MATT RATHBUN

Chief Technology Officer & Managing Director | Technology & Security Executive · Three-Time CSO

Chicago, IL • matt.rathbun.email • linkedin.com/in/matt-rathbun-7104207 • CISSP #378641

Decision record & verifiable history: matt.rathbun.email/decisions•matt.rathbun.email/llms.txt

EXECUTIVE SUMMARY

Each chapter built on the last. I wrote the audit methodology that helped build the foundation for FedRAMP, which got me recruited to Azure. Azure gave me cloud security depth at true hyperscale. Two Sigma taught me what security means when the IP is the product. At OCC I came in to lead security, was tapped to drive AI transformation, took on Technology Strategy & Innovation, and was appointed Chief Technology Officer when the firm committed to digital assets as its forward strategy.

Today: Chief Technology Officer & Managing Director at OCC—the Systemically Important Financial Market Utility behind every listed U.S. equity option, under SEC and CFTC oversight—accountable for enterprise technology strategy, architecture, AI, digital asset infrastructure, and the resilience the options market depends on. A three-time Chief Security Officer (Microsoft Azure Global, Two Sigma, OCC): security is the foundation everything else is built on. Among the first security leaders to deploy generative AI in production, at an institution where getting it wrong is not an option.

CORE COMPETENCIES

- Enterprise Architecture & Technology Strategy
- AI Transformation & Governance
- Digital Asset Infrastructure (Strategy)
- Critical Infrastructure Resilience (SIFMU)
- Cloud Security Architecture
- Security Leadership (CSO / CISO)
- Regulatory Compliance (SEC, CFTC, FedRAMP, NIST, RegSCI)
- Enterprise & Catastrophic Risk Management
- Board & C-Suite Communication

PROFESSIONAL EXPERIENCE

Chief Technology Officer & Managing Director | OCC — 2026 – Present

Options Clearing Corporation — SIFMU | SEC/CFTC Oversight | 100+ organization across architecture, AI & business technology

- **Enterprise mandate:** Own enterprise technology strategy and architecture for the infrastructure behind every listed U.S. equity option—accountable in production for resilience, recoverability, performance, availability, and total cost of ownership. I own the uptime the options market depends on.
- **Digital assets:** Lead the technology strategy for OCC's digital-assets initiative—architecture, partnerships, integration choices, and internal-systems enhancements behind digital assets as collateral, on-chain clearing of options, and collateral margining outside the traditional banking-hours cycle.
- **AI at enterprise scale:** Take AI beyond chatbots and coding agents to full agentic workflows—governed with the rigor and accountability demanded of quantitative models. Architect of the AI governance framework and the standards for how AI agents securely connect to enterprise data and tools.
- **Stakeholder leadership:** Senior technology voice to the Board, regulators, and Clearing Members on architectural resilience, AI governance, and digital asset infrastructure.
- **Hands-on:** I still understand the technical details myself before I ask anyone to adopt anything. Twenty-five years in, the method hasn't changed: understand how it actually works, then set the strategy.

Chief Security Officer & Head of Technology Strategy & Innovation | OCC — 2025 – 2026

Options Clearing Corporation — SIFMU | SEC/CFTC Oversight | ~100 reports

- **Dual mandate:** Led cybersecurity for the clearinghouse behind every listed U.S. equity option, processing billions in daily transactions; concurrently drove enterprise AI transformation and technology strategy. That execution led to appointment as CTO.
- **AI governance:** Built the AI governance framework and the standards for how AI systems securely connect to enterprise data and tools. Understood the technology directly before setting strategy—built proof-of-concepts personally—then drove firm-wide adoption of coding agents and agentic workflows.
- **Cloud security assessment:** Completed a comprehensive AWS security assessment against NIST CSF and RegSCI requirements—published as an industry reference architecture (joint AWS announcement).
- **GenAI deployment:** Led an AWS generative-AI implementation that improved operational efficiency in software testing, with human review retained at every critical decision point (joint AWS announcement).
- **Transformation & scope:** Converted Security from a functional organization into a service-delivery model aligned to platform resiliency, decision fidelity, and implementation quality. Led Cyber Operations, Security Governance, Security Engineering, and Red Team; developed catastrophic-risk strategy for market-infrastructure continuity under attack.

Chief Security Officer | Two Sigma — 2019 – 2025

Quantitative Investment Firm — SEC/CFTC/FSA Regulated | 50-person global organization | 65 business-critical products

- **IP protection at scale:** Built and led a security program spanning data loss prevention, insider threat, security engineering, and third-party risk—including DevSecOps teams that delivered security-critical services. Designed the security architecture that let Two Sigma compute its most IP-sensitive algorithms and models on GCP.
- **China office trust architecture:** Rejected the standard playbook—extend the perimeter, paper the gap with contracts—because contracts only work where someone enforces them. Designed independent trust infrastructure for an on-shore Mainland China office, protecting trading strategies while enabling regulatory approval and market access in an adversarial nation-state environment.

