Summary & Notes
Atlantic City CyberSecurity & Fraud Forum 2025

Review all materials, presentations, abstracts, Discussion Leader bios, and more on the **CxO Security Forum Online Community Portal**.

Forum Website (additional details): https://cxosecurityforum.com/AC/

The full Agenda can be found in the Online Forum, available as a .pdf via this link: https://hubs.ly/Q03Ls1rl0

Executive Summary

The 2nd Annual **Atlantic City CyberSecurity & Fraud Forum** brought together more than 100 executives, law enforcement leaders, academics, and practitioners to confront the fast-shifting realities of cyber risk, fraud prevention, and digital governance. Over twelve sessions, the Forum reinforced a clear mandate: cybersecurity is firmly a boardroom and regulatory priority, not just a technical concern.

Participants explored how vendor sprawl, AI disruption, and regulatory exposure are reshaping enterprise decision-making. **Richard Stiennon** mapped the 4,550-vendor ecosystem, underscoring the need for sharper vendor evaluation and AI reality checks. **Chase Cunningham** revealed how predictable market rebounds create “buy the breach” investment strategies, while reminding leaders that incident costs ultimately cascade to consumers.

Government leaders from the FBI, Secret Service, IRS-CI, DHS, and NJCCIC emphasized collaboration and rapid reporting as critical force multipliers in disrupting

cybercrime. Healthcare CISOs highlighted AI governance as a proving ground, balancing innovation with compliance. Negotiator **Kurtis Minder** exposed the psychology of adversaries, while **Mark Sangster** pressed leaders to confront biases, stress, and communication gaps in crisis decisions.

Legal and regulatory risks loomed large, with the **TD Bank case** reframing compliance failures as criminal negligence. Workforce sessions showcased the urgent need for mentorship, certifications, and practical training to close a 700,000-job skills gap. Finally, **Dr. Robert Riegle** urged a paradigm shift: in an era of autonomous systems and supply-chain risk, organizations must "verify before trust."

The Forum closed with a call to action: transform insight into impact by refining governance, exercising playbooks, strengthening partnerships, and building trust at every edge of the enterprise.

Supporting Solution Providers

Our sincere gratitude to our primary Solution Providers, who made the Forum possible via their financial support

Blumira

Blumira delivers enterprise-grade detection and response without the complexity or high costs of traditional SIEM solutions. Built for lean IT and security teams, Blumira combines automated threat detection, guided response, and expert support in one easy-to-use platform. By integrating quickly with your existing environment and surfacing actionable insights in minutes—not months—Blumira empowers organizations of all sizes to improve their security posture, stop attacks early, and meet compliance needs without adding headcount or overhead.

ThreatLocker

ThreatLocker is redefining Zero Trust security with a simple yet powerful approach to protecting organizations from cyberattacks. By combining application allowlisting, Ringfencing™, storage control, and privileged access management, ThreatLocker gives IT and security teams precise control over what can run and who can access sensitive data. Built for speed, scalability, and ease of use, the platform stops threats before they

spread—without slowing down business. Trusted by thousands of organizations worldwide, ThreatLocker helps teams lock down their environments, reduce risk, and stay ahead of evolving cyber threats.

Some Overarching Themes

- **Vendor Sprawl & AI Reality Checks**
  With 4,550+ vendors crowding the market, leaders must cut through noise, test vendor claims, and evaluate cultural and regional origins. AI is reshaping the field, but executives must separate engineered innovation from marketing hype.
- **Failure Is Expensive — and Predictable**
  Cyber incidents carry rising costs, yet markets often rebound. While breaches punish unprepared firms, disciplined defenders and investors can read the signals to their advantage.
- **Collaboration as a Force Multiplier**
  The FBI, Secret Service, IRS-CI, DHS, and NJCCIC emphasized the importance of rapid reporting, information sharing, and public–private partnerships. Time-to-report directly impacts the ability to disrupt criminal activity and recover assets.
- **Healthcare as a Test Case for AI Governance**
  Hospitals illustrate the tension between rapid AI adoption and strict regulatory compliance. Lessons learned — from synthetic data to human oversight — apply across industries navigating AI governance.
- **The Human Element of Cyber Conflict**
  Whether it's executive decision-making under stress or direct negotiations with ransomware gangs, leadership psychology and negotiation tradecraft matter as much as technical defense.
- **Legal and Regulatory Exposure**
  The TD Bank case reframed weak cyber controls as criminal negligence under the Bank Secrecy Act. Leaders now face personal and organizational liability if digital asset oversight fails.
- **Fraud and Cybersecurity Convergence**
  Fraud prevention is no longer just finance's responsibility. Unified "Cyber-Fraud

Fusion" teams improve detection and reduce losses by combining intelligence across domains.

- **The Workforce Gap**
  Despite "700,000 open cybersecurity roles," graduates often lack real-world readiness. Solutions include internships, mentorship, capstones, and tighter industry–academic alignment.

- **Trust at the Edge**
  In an era of autonomous systems, AI-driven disinformation, and supply chain risk, authenticity must be provable at the device and data level. The model is shifting from "trust but verify" to "verify before trust."

