Tab 1

2025 NORTHEAST ANNUAL

CxO Security Forum

CYBERSECURITY SUMMIT

13 NOVEMBER 2025 ❖ QUINNIPIAC UNIVERSITY – NORTH HAVEN, CT

The 2025 NorthEast Annual Cybersecurity Summit (NEACS) Summary & Notes

In this document, you will find an exhaustive summary & notes from each guest speaker, panelist, and discussion for the 2025 NorthEast Annual Cybersecurity Summit.

It took place on November 13th, at Quinnipiac University's North Haven Campus.

CxO Security Forum Online Community Portal

All of the available presentation and additional reference materials have been made available on the portal, which was also used during the Summit as our Event App. This link will remain live for the next several months:
https://www.engagez.net/CxO?snc=1855104#lct=customlocation-Location10

An **AI companion** is available there, and has been trained on all these materials as well as the notes that follow.

LINKS in this document will point to the portal.

WATCH the News Coverage of the Summit from WTNH - Fox News Hatrtford HERE

Agenda Overview

Topic	Discussion Leader(s)
Mapping the AI, the Cybersecurity Industry, & 4,550 Vendors	Richard Stiennon
#BuyTheBreach: How Cyber Failures Can Fund Your Future	Chase Cunningham
Espionage, Negotiation, and the Battle for Digital Control	Kurtis Minder
From the Gov't & Here to Help: Cyber Agencies & Partnerships	DHS: David Palmbach
Cyber Insurance: What is risk transfer anyway?	Amanda Draeger
Building an AI Secure SDLC	Karun Rajasekharan
The CVE Ecosystem + AI to Fix it!	Tim Rohrbaugh
Degrees, Certs & Grit: What Cyber Grads Can (& Can't) Do	Prof. Frederick Scholl Dr. Chad Williams CCSU Dr. Tirt. Gosh UNH Mario Di Natale Mike Tetto Karun Rajasekharan

Introduction

Michael Hiskey, CxO Security Forum

The **NorthEast Annual Cybersecurity Summit** (NEACS) has a 10+ year history. Michael took it over last year, and depend the collaboration across professional associations, including more and inviting them to further craft the agenda.

Solution Providers help to support the Summit; they subsidize expenses. Participants are encouraged to take the time to understand if solutions from those firms fit their needs.
Partner Associations

ISC2 Southern Connecticut Chapter

Contact: Bryce Candelora - treasurer@isc2ct.org
Website: https://www.isc2ct.org/

- Holds speakers, monthly meetings, and events to promote cybersecurity education.
- Actively looking for speakers/presenters to deliver speeches

ISACA Greater Hartford Chapter

Contact: Peter Gutierrez - Secretary@isacact.org
Website: (https://engage.isaca.org/greaterhartfordchapter/home

- Their goal is to educate and automate the workforce in cybersecurity.
- 700+ members; 1 out of 228 chapters worldwide
- Holds numerous events throughout the year, offering CPE credits
- $175 fee, student membership is free
- Offers two new certifications:
  - ISACA Advanced in AI Audit
  - ISACA Advanced in AI Security Management

OWASP New York Metro Chapter

Contact: Guy Osa - Guy.Osa@owasp.org
Website: (https://owasp.org/www-chapter-new-york-city/)

- Opening a **CT Chapter** and are looking for volunteers (contact Guy for info)
- Goal is to educate cyber people on how to develop secure programs and projects

Agenda Detail

The State of Cybersecurity 2025: Mapping the Industry, Measuring AI's Real Impact, and Making Sense of 4,550 Vendors [Discussion Pod #1]

Richard Stiennon, veteran analyst and industry provocateur kicked 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.

Presentation on CxO Sec Forum Online Community Portal

More Info on IT Harvest

This talk was not just about the numbers. Richard broke down the practical implications for executives:

- How to navigate a vendor landscape bloated with similar claims and vague value props
- Where **AI is truly being built** in cybersecurity—what's real, what's noise, and what **agentic AI** might change
- What *vendor origin* says about product capability, reliability, and alignment with enterprise needs
- Why **vendor consolidation isn't the answer**—and what to do instead

He also spotlighted key global dynamics, such as Israel's IDF-fueled innovation engine, Germany's vendor loyalty culture, and the emergence of **AI Security** as a distinct and fast-growing segment.

If you've ever asked "What should I actually be paying attention to in cybersecurity right now?"—this is your answer. This session set the tone and context for the day, offering a strategic foundation for every discussion that follows.