- **FPGA-to-cloud migration:** Led the engineering team converting crypto market-making infrastructure from custom FPGA hardware to cloud-native AWS—persuading the CTO that Security Engineering should build the system, because crypto lacks the legal safety nets of traditional finance and the gap had to be filled architecturally.
- **Early GenAI deployment:** While peer firms blocked ChatGPT, cleared the legal, regulatory, and IP objections one by one and shipped generative AI to full production by mid-2023—guardrails designed from scratch because no playbook existed, at a firm where a small leak could move markets.
- **Board communication:** Provided regular security reporting to the Management Committee and Boards of Directors; made security risk legible to a board that evaluates everything through a quantitative investment lens.

CSO, Azure Global / CISO, Azure Government | Microsoft **2015 – 2019**

Hyperscale cloud security & compliance — ~100-person globally distributed team | FedRAMP | Federal, DoD, state & local

- **Revenue impact:** Delivered 100+ customer-facing presentations annually—security architecture engagements, CSA Federal Summit keynotes, compliance deep dives—directly attributed with over $1 billion in Azure annual recurring revenue.
- **Azure Government CISO (2015–2018):** Led information security, regulatory compliance, and customer commitments across federal, DoD, and state/local agencies. Managed FedRAMP authorization for government cloud, and worked directly with the NSA on a framework for quantitatively assessing DoD cyber program effectiveness.
- **Azure Global CSO (2018–2019):** Led a globally distributed team responsible for the entire Azure platform. Owned 117 global compliance certifications and the supply-chain security program for Azure hardware and software. Transformed reactive vulnerability management into a proactive remediation cadence that compressed timelines across every region worldwide.
- **AI & data ethics:** Led the data ethics council (2017–2018), governing AI's impact on customer-data decisions before it was a commercial concern—early governance work that previewed today's AI policy challenges.

Engineer → Senior Vice President | First Information Technology Services **2007 – 2015**

Built cybersecurity division from small practice to 100+ personnel | West coast operations | Multi-framework audit methodology

- **FedRAMP foundation:** Hired as a contractor to write an audit protocol against NIST 800-53—a standard the industry considered un-auditable, where Big 4 firms estimated a single audit would exceed the three-year coverage window. Rather than compressing their sampling methodology, read everything NIST published and produced a protocol two engineers could execute in one month.
- **Validated at scale:** DHS validated the methodology against Inspector General results across five systems—audits completed in 10% of the time, finding two orders of magnitude more issues. Repriced federal security assessments and displaced Big 4 incumbents on price and quality.
- **DHS transformation:** Methodology helped DHS raise its congressional cybersecurity score from D to B+ in a single year. Subsequently wrote the cloud audit protocol and standards interpretation that DHS, DoD, and GSA developed into FedRAMP.
- **Division growth & recruitment:** Grew the security division more than tenfold in personnel and revenue across major cloud providers; opened the Seattle office; promoted from engineer to SVP in under seven years. Recruited to Microsoft in 2015 after the head of Azure Global saw his team defer to me in client meetings.

IT Manager | The Bank of Washington 2005 – 2007 — Information security and risk programs, IT infrastructure, regulatory compliance, disaster recovery planning, board reporting.

Systems Analyst | Siemens Business Services 2003 – 2005 — OS upgrade project management for The Port of Seattle. Automated software deployment and compatibility testing.

PUBLISHED WORK & INDUSTRY PRESENCE

Active writer on AI security, cybersecurity economics, and organizational leadership at matt.rathbun.email. **Decision record**—six load-bearing career decisions with the reasoning, rejected alternatives, and risks preserved: matt.rathbun.email/decisions.

Selected essays: "The Long Con at Machine Speed" (how AI collapsed the economics of cyberattacks) · "AI Won't Be Afraid of Getting Fired" (the social contract as invisible security architecture) · "The Invisible Operating System" (AI security, organizational intent, and the tacit human substrate) · "The Architecture You Can't Document" (leadership as emotional infrastructure).

Press, panels & forums: Joint AWS announcements on cloud security assessment and generative-AI operational-efficiency work at OCC (2025). Featured in WatersTechnology / Risk.net on generative AI with guardrails; John Lothian News (FIA EXPO); The Defender's Journal; Techfellow Ltd. Member of FS-ISAC, The CHEF, and ARC. MFA security & technology panelist (2019, 2023, 2024). CSA Federal Summit keynotes; 100+ presentations per year during the Microsoft chapter.

EDUCATION & CERTIFICATION

CISSP — Certified Information Systems Security Professional | #378641

Kansas State University — B.S. Political Science