Cybersecurity: How Are You Innovating to Stay Ahead of Cyber Attacks?

Brett Conlon
Chief Information Security Officer
American Century Investments

Setting the Stage

- **The threat landscape has fundamentally shifted.**
- Financial services remains the #1 targeted industry globally. Adversaries are no longer just stealing data — they are disrupting operations, manipulating markets, and eroding trust.

- **Three forces converging now:**
- 1. AI-powered attacks at machine speed
- 2. Identity as the primary attack surface
- 3. Regulatory pressure accelerating (SEC, DORA, NIST CSF 2.0)

- The question isn't whether you'll face a sophisticated attack — it's whether your innovation pace matches the adversary's.

What Has Changed: The Adversary Has Evolved

- **Yesterday's Attacker**
- Phishing emails with typos, brute-force password spraying, opportunistic malware

- **Today's Attacker**
- AI-generated deepfake voice calls impersonating executives
- Living-off-the-land techniques that bypass endpoint detection
- Supply chain compromises targeting your trusted vendors
- Credential theft at scale — 80%+ of breaches involve compromised identities

- **Key Insight:**
- The perimeter is no longer your firewall. The perimeter is your identity fabric.

Innovation Area #1: AI as a Defensive Multiplier

- **Reality vs. Hype**
- AI is not a silver bullet. But it is the only way to match machine-speed attacks with machine-speed defense.

- **Where AI is delivering real value today:**
- Behavioral analytics — detecting anomalous access patterns across millions of events
- Automated triage — reducing SOC alert fatigue by 60-70% through intelligent correlation
- Threat intelligence synthesis — connecting indicators across feeds in real time

- **Where AI is still hype:**
- Fully autonomous remediation without human oversight
- Replacing skilled analysts with chatbots
- Vendor claims of “AI-powered” with no explainability

Innovation Area #2: Identity and Access — The New Perimeter

- **Identity is the control plane of modern security.**
- Every cloud workload, every API call, every SaaS login — it all starts with identity. If you don't govern identity, you don't govern anything.
- **Innovation levers in IAM:**
- Zero Standing Privilege — no persistent admin access, just-in-time elevation
- Continuous authentication — moving beyond point-in-time MFA to session-level risk scoring
- Machine identity governance — service accounts, API keys, and workload identities at scale
- Permission boundaries and guardrails — self-service that's secure by default

Innovation Area #3: Security as a Business Enabler

- **The old model: Security as a gate.**
- Teams wait weeks for approvals. Developers route around controls. Shadow IT proliferates.

- **The new model: Security as guardrails.**
- Self-service security catalogs — engineering teams get pre-approved patterns, not tickets
- Risk acceptance owned by business leaders — not security holding the pen
- Governance frameworks that enable speed, not friction

- **The CISO's innovation imperative:**
- If your security program slows the business down, the business will find ways around it. The most innovative CISOs build programs that make the secure path the easy path.

The Regulatory Tailwind

- **Regulation is no longer lagging — it's pushing innovation.**
- **SEC Cybersecurity Rules:**
- Material incident disclosure in 4 business days. Board-level cyber governance is now expected.
- **DORA (EU):**
- Operational resilience testing, third-party risk mandates, ICT incident reporting.
- **NIST CSF 2.0:**
- New "Govern" function elevates cyber risk management to enterprise governance.
- **The opportunity:**
- Use regulatory requirements as a catalyst to modernize, not just a compliance checkbox.

What Separates Leaders from Laggards

- **Laggards:**
- Treat cybersecurity as an IT cost center
- React to incidents after the fact
- Measure success by audit findings closed
- Run security as a tollbooth

- **Leaders:**
- Position cybersecurity as a strategic business function
- Invest in proactive threat hunting and continuous validation
- Measure success by operational resilience and time-to-detect
- Build security guardrails that accelerate the business

- **The board isn't asking "are we secure?" They're asking "are we resilient?"**

Three Takeaways for This Room

- **1. Identity IS your perimeter.**
- If you haven't reimagined IAM as a strategic capability, start now. Zero Standing Privilege, continuous authentication, and machine identity governance are table stakes.

- **2. AI defense must match AI offense.**
- Deploy AI where it delivers measurable outcomes — behavioral analytics, automated triage, threat intel synthesis. Be skeptical of vendor hype without explainability.

- **3. Make security the easy path.**
- The organizations that innovate fastest are the ones where security enables velocity. Guardrails, self-service, and business-owned risk acceptance are the future.