Priority Actions for Leaders

1. **Refine Vendor Evaluation**: Focus on evidence, AI substance, and vendor origin
2. **Update Governance Models**: Integrate cyber risk into board-level KPIs and decision frameworks
3. **Strengthen Partnerships**: Build relationships with FBI, InfraGard, and fusion centers before crises
4. **Exercise Playbooks**: Include negotiation, fraud convergence, and regulatory scenarios in tabletop drills
5. **Harden Compliance Links**: Align security and compliance teams to prevent legal exposure
6. **Invest in Workforce Pipelines**: Support internships, mentorship, and cert-first pathways
7. **Adopt Edge Trust Practices**: Pilot device attestation and supply chain verification

Session Summaries

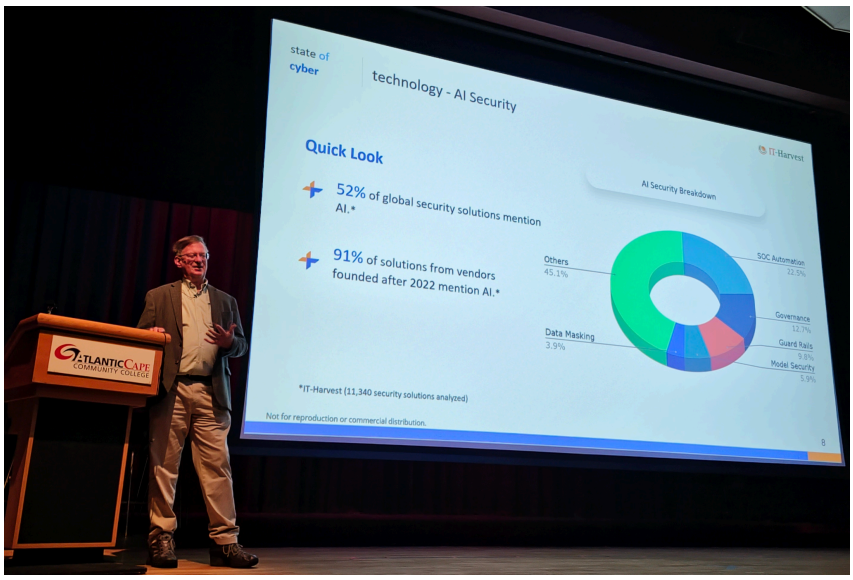
Discussion Pod #1:

The State of Cybersecurity 2025 – Mapping the Industry, Measuring AI's Real Impact, and Making Sense of 4,550 Vendors

Discussion Leader: Richard Stiennon (IT-Harvest)

Context / Introduction

A veteran analyst and industry provocateur will kick off the Forum, taking us on a data-rich tour of the entire cybersecurity industry—all 4,550 vendors, 660 subcategories, and $12 billion in recent funding. Drawing from his forthcoming book Security Yearbook 2025, Stiennon will share insights derived from two decades of studying cyber trends at Gartner and now IT-Harvest—the only firm systematically cataloging the global cyber vendor ecosystem.



Main Flow / Core Points

- Vendors grew from ~600 (2003) to 4,500+ today
- ~7% acquired yearly, but industry keeps expanding
- 47% of companies adding headcount (down from >50%).
- AI security fastest growth: 161 startups, $2.5B invested, $2.7B ROI.
- Global spread: US 72% (Bay Area heavy), Israel 300 vendors (global mindset),UK/Germany ~300 (local focus), Canada rising.
- Largest category: GRC (~574 vendors). Network shrinking.
- Netskope IPO signals "SASE wars" with Cato Networks

Case Studies / Examples

Israel: Military-driven innovation engine spawning high-growth vendors.

Germany: Strong trust in homegrown security firms, demonstrating cultural impacts on vendor selection

AI security: Emerging as its own fast-growing category, distinct from traditional cybersecurity.

Notable Quotes

“Journalists always say the industry is consolidating—yet it keeps expanding.”
“AI security is the fastest growing segment I’ve ever seen.”

Challenges & Critiques

- Buyers lack clarity on how to differentiate meaningful solutions from marketing noise
- Executives struggle to connect vendor promises with business needs and outcomes

Takeaways / Recommendations

- Don’t assume consolidation solves complexity
- Probe AI claims carefully
- Consider vendor origins.
- GRC boom shows rising regulation maturity

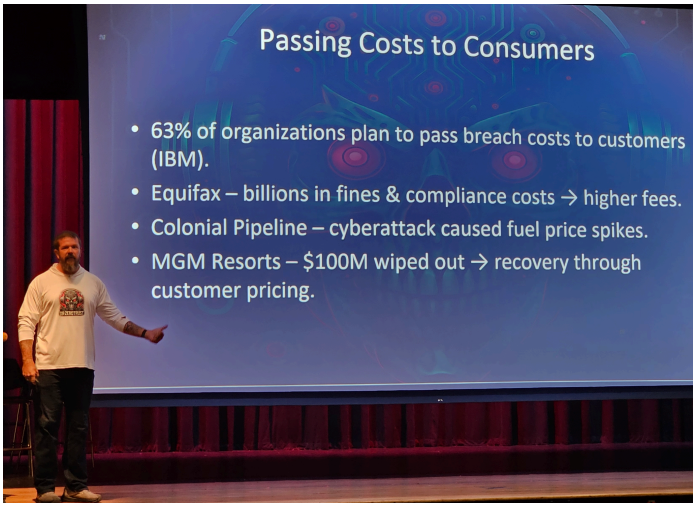
Reflection / Links

Set the strategic frame for the day: vendor selection, AI reality checks, regional/market dynamics. More info: https://share.google/195QxYU1REJ1V089R

