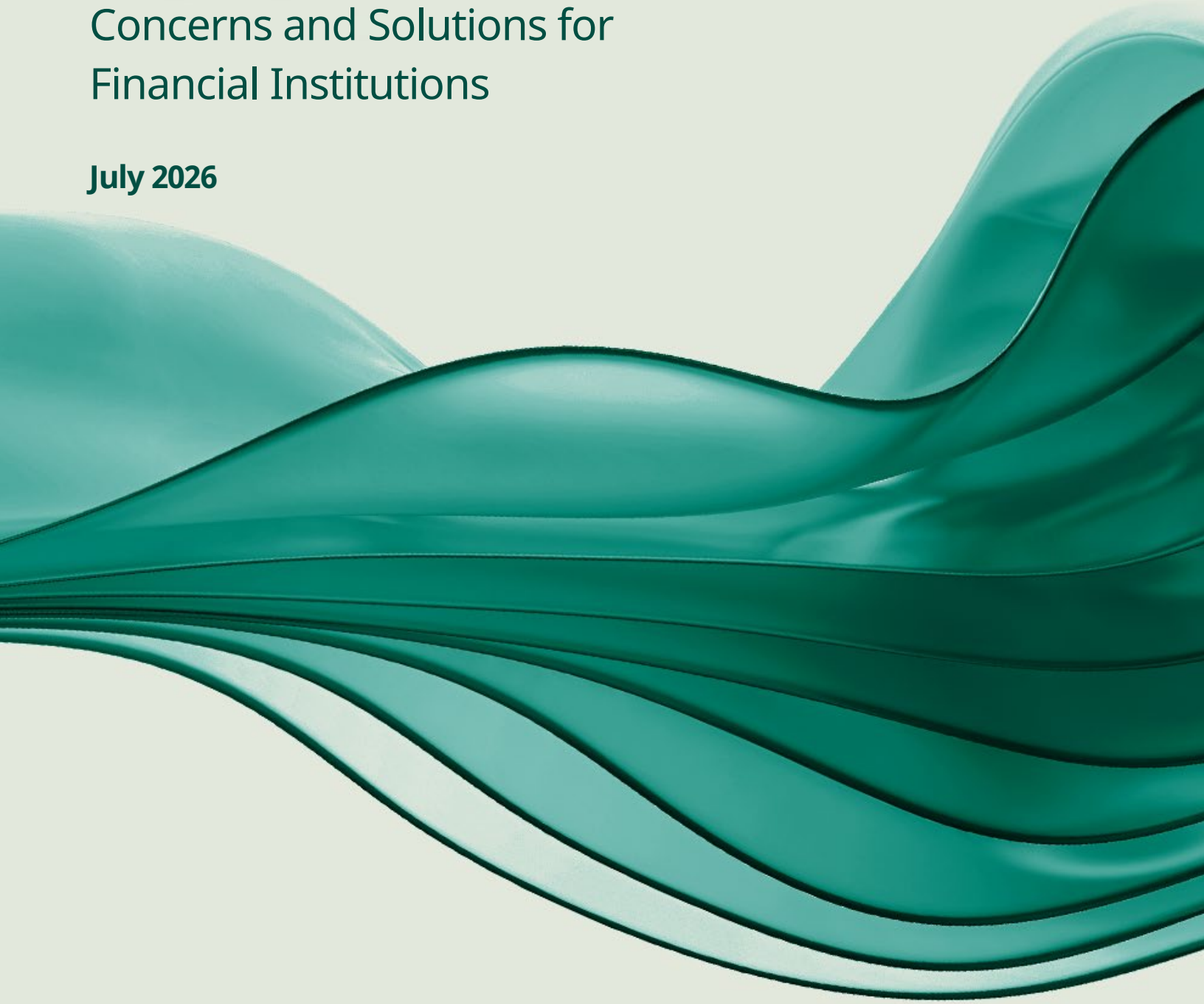
NCR ATLEOS | Trellix

Securing the Modern Banking Ecosystem – Part 2

From Physical Threats to AI-Enabled Fraud:

Concerns and Solutions for Financial Institutions

July 2026



NCR ATLEOS | Trellix

July 2026

From Physical Threats to AI-Enabled Fraud:

Concerns and Solutions for Financial Institutions

Table of contents

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.