Executive Summary

Richard provided a comprehensive, data-driven overview of the cybersecurity vendor ecosystem, emphasizing a market defined by rapid change, high volatility, and an AI-driven transformation. He discussed hundreds of annual acquisitions, funding rounds, and new market entrants, navigating a "funding winter." He highlighted how his analysis combines AI automation with human expertise to track vendors effectively. AI Security emerged as the most transformative and fast-growing sector, signaling profound implications for the industry's future.

Key Points

- The global cybersecurity market remains largely stable in sector rankings compared to last year.
- The industry is vibrant, growing, and rapidly shifting due to AI integration.
- There are currently 4,000+ cybersecurity vendors worldwide.

Statistics

- AI Security is the fastest-growing sector with +42% growth.
- From Q1–Q3 2024, 54% of vendors grew; from Q1–Q3 2025, only 44% grew — a noticeable slowdown.
- Around 900 vendors lack necessary funding, causing hiring freezes.
- Email security vendors are experiencing growth.

Notable Insights

- GRC (Governance, Risk & Compliance) has been the strongest sector for several years.
- Data security is also a major growth area.
- Other notable sectors:
  - IAM (Identity & Access Management)
  - Network Security
- Nearly 200 AI security vendors now exist (up significantly year-over-year).

Distribution of Vendors

- 53% – United States (especially Northern California)
- 8% – Israel
- 7% – United Kingdom
- 4% – Germany
- 4% – Canada

[Many vendors remain heavily focused on local markets]

AI Growth in Cybersecurity

- 321 cybersecurity investments this year totaling US $12.9 Billion
- AI Security Funding & Activity:
  - 200+ vendors
  - 13 acquisitions
  - $2.15 billion in funding

A Dynamic and Volatile Ecosystem

- Approximately 350 acquisitions and 450 funding rounds occur annually.

- Around 225 new companies enter the market each year, often stealthily.
- Tracking failures is challenging; analysis monitors over 4,000 active vendors using website checks and LinkedIn to confirm shutdowns.
- Current market includes 4,010 active vendors and 550 archived vendors.

Strategic Takeaways

- Adapt to AI acceleration; SOC efficiency, threat intelligence, and automation are transforming operations
- Validate rigorously; scrutinize AI claims and acquisitions through testing and due diligence.
- Track early movers; startups leveraging AI effectively can scale rapidly and define new categories.

Richard concluded by emphasizing that AI represents both a monumental opportunity and a significant challenge. A disciplined, analytical approach is essential to navigate the rapidly evolving cybersecurity landscape.

Also see the **Cyber 150:** https://cyber150.com/, Richard's analysis of the 150 hottest start-ups in the market.

- The Cyber 150 ranks startups with 50–500 employees, highlighting the fastest-growing vendors. Companies like ChainGuard illustrate simple, high-impact business models achieving rapid revenue. Data-driven tracking identifies winners and losers, highlighting a gap between quantitative insights and traditional VC gut instincts.

#BuyTheBreach: How Cyber Failures Can Fund Your Future

[Discussion Pod #2]

Chase Cunningham, Ph.D. the Author of "Buy the Breach: Hacking Failure for Market Success," is also known to cyber leaders as "Dr. Zero Trust." He led a fun, informative, and thought-provoking talk which will lead into what should be an eye-opening discussion!

Book: #BuyTheBreach (also see his many other titles)
Podcast: Dr. Zero Trust

In this talk, he shined a spotlight on one of cybersecurity's most underexplored truths: the market *rewards* failure. Drawing from his groundbreaking book, Chase walks through how cybersecurity professionals—yes, you—can outperform hedge funds without ever learning complex finance. Just by applying the same analytical skills you use to track vulnerabilities and threat actors, you can spot profitable market patterns tied to breaches, outages, and incidents.

This isn't theoretical: Chase shared real-world portfolio results, case studies from Marriott, Equifax, CrowdStrike, and others, and the exact strategy he uses to buy low during breach-triggered panic and ride the inevitable recovery wave.

Participants learned:
* How to decode SEC 8-K filings like a forensic investor
* Why public outrage rarely translates to long-term losses
* What timing data shows about the "bounce" after a breach
* How to ethically profit from chaos—while still fighting the good fight

- BuyTheBreach is a disciplined contrarian investment strategy based on the idea that:
  - Cyber breaches are inevitable.
  - Companies often recover financially, sometimes even becoming stronger (as proven by stock recovery and increase in value).
  - Investors can profit by buying after a breach once fundamentals re-stabilize.
- Cyber breaches are rising sharply, driving cyberflation as companies pass costs to consumers through higher prices, fees, and premiums.
- Major industries (healthcare, finance, energy, retail) face massive breach-related expenses and insurance hikes.