Discussion Pod #2

#BuyTheBreach: How Cyber Failures Can Fund Your Future

Discussion Leader: Dr. Chase Cunningham - “Dr. Zero Trust”

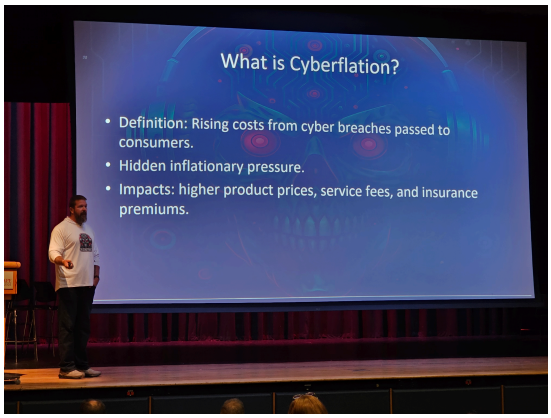


Context / Introduction

Ph.D. the Author of “Buy the Breach: Hacking Failure for Market Success,” is also known to cyber leaders as “Dr. Zero Trust.”

Main Flow / Core Points

- Breach costs rising: average U.S. breach now ~$10M.
- 78% increase in breach frequency (2022–23).
- Cyberflation Index outpaces CPI—businesses push costs to consumers (e.g., fuel, credit monitoring, higher service fees).
- Sector impacts: healthcare $10M avg. breach cost; energy costs spike 50–130%; banks add new fees; retail prices rise.
- Cyber insurance premiums up 50–100% in 2 years; compliance and litigation add to costs



- Executives rarely penalized—record payouts even after major failures (e.g., CrowdStrike CEO $46M after outage)
- Stock market behavior: breach dips (6–8% short term; larger dip at 60–90 days), then rebounds within 12–18 months.
- **“Buy the Breach” strategy:** buy stock during 60–90 day dip, sell after recovery (15–30% return).
- Method validated with 10+ years of data; portfolio example showed 25% monthly gains.

Case Studies / Examples

- Colonial Pipeline: ransomware → fuel shortages → 16% price hike
- Equifax: billions in costs, offset by higher fees; consumers misled by “free” credit monitoring
- MGM Resorts: $100M lost in one week, recouped via higher customer prices
- CrowdStrike outage (2024): $10B global cost, lawsuits pending—yet stock rose and CEO paid $46M
- Other recoveries: Equifax (+35% in 1 yr), SolarWinds (+25–30%), Marriott, T-Mobile

Notable Quotes

“Cyberflation is a real hidden cost—every breach means you pay more.”
“Breaches are good for business. Stocks dip, then bounce back.”

Challenges / Critiques

- Executives rewarded despite catastrophic failures
- Insurance and compliance costs drive up consumer prices
- Public apathy—breaches fade from memory in ~60 days.

Takeaways / Recommendations

- Expect cyber costs to be passed to consumers across all sectors
- Investors can exploit predictable stock dips post-breach
- Track SEC breach reports (96-hour disclosure rule) for trading signals
- Only buy if companies respond transparently and recover credibility.

Reflection / Links

- Shows macroeconomic effects of breaches and why resilience matters.
- https://share.google/XdhP7HhxAJaXskG1h
- https://www.engagez.net/#9pnd-1923129=resource_1083931

Discussion Pod #3 (panel)

Leading the Fight: Cybersecurity & Government Agencies

Discussion Leaders: Michelle Liu (FBI), Jonathan Helmstetter (IRS-CI), Stanley Field (CISA), Krista Valenzuela (NJCCIC)

Context / Introduction

When cybercrime intersects with national security, terrorism, cross-border issues, or financial stability, the US Secret Service, Department of Homeland Security, FBI and state fusion center (NJCCIC) step in—not just with investigations, but with leadership. Drawing from real-world cases—ranging from cryptocurrency scams to insider threats—RAIC Cerra will outline lessons learned for private-sector leaders.

Main Flow / Core Points

- CISA role: advisory, non-regulatory support, offering free tools (e.g., cyber hygiene scans, Malcolm SIM)
- FBI role: first priority is helping victims, sharing IOCs/TTPs, then moving into investigation
- IRS-CI: follows the money—specialists in tracing, freezing, or seizing illicit funds, including digital assets.
- NJCCIC: provides resources (e.g., endpoint protection via federal grants), advisories, and threat bulletins for state/local entities
- Partnerships have strengthened significantly in past year—daily communication across agencies
- Incident response: early (first 24–48 hours) engagement is critical; IC3 reporting is useful but secondary
- NJ breach reporting law (2023): all public agencies/contractors must notify NJCIC within 72 hours.
- Common message: collective defense requires immediate collaboration and trusted contacts.

