If you lead security in Financial Services, this is your room — filled with people who live the same reality you do and talk about it.

When we launched **CISO New York** last September, the response from teams at **HSBC, Wells Fargo, and New York City Council** was: *"This feels built for us." "You don't usually hear these conversations on stage." "This is a community."*

On **February 26, 2026**, we're bringing that same energy, but this time, it's **Financial Services**.

- The new attack patterns targeting financial data right now
- Securing cloud + multi-cloud when nothing is standardized
- AI that cuts SecOps noise instead of adding more
- The fraud and insider threats everyone is feeling but no one is openly talking about

You don't need another event filled with long lectures and generic sessions- you need the community, and the formats that give you answers.

- **Ask-Me-Anything** —unfiltered answers from veteran CISOs
- **Yes / No / Maybe** —fast gut checks on the topics no one agrees on
- **Quick Wins or Just Noise** — tools + tactics that your peers say work
- **Live Poll Debate** — the entire room votes in real time
- **The CISO Challenge Hackathon** — one live cyber crisis, solved together

**Get in touch with the Conference Producer for this event via monika.dincheva@coriniumgroup.com*

Confirmed Speakers:

Noreen Fierro, *Enterprise Chief Ethics & Compliance Officer* - **Principal Financial Group** *(Advisory board member)*

Scot Miller, *Chief Information Security Officer* - Mr. Cooper *(Advisory board member)*
Ellis Wong, *Chief Information Security Officer* - JST Capital *(Advisory board member)*
Jessica Wilson, *Business Information Security Officer* – Bank of America
Albert Laweh Tetteh, *Chief Information Officer* - GCB Bank Limited *(Advisory board member)*
John Decker*, Chief Technology Officer* -**Trian Partners**
Alex Dickson, *Chief Information Security Officer* - GCM Grosvenor *(Advisory board member)*
Matthew Hyland, *Executive Director, Cloud Security Risk Management* – WELLS FARGO
Alexander Abramov, *Head of Information Risk* -Financial Services
Nishit Mehta, Vice President, *Analytics Solutions Manager* – JPMorganChase
Jane Domboski, *Chief Information Security Officer* - OneMain Financial (tbc)
Imran Khan, *Data Protection Officer*- Statistics Canada (tbc)
Arsen Danilyan, *Vice President - Information Security Officer*- Société Générale (tbc)

CISO FS NY February 26th, 2026	
08:00 – 08:45	*Registration & Coffee in the Exhibition Area*
8:45 - 8:55	Chair's Opening Remarks
8:55- 9:00	Speed Networking – Making new connections at CISO FS NY! During this 5-minute networking session, the aim of the game is to go and meet two people you don't already know.
09:00 - 09:30	Opening Panel: Confessions of CISOs: What They Don't Tell You About the Job • How can sleepless nights, board politics, and regulator heat be managed without burnout? • Which AI-driven threats and hybrid risks are keeping CISOs awake in 2026? • When speed clashes with security and compliance with agility, how can the trade-offs be survived? • What do CISOs wish had been known before stepping into the role? Albert Laweh Tetteh, *Chief Information Officer* - GCB Bank Limited

09:30 - 10:00	**Panel Discussion: How to Stop Compliance Spend Becoming a Black Hole?** • Where do compliance frameworks overlap across borders, and how can the duplication be cut? • What makes a compliance budget credible as resilience spending? • When does compliance move from obligation to competitive advantage? • Which signals of audit readiness build market trust? Moderator: Alexander Abramov, *Head of Information Risk* -Financial Services Noreen Fierro, *Enterprise Chief Ethics & Compliance Officer* - Principal Financial Group Nishit Mehta, *Vice President, Analytics Solutions Manager* – JPMorganChase	
10:00 - 10:30	**Expert Ask-Me-Anything: AI, Risk & Regulation** An informal, interactive session where attendees ask questions directly to a panel of cybersecurity leaders. Focus Areas: AI risk and security, regulatory complexity (SEC, NYDFS, DORA), board-level communication, and building resilient cyber teams. Moderator: Alexander Abramov, *Head of Information Risk* -Financial Services Jessica Wilson, *Business Information Security Officer* – Bank of America	
10:30- 11:00	Session Placeholder- Details TBA	
11:00 11:30	*Mid-Morning Coffee & Networking in the Exhibition Area*	
	The CISO Boardroom	Cloud & DevSecOps Lab

