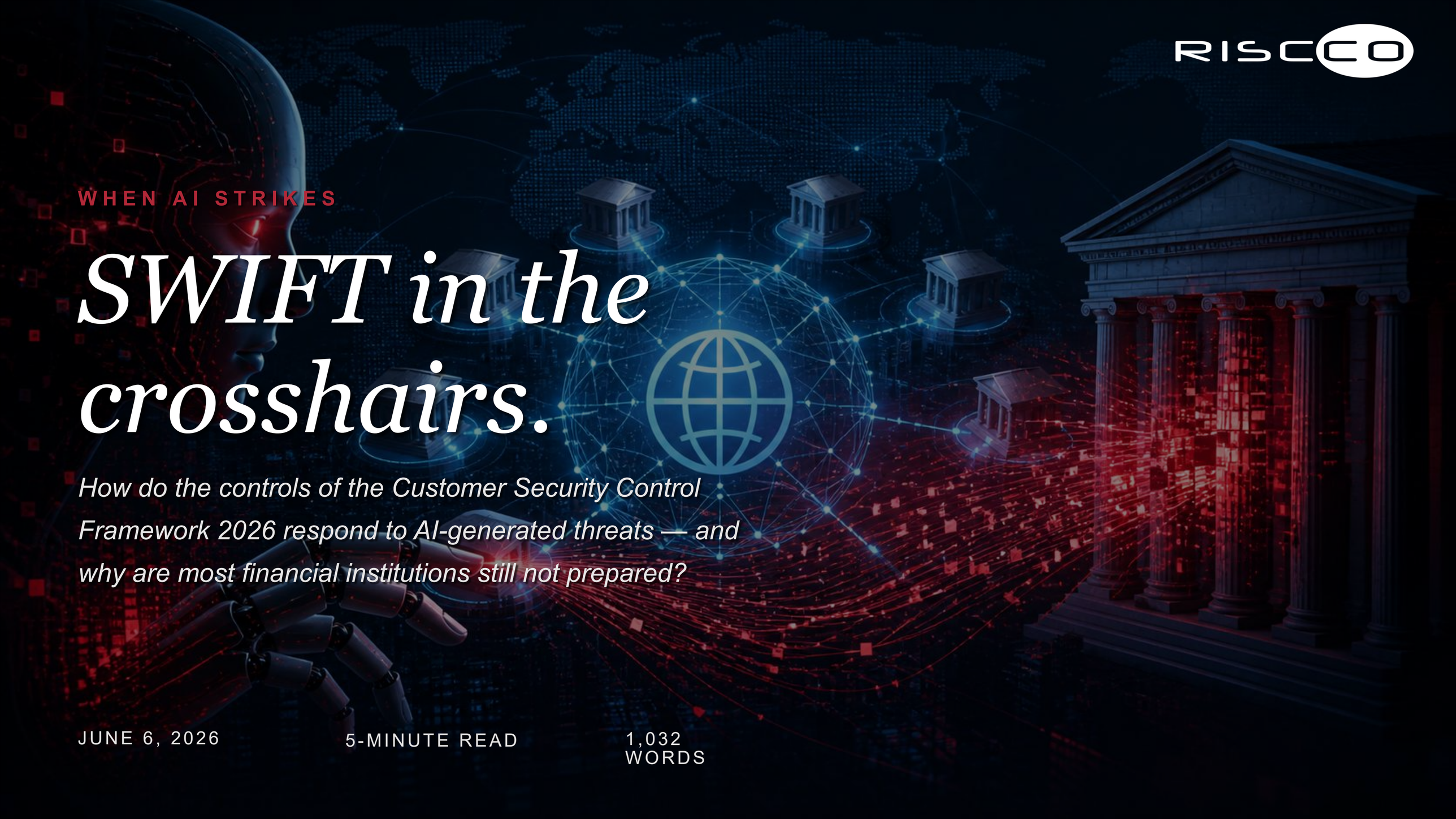

WHEN AI STRIKES

SWIFT in the crosshairs.

How do the controls of the Customer Security Control Framework 2026 respond to AI-generated threats — and why are most financial institutions still not prepared?

JUNE 6, 2026 | 5-MINUTE READ | 1,032 WORDS

EXECUTIVE SUMMARY

Generative AI has permanently transformed the cyberthreat landscape in the financial sector.

What once required specialized attacker teams can now be executed with accessible, cheap, and highly effective AI tools.

For institutions connected to the SWIFT network, this is not a future threat. It is an operational reality — present and future.

THIS ARTICLE HIGHLIGHTS THE MOST RELEVANT ATTACK VECTORS AND THE ACTIONS ORGANIZATIONS MUST PRIORITIZE.

THE PROBLEM AND THE RISK

AI has rewritten the rules of cyber attack.

16%

of security breaches already involve AI-driven attacks.

IBM COST OF A DATA BREACH REPORT · 2025

97%

of affected organizations lacked adequate access controls.