Case Studies / Examples

- NJCCIC grant-funded endpoint monitoring helped municipalities/schools detect incidents outside business hours
- FBI example: agents embedded with a private sector org for 72 hours during an incident
- IRS-CI: leveraging IC3 data to trace money laundering linked to cybercrime (more below regarding TD Bank investigation, case, and implications)

Notable Quotes

“When we’re attacking cyber incidents, it’s really a team sport.” — Michelle Liu
“At the end of the day, criminals do this to make money—we’re good at following the money.” — Jonathan Helmstetter
“If you’re hit, find a human to call. Our best value is in the first 24–48 hours.” — Michelle Liu

Challenges / Critiques

- Misconceptions: FBI isn’t there to “raid” companies during incidents
- Limited local resources—many small orgs can’t afford protections without grants
- Reporting delays reduce the value of data for real-time response.

Takeaways / Recommendations

- Build relationships with federal/state cyber contacts before an incident
- Report to NJCCIC (within 72 hours if required) and engage agencies quickly
- Use free resources like CISA’s cyber hygiene scans
- Early, transparent collaboration improves outcomes.

Reflection / Links

Operationalizes earlier themes: speed & collaboration are decisive:
https://www.engagez.net/#9pnd-1922367=resource_1083931

Panel

Healthcare as the Proving Ground: AI, Cybersecurity, and the Future of Regulated Innovation

Discussion Leaders: Douglas Copley (AtlantiCare), Hugo Lai (Temple Health), Panelists

Context / Introduction

Douglas Copley: 30+ years in IT/security, 13 years in healthcare, founder of Michigan Healthcare Cybersecurity Council. Focused on governing AI in healthcare to manage risk

Hugo Lai: CISO at Temple Health (4 years), joined after a breach; healthcare system serving underserved communities. Focused on improving patient outcomes through AI efficiency.

Main Flow / Core Points

- AI is critical for healthcare outcomes, especially in imaging and clinical workflows
- Integration of personal health devices (smartwatches, Oura rings) is desirable but technically challenging
- Regulation: healthcare is already highly regulated; more guidance is preferred over strict new rules
- Human oversight is essential to validate AI-generated outputs
- Data governance: AI models must maintain referential integrity while de-identifying patient data
- Cybersecurity priorities: focus on foundational controls, third-party risk, and resource-limited hospitals
- Collaboration among CISOs for best practices and vendor evaluation
- HIPAA needs modernization to balance confidentiality with availability and operational continuity.

Case Studies / Examples

- AI for MRI, CT, PET scans to detect conditions faster
- Clinical AI agents transcribing and recommending physician actions

- Michigan Healthcare Cybersecurity Council is helping smaller hospitals implement cybersecurity

Notable Quote

“AI must improve outcomes — otherwise it’s a distraction.” (Paraphrase)

Challenges / Critiques

- Rapid AI development vs. slow regulatory adaptation
- Limited integration of personal devices into Electronic Medical Records (EMRs)
- Balancing efficiency with human oversight
- Smaller hospitals lack resources, not knowledge, for cybersecurity

Takeaways / Recommendations

- Focus on foundational cybersecurity controls at high quality
- Evaluate third-party risks for AI solutions
- Ensure human validation of AI outputs
- Collaborate with peer CISOs for guidance and best practices
- Preserve data integrity while de-identifying patient information

Reflection / Links

Healthcare shows governance lessons applicable to other regulated sectors

Discussion Pod #4

Inside the Mind of the Adversary: Espionage, Negotiation, and the Battle for Digital Control

Discussion Leader: Kurtis Minder, Cyber-Espionage Expert and Author, Cyber Recon:

Context / Introduction

Kurtis Minder shared his 30+ years of experience in cybersecurity, including founding Groupsense, a company specializing in cyber espionage and ransomware negotiation. His work focuses on understanding threat actors, engaging in direct communication, and mitigating cyber risk for organizations.

Main Flow / Core Points

- **Cyber Espionage & Dark Web Monitoring:** Minder's company, Groupsense, communicates directly with cybercriminals to validate threats and monitor the dark web.
- **Ransomware Negotiation:** Shared experience negotiating ransoms, reducing a $2M demand to $120K, showing the mix of strategy, psychology, and technical knowledge
- **Threat Actor Profile:** Modern attackers are organized businesses with salaries, quotas, and profit motives; they target suppliers for maximum impact
- **Initial Access Brokers:** Individuals or groups sell network access on dark web marketplaces; ransomware actors then exploit these vulnerabilities
- **Data Exfiltration & AI Use:** Attackers now steal large amounts of data and may use AI to extract sensitive information efficiently
- **Incident Response & Planning:** Emphasized the importance of testing and preparing response plans before an attack occurs
- **Ethical Considerations:** Discussed moral dilemmas in ransom payment and tracking how money is used by attackers
- **Empathy in Negotiation:** Understanding the human side of threat actors improves negotiation outcomes without condoning actions

- **Civic Responsibility:** Encourages basic cyber hygiene for individuals and employees to reduce national cyber risk

Case Studies / Examples

- Negotiated a ransomware attack for a publicly traded software company, saving millions.
- Charity ransomware case: negotiated a reduced ransom of $5,000 instead of $2M.
- Insider threat case involving a law firm and sensitive files on a high-profile case.
- Examples of initial access broker activity on the dark web, including the sale of government network access

Notable Quote

“Just like you don’t have to be a doctor to know how not to die, you don’t have to be a cybersecurity expert to practice basic cyber hygiene.”