Chasse reminded the audience that he is not a licensed investor, framing his talk as data-driven guidance rather than financial advice. He emphasized that his insights are based on publicly available data, asserting that mathematics and data remain the ultimate truths in the field.

Cyberflation: The Core Crisis

- "Cyberflation" is the phenomenon where rising costs from cybercrime are passed down to consumers.
- **Mechanisms Driving:** Companies facing escalating cybersecurity costs, investor pressure, and market volatility often pass these costs to end consumers.
- Traditional economic metrics, such as the Consumer Price Index (CPI), fail to fully capture the pervasive impact of cyberflation.

Rising Cost of Breaches: Since 2020, global cyber incident costs have doubled. The U.S., despite high cybersecurity spending, remains a highly targeted market.

Increasing Breach Frequency: Cyberattack frequency surged by 78% over a two-year window, with attackers increasingly targeting small and medium businesses (SMBs).

- Consumers are effectively paying a hidden “cyber tax,” impacting prices across almost all products and services globally.

Turning Cyber Incidents Into Investment Opportunities
A data-driven investment methodology leveraging predictable market reactions following public cyber incidents.

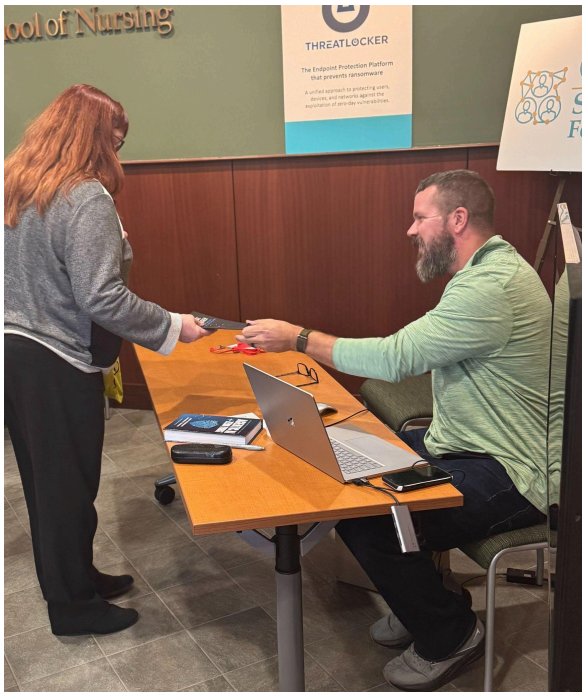
- TIMING AND STRATEGY: Optimal stock purchase window: 60–90 days post-breach (typically 70–77 days).

Strategy Steps

1. Buy after the initial dip.
2. Hold for recovery, often exceeding pre-breach levels.
3. Sell half at recovery, allowing the remainder to continue appreciating.
4. Optionally, transfer profits into high-yield alternatives such as Ethereum staking (22% APY).

Cyber Breaches Fuel Growth

- Breaches drive demand for cybersecurity solutions; existing customers often increase spending post-incident
  - Vendor Examples: CrowdStrike, Zscaler, Palo Alto, and Qualys demonstrate repeated revenue growth post-breach, likened to “Big Pharma for Cyber.”
- Historical data shows that companies responding rapidly and effectively recover within approximately 90 days.



Sector-Specific Observations

- Finance & Retail: Strong post-breach rebounds; prime Buy the Breach opportunities.
- Healthcare: Major breaches create high-value market opportunities.
- Manufacturing & Oil & Gas: Recovery is slower and less predictable.

Public Perception and Breach Impact

- Consumer behavior rarely changes after breaches.
- SEC fines or cyber insurance claims are often treated as routine costs.
- Effective communication and remediation accelerate stock recovery.

Practical Investment Guidelines

- Focus on breaches involving PII, HIPAA, PCI, or other high-trust data.

- Avoid poorly managed companies with weak IP protection.
- Monitor post-breach recovery trends to inform buy/sell decisions.
- Track earnings cycles; public relations responses influence recovery speed.

Notable Examples

- **Equifax:** 35% stock drop, full recovery within one year.
- **Marriott, SolarWinds, T-Mobile:** ~90-day recovery patterns.
- **Blue Cross Blue Shield & United Health:** High-value Buy the Breach opportunities.