In the second whitepaper we move our focus towards Operational Resilience, more specifically disaster recovery and security in the supply chain

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

Disaster recovery

Disaster recovery and operational resilience remain inconsistent across organizations, with many lacking fully tested, evidence-backed plans capable of handling real-world crises. This section examines key vulnerabilities across the FinTech ecosystem and highlights the importance of industry-wide collaboration to strengthen collective resilience.

Gaps in planning and testing

The team immediately recognized that fully developed disaster recovery plans are uncommon. In many organizations, existing plans fall short of preparing teams for a real scenario in which operations come to a complete standstill. Key concerns raised included:

- Plans are created primarily to satisfy audit checkboxes, rather than to support effective crisis responses
- Plans are not fully tested, leaving organizations unprepared for genuine, large-scale breakdowns.
- Review cycles are too infrequent, meaning plans become outdated and misaligned with evolving risks.
- Plans may be inaccessible during technology outages, highlighting the need for maintained hard-copy versions.
- Businesses are not taking into account their partners and vendors when making plans, making sure they are contactable when all systems are down and that person can be authenticated.

Collectively, these issues underscore the need for disaster recovery plans that are practical, regularly tested, and accessible—even in worst-case scenarios—rather than merely reliant on digital copies.

Evolving risk landscape

As technology continues to advance, the risks facing businesses evolve just as rapidly, requiring organizations to continuously reassess and remodel their threat assumptions. As these risks shift, both the tools used to manage them and the experience of those operating them must keep pace. The discussion highlighted several key areas of concern:

- Crisis tooling is often outsourced without sufficient hardening, creating identity and segmentation weaknesses that can become critical single points of failure.

- Industry risk modelling is not adapting quickly enough, leaving organizations misaligned with the realities of modern, rapidly changing threat environments.
- Plans frequently prioritize systems over people, overlooking the real-world risks faced by field teams—including coercion, violence, and severe weather—and raising broader questions about how we protect employees, customers, and the wider community.
- The wide range of tools and frameworks in use across organizations makes it difficult to establish a single, consistent industry standard during a crisis.
- There was no clear consensus on which indicators should be used to measure an organization's resilience strategy.

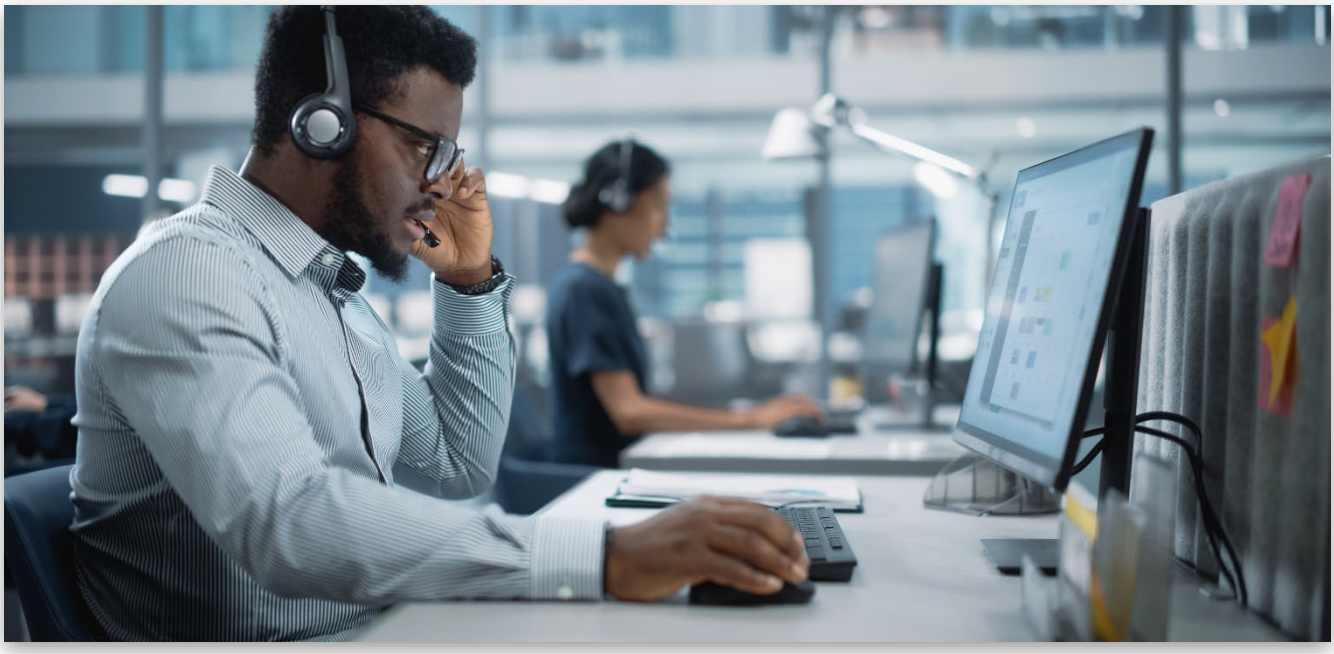
Regulation requires banks to reimburse customers who fall victim to fraud, offering essential consumer protection. Yet this introduces a **moral hazard dilemma**:

- If consumers assume banks will always refund losses, risk-taking may increase.
- Banks argue this undermines personal responsibility and increases systemic costs.
- Regulators emphasize protection in an environment where fraud evolves rapidly.

Overall, the team concluded that staying resilient in an evolving risk landscape requires adaptive modelling, strengthened technical controls, and a shift toward people-centric planning that fully accounts for the human impact of emerging threats.

Accountability in disaster recovery

Accountability is pivotal for a speedy and successful disaster recovery effort, therefore placing significant strain on the people responsible for maintaining resilience, particularly when resourcing and training are insufficient. Key concerns included:

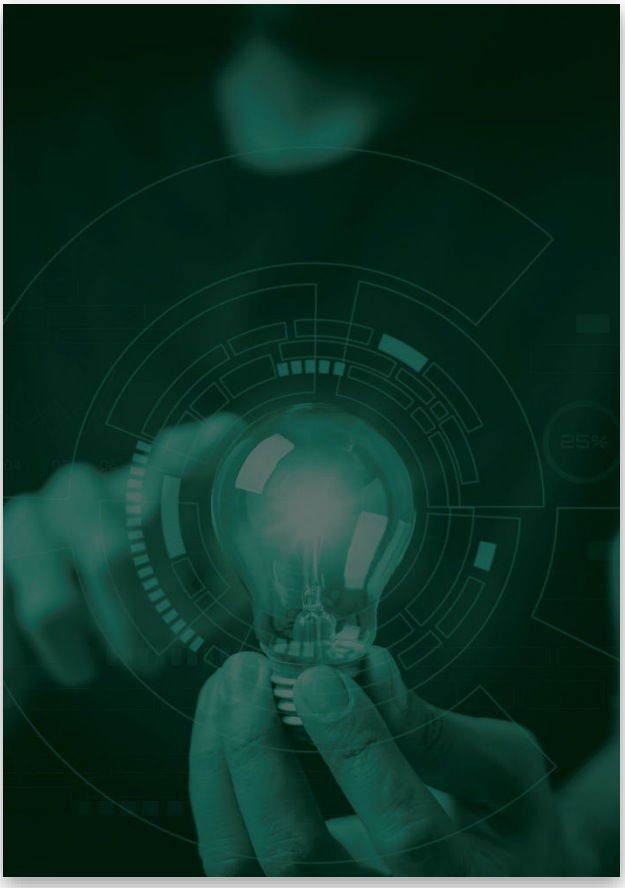


- Prolonged incidents (often weeks) drive burnout.
- Smaller businesses don't have the employee base to have a CTO or a CIO; legally they have the same responsibilities but not the manpower to match large global organizations with dedicated risk teams.
- IR/BC roles are secondary jobs for many, meaning it is not the primary focus making accountability difficult to enforce through policy.
- Operational resilience is constantly evolving; organizations adapt and train continuously, but a single training set is ineffective. Training must be tailored department by department, recognizing that resilience extends beyond architecture and critical systems to the entire organization.
- Difficulty communicating the real need for the business to organization leaders, which would ensure adequate financial resources are available for prevention over reactive actions.
- Smaller organizations often lack dedicated teams for proactive threat hunting, limiting their ability to identify and mitigate risks before they escalate into incidents requiring disaster recovery.