Challenges / Critiques

- Organizations underestimate operational impacts of ransomware, treating incidents as mere nuisances rather than full business interruptions
- Cyber incident response plans are often outdated or untested, failing under real attack scenarios
- Negotiating with professional threat actors requires balancing empathy, strategy, and legal/ethical considerations

Takeaways / Recommendations

- Exercise incident response playbooks
- Map supplier ecosystems
- Train negotiation/empathy skills

Reflection / Links

Human side of cyber conflict; shows why governance & collaboration matter.
https://www.engagez.net/#9pnd-1923144=resource_1083931

Discussion Pod #5

Cyber-Conscious Leadership: Boardroom Issue vs IT Problem

Discussion Leader: Mark Sangster, Author "Cyber-Conscious Leadership"

Context / Introduction

Mark Sangster goes beyond the headlines and surface-level frameworks to expose the invisible forces that shape today's most devastating breaches. Drawing from his books "Cyber-Conscious Leadership" and "No Safe Harbor," Mark unpacks real-world case studies—ransomware attacks that began as innocent supplier emails, regulatory landmines triggered by seemingly minor missteps, and grey zone attacks that blur the lines between criminal and nation-state actors.

Main Flow / Core Points

Cyber-Conscious Leadership: Leaders must connect technical issues to business impact and manage stress, awareness, and emotions to make sound decisions.

Decision-Making Under Pressure: Executives often decide alone despite advisors—clarity, credibility, and timeliness in communication are essential.

Team Dynamics: Cybersecurity teams embody personas (Cowboy, Martyr, Hinderer, Magpie, Governor, Lawyer); balance of traits strengthens response but unmanaged behaviors create risks.

Cognitive Biases: Hindsight, outcome, confirmation, and time biases distort judgment during incidents; awareness helps teams act more objectively.

Incident Response Best Practices: Regular simulations, defined roles, cross-business collaboration, listening to experts, and leading by example build resilience.

Boardroom Engagement: CISOs earn trust through steady communication, scenario exercises, and educating boards on the financial and strategic stakes of cyber risk.

Case Studies / Examples

- Cowboy CEO paid ransom without involving advisors → lost insurance coverage and $50M business value *(it was a great story!)*
- FEMA liaison developed trust with DHS Secretary → clear communication allowed urgent matters to be prioritized.

Notable Quote

Uniquely, “Cyber crimes are crimes you have to self-manage.”

Challenges / Critiques

- Team dysfunction from certain personas (e.g., hinderers, magpies)
- Emotional responses and biases can impair incident decisions
- Misalignment between IT teams and board understanding

Takeaways / Recommendations

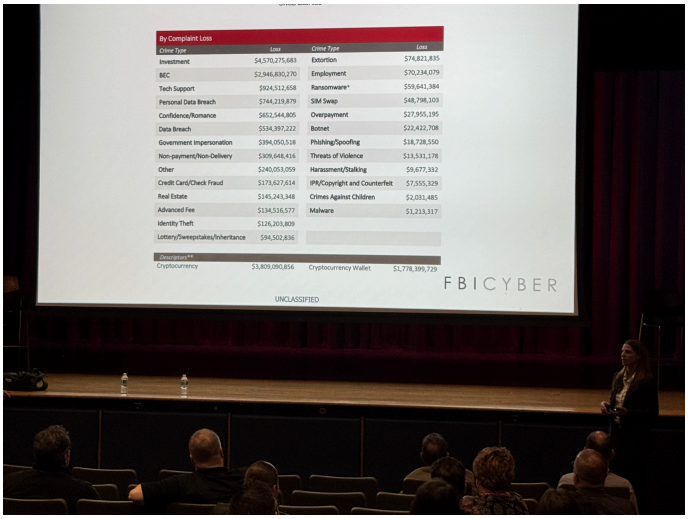
- Build teams with complementary personas; train through scenarios.
- Manage stress and biases consciously.
- Engage leadership in meaningful, trust-based communication.
- Focus on actionable information & decision-making frameworks (Sacro Red)

Reflection / Links

- Cybersecurity leadership is as much about human psychology and communication as technical knowledge.
- Effective incident response requires preparation, empathy, and structured team dynamics
- https://www.engagez.net/#9pnd-1922607=resource_1083931

Discussion Pod #6

Threats, Trends & Trust: Cybersecurity Collaboration with the FBI and InfraGard



Discussion Leader: Supervisory Special Agent **Michelle Liu** (FBI Newark)

Context / Introduction

- Cybersecurity leadership is as much about human psychology and communication as technical knowledge.
- Effective incident response requires preparation, empathy, and structured team dynamics

Main Flow / Core Points

Cybercrime Landscape: Phishing and spoofing surpass ransomware in frequency, while financial fraud and business email compromise cause the biggest monetary losses.

