

APRIL 28, 2026

# CISO Chicago

▶ Connecting you to what's next in infosec

## CISO CHICAGO

If you lead security in a complex, fast-moving enterprise, this is your room, filled with CISOs and security leaders who are navigating the same pressures, trade-offs, and expectations you are. This April in **Chicago**, we're bringing together senior security leaders for a day built around **real-world experience, peer insight, and practical decision-making.**

This is where we'll openly discuss:

- The attack patterns CISOs are dealing with right now, identity abuse, AI-enabled fraud, and supply-chain exposure
- Securing cloud and multi-cloud environments when architectures, ownership, and controls are anything but consistent
- Using AI to reduce SecOps noise and analyst burnout, without introducing new risk
- The insider, cultural, and organisational issues everyone feels but few discuss openly
- What resilience actually looks like when prevention alone is no longer enough

You don't need another event filled with long lectures and surface-level panels.  
You need peers, candour, and formats that give you answers.

That's why this event is built around **highly interactive formats that give you real answers:**

- **Ask-Me-Anything** à unfiltered, candid insights from experienced CISOs
- **Live Poll Debates** à the room votes in real time on the topics everyone's arguing about
- **Burning Questions** à tackle the issues you've been hesitant to raise publicly
- **Confessions of a CISO** à hear the challenges, mistakes, and lessons that rarely make it to the stage

This isn't about hearing more voices, it's about hearing the *right* ones.

It's a room designed for security leaders who want clarity, honesty, and a community that understands the reality of the role.

## AGENDA

8:00	Registration & Networking Breakfast
8:45	Opening Remarks, Speed Networking Robert Wagner, Advisory CISO, <b>ISSA CHICAGO CHAPTER</b>
8:50	<p><b>OPENING PANEL: Confessions of CISOs – Today’s Operational Reality</b></p> <ul style="list-style-type: none"> <li>• Insights into the unfiltered realities CISOs face as cyber risk, AI adoption, and regulatory scrutiny converge.</li> <li>• Exploring how security leaders are balancing innovation demands with shrinking tolerance for failure.</li> <li>• What CISOs wish boards understood about operational risk, talent constraints, and security debt.</li> </ul> <p>George Coleman, Vice President, Chief Information Security Officer, <b>ARIEL INVESTMENTS</b>  Tellis Williams, Chief Information Security Officer, <b>THE DREAM EXCHANGE</b>  Kathryn Mattie, Chief Information Officer, <b>BRIGHTPOINT</b>  <b>Moderator:</b> Chris Carter, Partner, Chief Information Security Officer Services, <b>INFINITE PARTNERS</b></p>
9:35	<p><b>EXPERT AMA: AI, Governance &amp; Regulatory Complexity</b></p> <ul style="list-style-type: none"> <li>• What CISOs need to know about evolving AI regulation and executive accountability.</li> <li>• How to manage uncertainty when laws, standards, and expectations are still forming.</li> <li>• Insights from peers on engaging legal, risk, and compliance teams early.</li> </ul> <p>Oscar J Giraldo, Assistant Vice President of Data Security, <b>WATERTON</b>  Mel Fenner, Chief Digital Innovation Officer, <b>LINCOLN UNIVERSITY</b>  <b>Moderator:</b> Nidhi Luthra, Global Chief Information Security Officer, <b>BAXTER INTERNATIONAL (former)</b></p>
10:05	<p><b>KEYNOTE: Rewriting Leadership: Leading Humans and Machines Together</b></p> <p><i>As artificial intelligence reshapes how organizations operate, compete, and innovate, leadership itself is undergoing a fundamental rewrite. No longer confined to managing people and processes, today’s leaders must orchestrate dynamic ecosystems where humans and intelligent machines collaborate, learn, and make decisions together.</i></p> <p><i>This keynote explores what it truly means to lead in a world where algorithms influence strategy, automation drives execution, and data becomes a core leadership asset. It challenges traditional management models and introduces a new leadership paradigm - one that blends human judgment, ethical responsibility, and emotional intelligence with the speed, scale, and precision of AI systems. Attendees will gain practical insights into building high-performing hybrid teams, fostering trust between humans and AI, and navigating the complex risks surrounding cybersecurity, bias, and governance. The session will also examine how leaders can create cultures that embrace continuous learning, adaptability, and responsible innovation while maintaining accountability in increasingly autonomous environments. Designed for forward-thinking executives and decision-makers, this keynote will equip leaders with the mindset and strategies needed to thrive at the intersection of human potential and machine intelligence - where the future of leadership is not just managed, but co-created.</i></p> <p>Jigar Shah, Chief Information Security Officer, <b>MEDUSIND</b></p>
10:35	<b>Spotlight Session: Security Teams That See Around Corners: Mitigating AI Risk in Real Time</b>