Ultimately, the team concluded that effective disaster recovery requires organizational support that prioritizes people—ensuring adequate staffing, reducing burnout risks, and providing tailored, role-specific training that equips all teams to contribute to true operational resilience.

Recommendations

- **Structured exercise cadence**: Conduct function-specific tabletop exercises alongside cross-supplier drills. Track after-action items through to completion with assigned owners and deadlines. Exercises should be performed annually at minimum, with increased frequency where feasible.
- **Dedicated threat-hunting capability**: Establish teams solely focused on proactive threat hunting to identify emerging risks before they evolve into incidents.
- **Resilience by default**: Implement zero-trust controls across crisis-management platforms, including Multifactor Authentication (MFA), device-posture validation, and role-based access control (RBAC). Ensure offline playbooks are available and establish robust communication-failover mechanisms.



- **People-centric disaster recovery:** Introduce duty-of-care measures such as buddy systems, safe-arrival check-ins, and duress codes. Establish fatigue thresholds and rota-based incident response coverage and incorporate field-safety scenarios into regular exercises.
- **Ecosystem-aligned best Ppractices:** Develop agreed-upon industry standards, including clauses and templates, to ensure clarity and consistency in contractual obligations across the security ecosystem.

In conclusion

Disaster recovery and operational resilience must evolve beyond audit-driven documentation and become rigorously tested, people-centered capabilities. Across the discussions, the team identified significant gaps: many organizations lack fully tested plans, rely on outsourced tooling with insufficient hardening, and depend on outdated or inflexible risk models that fail to reflect modern threats. Plans often prioritize systems over human safety, leaving field staff, customers, and communities exposed to coercion, violence, or severe-weather conditions. At the same time, smaller organizations face the same legal responsibilities as large enterprises but without equivalent staffing or specialized leadership, making sustained resilience far more challenging.

Equally critical is the human burden of prolonged incidents, burnout, and the widespread reality that incident response and business continuity duties are secondary roles. True resilience requires organizational support—adequate resources, rota-based coverage, and tailored departmental training that reflects the complexity and diversity of real operations. The recommendations—ranging from structured exercise cadence and zero-trust crisis controls to dedicated threat-hunting teams, people-centric safety measures, and ecosystem-aligned best practices—set a clear path forward. Together, they highlight the need for disaster recovery that is practical, adaptive, and firmly rooted in collaboration, ensuring that resilience becomes a reliable capability when it matters most.

Supply chain security

Modern supply chains are increasingly complex, interconnected, and globally distributed, making them a critical component of organizational resilience and security. Trust alone is no longer sufficient to manage supply-chain risk; businesses must be able to verify the security posture of their partners in a meaningful and consistent way.

Numerous elements were explored to identify opportunities for improving supply-chain security and resilience.

Supply Chain Hygiene

Supply-chain hygiene emerged as a key concern, highlighting the need for organizations to move beyond trust-based relationships and adopt meaningful mechanisms to verify the security posture of their partners. The discussion identified several hygiene-related issues that warrant attention:

- **Verification challenges:** Businesses lack consistent ways to validate security across their supply chains. Trust alone is insufficient, and the wide range of accreditation bodies and certificates often fails to meaningfully advance an organization's security posture.
- **Supply-chain complexity:** Modern supply chains are highly interconnected, where even a small supplier can provide business-critical components—such as semiconductor chips—capable of disrupting the entire chain, as seen in the PS5 release delays.
- **False sense of security among smaller organizations:** Some smaller suppliers perceive themselves as low risk due to their size and therefore underinvest in security, inadvertently increasing exposure for larger organizations that depend on them.

The discussion highlighted that weak supply-chain hygiene significantly increases systemic risk, driven by limited verification mechanisms, complex interdependencies, and uneven security maturity across suppliers. Strengthening supply-chain security requires greater transparency, meaningful assurance beyond accreditation, and a shared responsibility model that recognizes the critical role even the smallest suppliers play in the wider ecosystem.

Risk appetite and oversight

Building on the risks identified within supply-chain hygiene, the discussion naturally progressed into a deeper examination of risk appetite and oversight. As organizations rely on increasingly complex and interconnected ecosystems, understanding how risk is defined, accepted, and governed—both internally and across third parties—becomes critical.