Human Weakness: People remain the most exploited vulnerability in cyberattacks.

Negotiation Dynamics: Some organizations negotiate with attackers to limit losses or gather intel, with the FBI supporting through intelligence—not direct response.

Social Engineering Risks: Threat actors exploit poor identity verification, MFA bypasses, and public info; stronger policies and help desk protocols are critical.

Collaboration & Resources: Agencies like CISA, IC3, NJ Cyber, and the FBI provide guidance, intelligence, and support—organizations are urged not to handle incidents alone.

InfraGard Partnership: InfraGard is a vetted nonprofit partnership between the FBI and the private sector, dedicated to protecting U.S. critical infrastructure. Through cross-sector collaboration, information sharing, and initiatives such as

anti-human trafficking, it connects industry leaders, government officials, and law enforcement to advance national security.

- InfraGard website: https://infragard.fbi.gov/
- More info, contact Alex Tarabour, atarabour@infragardnj.org

Case Studies / Examples

- Business email compromise leading to financial loss in mortgage brokers.
- Social engineering call scenarios showing weaknesses in identity verification and MFA bypass.
- Shiny Hunters attack: AI-assisted social engineering.

Notable Quote

“People are the weakest link in all of these crimes.” – SSA Michelle Liu

Challenges / Critiques

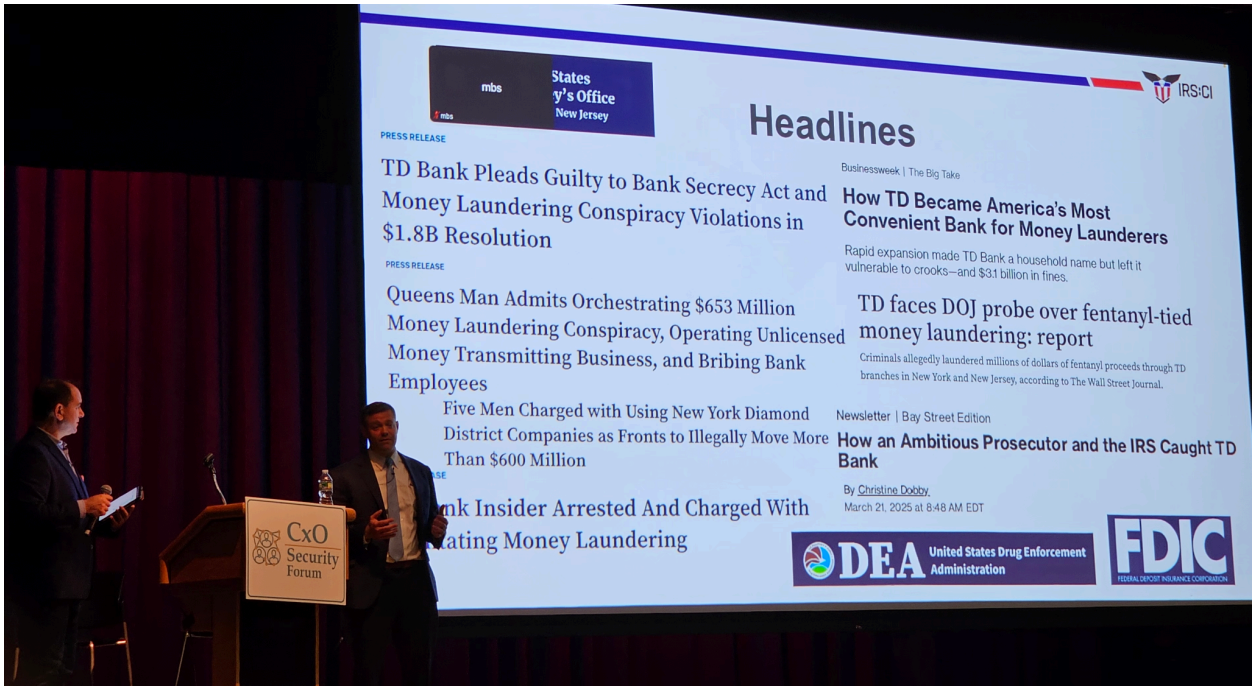
- Organizations may fail to escalate incidents or enforce proper verification protocols
- Outdated contact information and insufficient identity verification increase vulnerability
- Fear of retaliation or exposure can prevent organizations from reporting incidents to law enforcement

Takeaways / Recommendations

- Build FBI/InfraGard contacts.
- Maintain incident data readiness.
- Educate execs about law enforcement.

Reflection / Links

Stresses urgency of escalation & collaboration.