	<p><i>From vibe coding and autonomous agents to generative chatbots in everyday workflows, AI adoption is occurring at a pace that most security programs have not been able to realistically govern. Well-intentioned employees, misaligned agents, overly permissive access, and weak data controls are introducing new forms of risk, often without malicious intent. At the same time, adversaries are actively probing these gaps through indirect prompt injection and jailbreaking techniques. However, there's good news. More often than not, failures leave signals long before they become significant incidents. In this session, you'll learn how an AI security blueprint can help you identify emerging risk and align security controls to new and existing AI deployments, ensuring AI initiatives at every stage can realize their business value without security acting as a bottleneck.</i></p> <p><b>Marc Tabago, Senior Solutions Engineer, TRENDIAI</b></p>
10:45	<p><b>Morning Break &amp; Networking</b></p>
11:15	<p><b>Spotlight Session: Intelligent Defense: Orchestrating Security at the Edge in the Age of Automated Attacks</b></p> <p><b>Viken Shah, Senior Sales Engineer, FASTLY</b></p>
11:30	<p><b>Presentation: Email Is Still the #1 Breach Vector — and AI Is Changing the Threat Model</b></p> <ul style="list-style-type: none"> <li>• How to defend against AI-driven email threats that bypass traditional security controls</li> <li>• Exploring how generative AI is reshaping phishing, BEC, and social engineering at scale</li> <li>• Insights into why identity, not email, is now the true breach vector and what to do next</li> </ul> <p>Shelby Kiger, Cybersecurity Engineer, <b>MCDONALD'S</b></p>
11:50	<p><b>Presentation: Who Owns AI Risk When Things Go Wrong?</b></p> <ul style="list-style-type: none"> <li>• Exploring accountability models when AI systems cause financial, legal, or reputational damage.</li> <li>• What boards and regulators will expect CISOs to answer after an AI-driven incident.</li> <li>• How to define ownership across security, data, legal, and product teams.</li> </ul> <p>Mel Fenner, Chief Digital Innovation Officer, <b>LINCOLN UNIVERSITY</b></p>
12:20	<p><b>PANEL DISCUSSION: Reality Check: Security Investments That Truly Deliver</b></p> <ul style="list-style-type: none"> <li>• Insights into which security investments are driving measurable risk reduction versus noise.</li> <li>• How to justify spend using business-aligned metrics instead of technical outputs.</li> <li>• What CISOs are deprioritizing to reduce tool sprawl and operational friction.</li> </ul> <p>Kiran Rallabandi, Chief Technology Officer, <b>WARRANTY PROCESSING</b>  Jeremiah Johnson, Associate Director of AV Collaboration, <b>THE KRAFT HEINZ</b>  James Knighton, Chief Information Security Officer, <b>KNIGHTON REALTY</b>  <b>Moderator:</b> Chris Carter, Partner, Chief Information Security Officer Services, <b>INFINITE PARTNERS</b></p>
12:50	<p><b>Lunch Break &amp; Networking</b></p>
1:50	<p><b>Presentation: From Breach Headlines to Board Confidence</b></p> <ul style="list-style-type: none"> <li>• Insights into how public cyber incidents are reshaping board expectations.</li> <li>• How to proactively address reputational risk before an incident occurs.</li> <li>• What boards now expect CISOs to explain in the first 48 hours after a breach.</li> </ul> <p>Anamika Roy, Director, IT Audit &amp; Data Analytics, <b>OLD REPUBLIC GENERAL INSURANCE (former)</b></p>
2:10	<p><b>Presentation: Leadership Masterclass: How to Communicate Risk in Business Terms</b></p> <ul style="list-style-type: none"> <li>• Why Risk Communication Fails</li> </ul>