This section explores whether organizations and their suppliers truly share a common understanding of acceptable risk, and how effective oversight can be achieved in practice rather than assumed through policy or process alone.

- Alignment of risk appetite: There is limited assurance that organizations and their supply-chain partners share the same risk appetite. While businesses often assume alignment, there is a lack of common frameworks or benchmarks to demonstrate that risk is being managed to equivalent standards.
- SME capability and ownership gaps: Critical SMEs frequently lack the resources required to meet Financial Institution (FI) standards, with security ownership often distributed across roles or remaining unclear.
- Ineffective assurance mechanisms: Reliance on “questionnaire theatre” provides minimal assurance and drives slow improvement. When the value is unclear, assessments default to extensive questionnaires, resulting in hundreds of responses that are difficult to analyze and act upon.
- Vendor visibility in large organizations: In complex enterprises with multiple products and teams, there is insufficient oversight of which vendors and components are embedded across the product estate. During major vulnerability events—such as Log4j or CrowdStrike incidents—this lack of visibility makes it difficult to quickly determine exposure and respond effectively.

The discussion highlighted challenges stemming from misaligned risk appetites, fragmented oversight of multi-tier suppliers, and the systemic risk introduced by smaller but business-critical vendors. Addressing these challenges will require clearer alignment on risk expectations, improved visibility across supply chains, and stronger governance to ensure resilience across the entire ecosystem.

Global landscape

The issues identified across supply-chain hygiene and risk appetite are further compounded by global regulatory variation, increasing reliance on cloud service providers, and a growing skills gap as foundational technical expertise leaves the workforce. These factors introduce additional complexity for organizations operating across borders and technology models.

- Regulatory fragmentation: Globally, countries impose differing laws and requirements governing system behavior and data storage. This raises challenges in designing products that comply not only with industry standards but also with diverse legal frameworks worldwide.
- Cloud dependency and concentration risk: As organizations continue to adopt cloud-as-a-service models, outages affecting major providers—such as recent AWS incidents—can bring entire businesses to a standstill. While responsibility and control are increasingly delegated to cloud providers, questions remain as to whether they are subject to equivalent levels of scrutiny and assurance.
- Evolving skills and knowledge gaps: As generations of engineers with deep foundational knowledge retire, critical understanding of underlying technologies risks being lost. While newer generations have grown up using advanced technology, they may lack insight into the core principles that underpin existing infrastructure—knowledge that remains essential for maintaining current systems and designing future solutions.

Taken together, these challenges highlight the need for stronger global oversight, clearer standards, and sustained investment in both governance and skills to ensure resilience across an increasingly interconnected and internationally regulated FinTech ecosystem.

Recommendations

- Risk-tiered supplier onboarding: Apply proportionate assurance based on supplier criticality, including deep security testing and joint tabletop exercises for vendors supporting critical business flows, with lighter-touch checks for low-risk suppliers.
- Sponsor-and-uplift model for critical SMEs: Provide funding, tooling, or coaching to help key SMEs meet baseline security controls—such as MFA, logging, and vulnerability management—in return for clearly defined SLAs and participation in incident response activities.

- Two-way culture and capability assessments: Evaluate security culture, operational maturity, and organizational fit as part of supplier due diligence to reduce the risk of misalignment during incidents.
- Clear contractual security obligations: Define explicit contractual requirements for incident notification timelines, reporting detail, and impact disclosure to ensure consistent and actionable information sharing during security events.
- Succession and knowledge-transfer planning: Actively invest in preserving foundational technical knowledge through structured knowledge transfer, recognizing that future generations bring new skills but rely on the stability of existing systems and expertise.

In conclusion

The discussions highlighted that supply-chain risk is driven not only by technical dependencies but by misaligned risk appetites, uneven security maturity, and limited visibility across increasingly complex ecosystems. Strengthening supply-chain resilience requires proportionate assurance, shared accountability, cultural alignment, and sustained investment in both people and partners—ensuring security expectations are clear, practical, and achievable across organizations of all sizes.

Final summary

The series of whitepapers highlight 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.

NCR Atleos and Trellix would like to thank everyone who took part in the cyber summit sessions, for their willingness to participate, contribute, and collaborate so openly throughout the discussions.