NIST ADVERSARIAL AI RESEARCH · 2025

80%

of large financial institutions failed their initial CSP assessment in 2025.

DELOITTE CSP ASSESSMENTS · 2025

Over the past decades, security in financial messaging systems, including SWIFT, was built on a clear principle: attackers need time, resources, and specialized knowledge. Generative artificial intelligence has permanently eliminated those entry barriers.

Today, an attacker can generate personalized phishing emails in seconds, automate reconnaissance of SWIFT infrastructure, and evade detection systems through adversarial manipulation techniques targeting security models.

For the SWIFT ecosystem, the risks are especially severe. The network moves trillions of dollars daily; a compromise window of just minutes can translate into irreversible losses.

80% of large financial institutions assessed in 2025 failed their first CSP assessment, according to an article published by Deloitte in April 2026.. This does not only reflect technical gaps, but that the speed at which threats evolve outpaces traditional compliance cycles.

KEY RISK VECTORS

Key AI threats for SWIFT.

> **“ 97% of organizations affected by AI attacks lacked adequate access controls to counter this type of attack. ”**

01

CRITICAL

Hyper-Personalized Phishing

AI generates messages tailored to the exact profile of the recipient using public data and leaked internal patterns. Traditional email filters cannot detect them.

02

CRITICAL

Authorization Deepfakes

Voice and video simulation of executives to bypass high-value transfer verification. CSCF 2026 addresses this explicitly in Control 7.2.

03

HIGH

AI Control Evasion

Adversarial techniques that manipulate fraud detection models to classify active attacks as legitimate transactions. Attacks on system logic.

04

HIGH

Attack Automation

AI agents perform continuous reconnaissance of SWIFT infrastructure and intrusion attempts at speeds that exceed any human response.

RECOMMENDATIONS

What organizations must do now.

CSCF 2026 provides the regulatory framework, but responding to AI threats requires decisions beyond the technology domain.

1 Elevate AI Governance to Systemic Risk.

The Risk Committee must periodically review AI attack exposure on SWIFT. Without an executive sponsor, efforts remain fragmented.

CSCF 2026 · CONTROL 1.1 · GOVERNANCE

2 Implement MFA Resistant to AI Social Engineering.

Traditional MFA schemes are vulnerable to AI deepfakes and phishing. Migrating to hardware-based MFA (FIDO2) for privileged access is urgent.

CSCF 2026 · CONTROL 4.2 · AUTHENTICATION

3 Deepfakes in Training Programs.

Required under Control 7.2. Staff must develop verification criteria for unusual instructions, regardless of their apparent legitimacy.

CSCF 2026 · CONTROL 7.2 · AWARENESS

4 Gap Assessment Before Q3.

Attestation opens July 1, 2026. 80% failed in 2025. Acting now avoids reputational costs and regulatory scrutiny from counterparties.

CSCF 2026 · KYC-SA · ATTESTATION

5 Inventory AI Systems in the SWIFT Environment.

Every AI system interacting with SWIFT flows must be documented and under explicit governance. Without inventory, the attack surface remains unknown.

CSCF 2026 · CONTROL 2.4 · BACK-OFFICE FLOWS

CONCLUSION

AI doesn’t wait. *Neither does CSCF 2026.*

The link between generative artificial intelligence and the criticality of SWIFT infrastructure creates a risk window that did not exist years ago. Attackers no longer need advanced technical expertise: AI facilitates attacks while organizations continue operating with processes designed for the pre-AI era.

CSCF 2026 represents SWIFT's formal acknowledgment that the perimeter has expanded and that threats are fundamentally different. However, the framework does not implement itself: it requires executive will, investment, and an organizational culture where security is everyone's responsibility.

Institutions that treat SWIFT compliance as a checklist expose themselves not only to regulatory sanctions, but to becoming the weak link in an ecosystem that depends on collective trust.

KEY MESSAGE

The AI your competitors use for operational efficiency, attackers use to compromise critical infrastructure.

RISCCO

CONTACTS

Panama, Central America and the Caribbean

Antonio Ayala I.
CEO
aayala@riscco.com

Rubén Fernández
Consulting Manager
rfernandez@riscco.com

Marinelda Morales
Commercial Manager
mmorales@riscco.com

Dominican Republic and Puerto Rico

Eury Valdez
Commercial Advisor
efvaldez@riscco.com

About RISCCO

RISCCO is an independent international consulting firm committed to transforming how organizations manage risk and adopt Artificial Intelligence. We combine a rigorous approach to GRC (Governance, Risk, and Compliance) with advanced data analytics and Artificial Intelligence to help our clients anticipate risks, strengthen governance, and solve complex challenges. Headquartered in Panama with a presence in six countries, in 2026 we mark 17 years serving more than 200 leading organizations across Central America and the Caribbean.

International rigor. Agile execution. Measurable impact.
We think like strategists. We execute like specialists.

riscco.com