Discussion Pod #7

It's Not Just Bad Hygiene — It's Criminal Negligence (TD Bank Case)

Discussion Leader: Special Agent Jonathan Helmstetter (IRS-CI)

Context / Introduction

- Focus: TD Bank case study on **criminal negligence in anti-money laundering (AML) compliance** and lessons for financial institutions and cyber teams.
- Highlights how poor processes and willful blindness can lead to criminal liability.

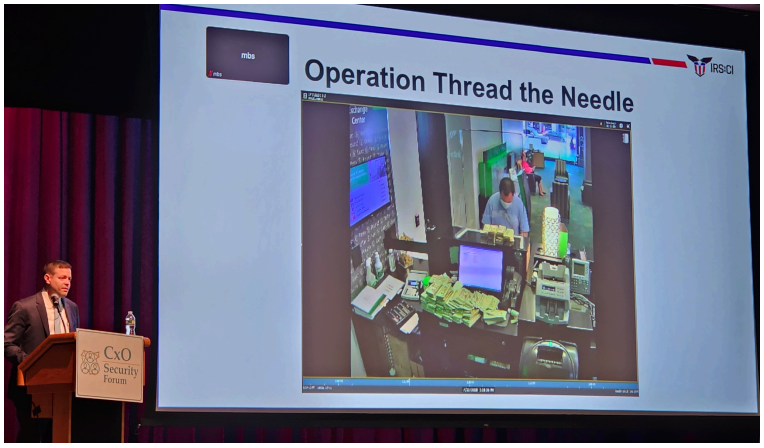
Main Flow / Core Points

Case Trigger & Scope: FinCEN data-mining uncovered laundering schemes—Operation *Thread the Needle* (cash deposits) and *4 C's* (diamonds/jewelry)—centered on TD Bank's compliance failures.

- **AML Oversight Failures**: Weak monitoring included ghost transactions, poor SAR review, inadequate due diligence, fake documents, outdated AML software, and even insider complicity
- **Investigation Findings**: Over $563 million laundered through TD Bank, with seizures of $3.7M cash and $1M jewelry/gold

- **Legal Outcomes**: TD Bank pled guilty to conspiracy to launder money, facing a record $3.9B fine; multiple individuals convicted
- **Remediation Measures**: DOJ/FincEN monitorship, retroactive SAR filings, and staffing upgrades to strengthen AML compliance
- **Regulatory Lessons**: Banks can be criminally liable for willful blindness; new rules (Genius Act, stablecoins oversight) extend compliance burdens, pulling in cyber/security teams when identity and access controls falter

Case Studies / Examples



- **Operation Thread the Needle**: Cash laundering through TD Bank branches, unreported and improperly documented
- **Operation 4 C's**: Laundering using diamonds and jewelry; TD Bank failed to detect linked accounts
- Insider bribery via Starbucks gift cards to bypass reporting (!!)

Notable Quote

"Cybersecurity failures can result in criminal enforcement risk."

Challenges / Critiques

- Bank's AML department **understaffed and undertrained**, unable to handle volume or evolving schemes
- Lack of proactive monitoring for new technologies and money laundering typologies
- Reliance on outdated procedures and failure to adapt to new regulatory guidance

Takeaways / Recommendations

- Strengthen KYC/AML controls. (and how KYC is like Identity & Access Management - IAM)
- Align compliance & cyber.
- Tight, auditable governance is needed.
- Early verification, continuous monitoring, and regular staff training are critical.

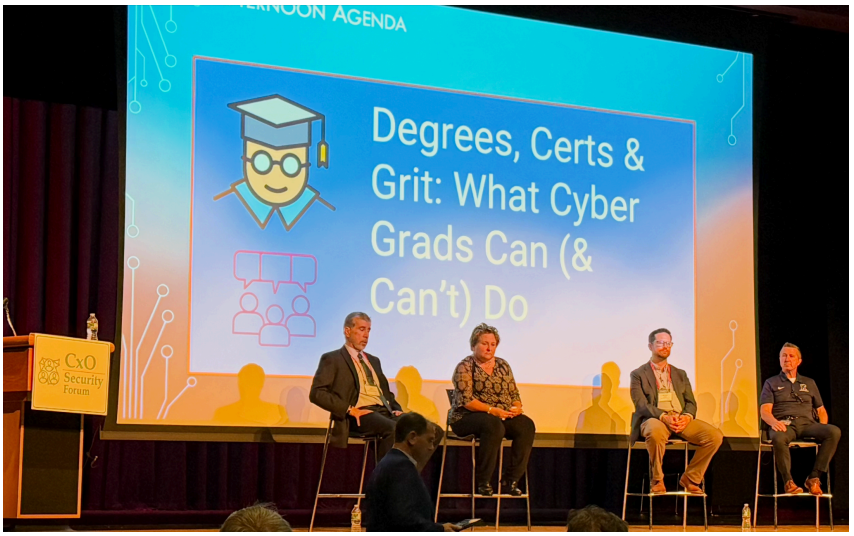
Reflection / Links

Wake-up call linking cyber failures to legal exposure

Panel

Degrees, Certs & Entry-Level Grit: What Cyber Grads Can (& Can’t) Do

Discussion Leaders: Dr. Stan Mierzwa, Prof. Michael Zambotti, Dr. Otto Hernandez, Tammy Klotz (CISO, Trinseo)



Context / Introduction

Focus: bridging the gap between academia and industry, highlighting degrees, certifications, and job readiness.