	<ul style="list-style-type: none"> <li>• Translating Risk into Business Impact</li> <li>• Practical Playbook that works</li> <li>• Driving Decision in Today’s Reality</li> </ul> <p>Pal Vankayalapati, Chief Information Officer, <b>PLZ CORP</b></p>
2:30	<p><b>FIRESIDE CHAT: Multi-Cloud Resilience, Regulatory Proof Points &amp; Preparing for Post-Quantum Risk</b></p> <ul style="list-style-type: none"> <li>• Exploring how organizations are proving security and compliance across hybrid estates.</li> <li>• How to maintain resilience when visibility, controls, and ownership are fragmented.</li> <li>• What regulators and auditors increasingly expect to see.</li> <li>• How to inventory cryptographic dependencies and prepare for post-quantum migration across multi-cloud environments.</li> </ul> <p>Abiola Olamoyegun, Vice President, Information Technology IA, <b>PHEAA</b>  Ross Esguerra, Technology Leader   DevOps Advocate Travel &amp; Hospitality, <b>HYATT HOTELS CORPORATION</b>  <b>Moderator:</b> Pal Vankayalapati, Chief Information Officer, <b>PLZ CORP</b></p>
3:00	<p><b>Afternoon Break &amp; Networking</b></p>
3:30	<p><b>LIVE DEBATE: Risk Roulette</b></p> <p><i>In cybersecurity, every decision comes with trade-offs, and not all risks are created equal. In this high-energy, live debate, top security leaders face off to tackle some of the toughest “what-if” scenarios CISOs encounter daily, from ransomware vs. silent data breaches, to strict access controls vs. business agility, and everything in between.</i></p> <p><i>Audiences will witness real-time arguments, expert insights, and a clash of perspectives as panelists defend their stance on difficult security dilemmas. Attendees will gain insights into:</i></p> <ul style="list-style-type: none"> <li>• A deeper understanding of the trade-offs behind major security decisions</li> <li>• Actionable frameworks for prioritizing risk in their own organizations</li> <li>• Fresh insights into how leading CISOs think under pressure</li> </ul> <p><i>Expect surprises, audience polling, and lively debate, because in cybersecurity, sometimes there is no right answer... only what’s worse.</i></p> <p><b>Moderator:</b> Arpi Long, Deputy Chief Information Security Officer, <b>COLLECTIVE HEALTH</b>  Karen Habercoss, Chief Information Security &amp; Privacy Officer, <b>UCHICAGO MEDICINE</b>  Dave Gerleman, Board Member, <b>INFRAGARD CHICAGO MEMBER ALLIANCE</b></p>
4:20	<p><b>Keynote: A Framework for Managing Artificial Intelligence &amp; Third-Party Risk Management: Medicare Advantage</b></p> <ul style="list-style-type: none"> <li>• Insights into why foundational TPRM controls are often undervalued and how reframing them drives stronger adoption.</li> <li>• How to design onboarding and ongoing monitoring practices that reduce third-party cyber risk before incidents occur.</li> <li>• Exploring peer collaboration as a catalyst for improving TPRM maturity and prevention strategies.</li> </ul> <p>Josh Aubey, Chief Compliance &amp; Privacy Officer, <b>WELLBE SENIOR MEDICAL</b>  Brandin Brooks, Senior Credentialing Specialist, <b>WELLBE SENIOR MEDICAL</b></p>

4:45	<b><i>Closing Remarks &amp; End of Conference</i></b>
4:50 – 5:50	<b><i>Networking Reception</i></b>