Post-Breach Best Practices & Investment Strategy

- **Assess the breach**: scope, type, potential impact, response quality, financial stability, and legal fallout.
- **Optimal action window:** 16–90 days post-breach. Verify breaches via SEC Edgar rather than social media.
- Diversify investments across multiple breaches and employ repeatable hedge fund strategies.
- Leverage automation for opportunity detection using API bots, Discord alerts, and trading platforms such as Robinhood.

Inside the Mind of the Adversary: Espionage, Negotiation, and the Battle for Digital Control [Discussion Pod #3]

Kurtis Minder has spent the last decade doing what most cybersecurity professionals only read about—**negotiating directly with cybercriminals**, including ransomware gangs, nation-state affiliates, and digital extortionists. As the founder and CEO of GroupSense, Minder built a world-class cyber espionage team, managing over 4,000 personas in multiple languages. He helped victims navigate headline-making ransomware attacks, and briefed everyone-from Congress to the Intelligence Community.

Kurtis' TEDx Talk "What You Need to Know About Ransomware": https://www.youtube.com/watch?v=m9lTueRnUY8

Kurtis draws from his new book, Cyber Recon, and his real-world experience leading some of the largest ransomware response efforts globally. Kurtis Minder delivered a compelling, experience driven overview of ransomware, incident response, and the national security implications of modern cybercrime. Drawing on decades of hands on experience and his leadership at GroupSense, Minder explained how seemingly small breaches can cascade into systemic risk, how the access economy and commoditized ransomware tools

have lowered the bar for attackers, and why incident response must evolve from ad hoc firefighting to practiced, negotiation aware, and intelligence driven operations. His talk combined technical insight, real world anecdotes, and actionable guidance for organizations of all sizes.

Blending operational insights with personal stories—from fake identities like “Vinny,” to briefing Congressional subcommittees—Kurtis offers a rare, behind-the-scenes look at the human element of cyber conflict. Whether you lead security for a Fortune 500 or a regional bank, you’ll leave with **concrete lessons on digital risk, negotiation, and resilience in the age of cybercrime.**

- Ransomware is accelerating, becoming easier to execute but far more destructive—shifting from minor disruptions to full business shutdowns.
- Hackers treat victims as “clients,” using ransom notes to detail stolen data and threats (but not the ransom amount), and stolen credentials can cascade into wider breaches due to global interconnection.
- ~80% of attacks originate from Russia/Eastern Europe, with extorted money partially funding military activity; victims often face a choice: pay or go out of business.
- Defense alone isn’t enough—businesses must invest in stronger frontend protection and overall resilience.
- Hackers cannot be trusted to honor promises, as some operate under governments that reward or protect them, such as amnesty policies.

Professional Background & Motivation

Minder described his 30 year security career and his role in founding GroupSense, a firm known for cyber espionage tracking and counter intelligence. Over the past decade-plus, he

increasingly engaged in ransomware incident response initially through opportunistic negotiations that reduced ransom payments, and later through repeated engagements for insurance carriers, law firms, and pro bono small business support. These experiences shaped his view that negotiation and intelligence are core elements of modern incident response.

Ransomware Trends & Industry Observations

- **Scale and Sophistication:** Ransomware frequency is increasing. The proliferation of marketplaces and ransomware as a service tools has dramatically lowered the technical threshold required to launch impactful attacks.
- **Commoditization of Access:** Initial access marketplaces and brokerage services enable attackers to buy ready made entry points for a wide range of organizations.
- **Lowered Skill Floor:** Attackers no longer need deep technical expertise; they can assemble attacks by purchasing access and leveraging automation.

Human & Organizational Costs of Breaches

- The impact of a breach extends well beyond immediate technical remediation. Key long term costs include:
    - **Morale and retention:** Angry or burned employees who leave impose hiring and training costs; replacing skilled staff is expensive and disruptive.
    - **Reputational damage:** Trust lost with customers and partners can take years to rebuild.
    - **Operational drag:** Business continuity interruptions and the time executives spend managing crises reduce long term productivity.

To Pay or Not to Pay: Values are the First Decision “Gate”

- Before tactical decisions are made, foundational question: “Does paying a ransom conflict with your organization’s core values?”
- This values based gate helps leadership decide whether paying is even an option. Examples:

- A healthcare provider bound by the Hippocratic principle “first, do no harm” may conclude that failing to restore critical services would violate its mission making payment an unavoidable, if painful, choice.
- Small community businesses and family firms face existential risk; for them, paying a ransom might be the only alternative to collapse.
- **Ransom decisions should be explicit, aligned with stated values, and documented as part of an incident response policy.**

Legal & Policy Considerations: Should Paying Ransoms be Illegal?