Main Flow / Core Points

- **AI & human skills:** Gen AI complements, not replaces, humans. Critical thinking, creativity, communication, and resilience remain essential
- **Certifications:** Programs integrate industry certifications (e.g., CompTIA) alongside degrees to enhance employability
- **Soft/Power Skills:** Communication, ethics, problem-solving, and adaptability are emphasized
- **Internships & industry partnerships:** Key to experience, employability, and connecting students with local employers
- **OT/IT exposure:** Courses cover risk management, IOT/OT elements, and cross-disciplinary skills

Case Studies / Examples

- Labs, industry projects, hackathons.

Notable Quotes

“Your tech skills will get you hired; your soft skills will get you promoted.” – Otto Hernandez
“Students may meet 30–40% of a job posting’s requirements—send the application anyway.” – Stan Mierzwa
“AI will replace those who don’t use it, not the profession itself.” – Tammy Klotz

Challenges / Critiques

- Rapidly changing tech landscape requires curriculum agility.
- Job postings often demand 5+ years of experience for entry-level roles.
- Students sometimes lack foundational professional skills like communication and etiquette.
- Industry skepticism of AI’s impact and how it integrates with human roles.

Takeaways / Recommendations

- Consider the mix of new college hires AND training for existing staff to get the most out of AI.
- Two-year degrees plus certifications and internships can produce highly employable graduates (as opposed to traditional 4-year degree programs)
- Industry professionals can support programs through internships, guest lectures, or advisory boards
- Continuous engagement ensures curriculum aligns with evolving cybersecurity needs.

Reflection / Links

Talent pipeline health underpins SOC maturity and resilience.

Discussion Pod #8

Trust, Verify, and Authenticate: Securing the Edge in a New Era of Operational Threats

Discussion Leader: Dr. Robert Riegle, former DHS Director

Context / Introduction

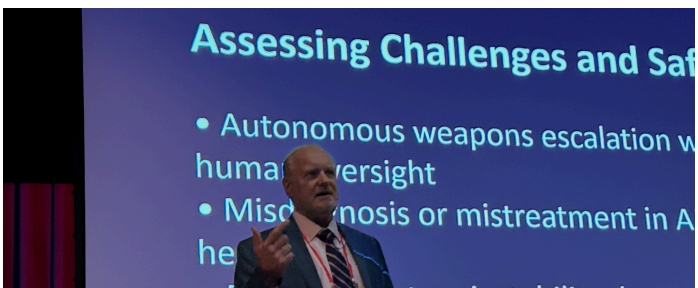
Dr. Riegle challenged participants to rethink how authenticity, attribution, and assurance must be redefined at the device and data layer, primarily for Operational Technology (OT) requirements, with implications for all of cybersecurity, risk management and fraud prevention

Main Flow / Core Points

- **AI Disruption:** Autonomous AI is rapidly changing risk landscapes; speed and scale of AI and quantum computing outpace traditional cybersecurity measures.
- **Secure by Design:** Chips and firmware must be authenticated at manufacture, with a verifiable registry of origin, intent, and ownership. Hardware becomes the critical trust anchor.
- **Evidentiary Function:** Without a verifiable origin of hardware/software, investigations and accountability are impossible.
- **Human Oversight:** Critical decisions must retain a human-in-the-loop; AI alone cannot be fully trusted.
- **Ethical and Legal Risks:** Accountability gaps, emergent behaviors, and unintended consequences will be amplified by AI.

Case Studies / Examples

- Tesla autopilot crashes highlight gaps in accountability and access to diagnostic data.
- Financial markets could be rapidly manipulated by AI-driven trading and quantum computing.
- Healthcare automation risks overdoses or errors if human oversight is removed.



Notable Quote

“Secure by design means a chip is verified, registered, and trustworthy from the moment it’s manufactured.”

Challenges / Critiques

- Industry reluctance to disclose proprietary information.
- Global supply chain issues, particularly reliance on China for chip manufacturing.
- Complexity in incentivizing compliance and implementing standardized governance frameworks.

Takeaways / Recommendations

- Begin risk mitigation at the point of origin: chip manufacturing, firmware, and biometric authentication
- Maintain human-in-the-loop oversight for all critical decisions
- Implement rigorous monitoring, testing, and audit trails validated by third parties
- Advocate for policy and legislative support to standardize secure-by-design practices and indemnify compliant industry participants.

AC CyberSecurity & Fraud Forum: Closing Reflection

The Forum underscored that cybersecurity is no longer just about staying ahead of threats. It is about **leading with purpose** — integrating resilience, governance, and human judgment into every decision. Participants leave with both a sharper awareness of today’s challenges and a clearer mandate: turn insight into impact

Special Thanks

To Atlantic Cape Community College, all our discussion leaders, the state and federal agencies who participated and supported us and our Student Ambassadors for all their hard work!