11:30- 12:00	**Who Takes the Fall When AI Fails?** • How can deepfake fraud, model poisoning, AI-powered phishing, and AI in credit or lending decisions be stopped? • Who owns AI risk, and which frameworks or guardrails keep innovation safe? • Who carries the liability when AI fails in FS? • How is AI risk best reported in board language? • What playbooks work for AI-specific incidents like data leakage or model poisoning?	**Presentation: DevSecOps in FS: Automate, Delegate, or Burn Out?** • Which pipeline controls are best enforced through policy-as-code? • How can security checks be safely delegated to dev teams in regulated contexts? • What metrics demonstrate DevSecOps reducing audit findings? • Where does human review still outperform automated tools in FS? Ellis Wong, *Chief Information Security Officer* - JST Capital
12:00 – 12:15	**Yes, No, Maybe? A Reality Check for FS Cyber Leaders** The moderator throws out a statement, and the audience vote: yes, no, or maybe. Topics include third-party risk, overlapping compliance, board metrics that miss the point, and whether resilience plans would hold up.	**Quick Wins or Just Noise? Cutting Through the Cloud & DevSecOps Hype** Every week there's another "must-have" tool. In this session we run through common practices — IaC scanning, SAST/DAST, secrets management, SBOMs, automated checks, and more. For each one, you vote: real value or just noise. A few volunteers share why. Jessica Wilson, *Business Information Security Officer* – Bank of America
12:15- 12:30	**Spotlight Session** *Speaker and topic to be announced*	**Spotlight Session** *Speaker and topic to be announced*
12:30 - 13:00	**Why Zero Trust Keeps Stalling in Financial Services and What to Do About It?** • "Never trust, always verify" sounds good, so why does it stall in practice and slow workflows?	**Why Multi-Cloud Compliance Is Still Broken, and How to Fix It?** • What's the right way to automate compliance evidence in multi-cloud?

	• How can sysemic risk from multi-cloud reliance be contained before it cascades? • Regulators are demanding proof - what evidence convinces them that Zero Trust works? • Can airtight access controls and smooth user experience ever succeed at the same time?	• How can the gap between visibility and operational control be closed? • Which compliance evidence must be automated to satisfy regulators? • Can cloud resilience be stress-tested before regulators force the issue? • Where's the breaking point when balancing cost, performance, and security?
13:00 – 14:00	*Lunch & Networking in the Exhibition Area*	
	The CISO Boardroom	Cloud & DevSecOps Lab
14:00-14:30	How to Catch Insider Fraud Without Destroying Culture and Trust? • Where does privileged access and hybrid work create fraud blind spots? • Can behavioral analytics catch risk early enough to stop escalation? • How can HR, legal, compliance, and the CISO work from one playbook? • What builds trust culture without slipping into surveillance overkill? Albert Laweh Tetteh, *Chief Information Officer* - GCB Bank Limited	When AI Ships Code Faster Than You Can Review It: How to Stay in Control • How do you catch misconfigurations, leaked secrets, and insecure patterns at AI speed? • What guardrails stop GenAI code assistants from introducing vulnerabilities? • Which parts of threat modeling and secure code review can be safely automated? • How do you prevent hallucinations, false positives, and "AI-led security drift" without slowing delivery?

14:30-15:00	Panel Discussion: Who Owns the Fallout When AI Models Misfire - Security, Risk, or the Board?	Panel Discussion: What Breaks in Hybrid/Multi-Cloud and How to Prove Resilience?

	• Who owns AI risk when models impact lending, underwriting, or fraud detection? • How do you embed AI monitoring into cyber risk management? • What guardrails prevent AI misuse without stifling innovation? • How do you prepare for AI-specific incidents like data leakage or model poisoning? Matthew Hyland, *Executive Director, Cloud Security Risk Management* – WELLS FARGO	• How can Zero Trust be implemented across hybrid and multi-cloud environments? • What evidence of resilience does regulators expect to see? • How can systemic risk from single-cloud dependence be avoided? • Can customer experience be protected while workflows are locked down?
15:00-15:30	Discussion group A: What Happens When Agentic AI Runs Your Security Ops Before You Do? • What risks come with AI-on-AI escalation between defenders and adversaries? • How can effective oversight frameworks be built for AI-augmented SOCs? • What early wins, and early fails are showing up in adopting agentic AI for security? • How can human analysts stay in the loop when machines move first? Ellis Wong, *Chief Information Security Officer* - JST Capital	Discussion group B: What's Your First Move When Your Multi-Cloud Setup Gets Hit at 2am? • How do you embed post-quantum readiness into cloud strategy? • How can you secure serverless and containers without slowing delivery? • What AI analytics improve cloud threat detection accuracy? • Which cloud security capabilities will be baseline by 2028?
15:30-16:00	*Afternoon Break & Networking in the Exhibition Area*	
16:00-16:30	Ransomware in Financial Services: What to Tell Regulators When You're Still Locked Out? • Which ransomware attack patterns and entry points are hitting FS the hardest? • How should payment dilemmas be handled under regulatory scrutiny in 2026? • Where do incident response playbooks usually break down?	

	• What resilience gaps do tabletop exercises expose?
16:30- 17:00	Live Poll Debate: Would You Trust AI to Act Before Your Team Can? Experts go head-to-head, using real incidents and risks from the field. We'll start with a live poll to see where the room stands, then run it again at the end to track if minds have shifted. The debate centers on one tough question: *should we ever let technology act on its own during a live cyber incident in financial services?* The audience is part of it too so ask your questions, share your views, and see how your take stacks up against your peers. Jessica Wilson, *Business Information Security Officer* – Bank of America
17:00- 17:30	Closing Hackathon: The CISO Challenge Which crisis hurts Financial Services most today: AI fraud, regulator-pressure ransomware, or an insider leak? Pick one and solve it. Split into three teams (Technical, Board & Regulators, Communications & Customers). Each team has 8 minutes to agree on their top two actions in the first 24 hours, followed by quick share-backs and audience reactions.
17:30- 17:35	Chair's Closing Remarks
17:35 - 18:30	*Networking drinks and Prize Draw*
18:30	END OF CONFERENCE