- **Argument for prohibition:** If ransoms are illegal, demand should fall and extortion could become less profitable.
- **Practical downside:** Banning payments may simply drive transactions underground, reduce transparency, and remove visibility for regulators and investigators increasing overall risk.
- **Human consequences:** For small businesses and mission critical care providers, the inability to pay could mean going out of business or endangering lives.
- **Visibility & Attribution Challenges:** Since ransom payments are commonly transacted via cryptocurrencies, so highly unattributable flows that hinder governance and oversight. Criminals and intermediaries will likely find workarounds if payments are criminalized, eroding detection and law enforcement intelligence.

Kurtis has briefed congressional committees on these tradeoffs and argued that policy must consider practical outcomes, not just theory.

Ransom prohibition is attractive in theory but risky in practice without parallel investments in detection, resilience, and conditional insurance reform. Accountability and governance must be balanced with realistic support for organizations that face existential threats. A multifaceted approach to policy, investment, operational maturity, and value based decision framework offers the best prospect for reducing the harms of ransomware while protecting businesses and communities.

Agencies like CISA have historically been underfunded, limiting their ability to assist with proactive measures. Increased funding and resources could enable CISA or similar organizations to support both prevention and recovery, providing organizations with a third option besides paying ransom or going out of business.

A “Third Option”: Invest on the Front End

- Rather than a binary pay-or-die outcome: proactive, front end investment to reduce breach likelihood and blast radius. Elements include:

- **Stronger baseline security:** Microsegmentation, privileged access management, and modern identity controls to limit lateral movement.
- **Early detection & threat hunting:** Reduce dwell time and scope of compromise; faster detection reduces the leverage of extortionists. Resilience planning: Faster recovery options (immutable backups, tested playbooks) so organizations can stay operational without negotiating.
- **Insurance reform & conditionality:** Align cyber insurance coverage with demonstrable security controls and incident response readiness to avoid moral hazard.
- **Community & public resource sharing:** Trusted, anonymized intelligence sharing to help small firms detect and mitigate threats before escalation.

These investments can be a way to create *real choice* for victims making paying a ransom less likely to be the only viable option.

Real-World Context

Kurtis referenced his pro bono work for SMBs (e.g., accounting firms, family run services) where boardrooms and legal counsel push toward whatever keeps the company alive. These cases underscore the moral and practical complexity that blanket policy solutions fail to address.

The Value of *Really* Practicing Incident Response Plans

Minder stressed the critical impact of regularly testing and running tabletop exercises for Incident Response (IR) plans. Organizations that practice their plans experience significantly smoother cyber incident management. Beyond operational efficiency, practicing playbooks also reduces stress for staff, akin to a preventative health measure, allowing personnel to respond calmly and confidently during real incidents.

Accountability in Software Development

Minder proposed a shift in accountability for software security, drawing an analogy to the automotive industry: if a car defect causes an accident, the manufacturer bears responsibility. He argued that software providers should similarly be responsible for vulnerabilities in their products. The current model expects organizations or IT staff to fully understand and mitigate risks associated with complex software, which is unrealistic for the average user. Holding providers accountable could reduce breaches and improve overall cybersecurity.

(more on this in the discussion of **AI-SSDLC** later in the agenda!)

Insights from IR Reports

Drawing on his experience reviewing ransomware and cyber incident cases, Minder shared insights from reports provided by attackers. While some threat actors submit minimal or dismissive reports, others provide detailed accounts of how they gained access and pivoted within networks.

Analysis of these reports reveals consistent patterns: many attacks exploit basic weaknesses such as poor email security, weak credential management, and inadequate password policies. These low-hanging fruits often have the largest impact on the overall security posture.

Key Lessons from Real-World Cases

- **Negotiation Matters:** Early, strategic negotiations can substantially reduce ransom payments and limit downstream damage.
- **Small Breaches Cause Big Problems:** Even minor compromises can be combined into high impact attacks, underscoring the need to treat every breach seriously.
- **Preparation Pays Off:** Organizations that practice incident response, maintain tested playbooks, and engage threat intelligence teams recover faster and more cleanly.

Initial Access Brokers (IABs) & the Access Economy

- **Productized access:** IABs list persistent credentials and domain level access with metadata (industry, revenue) often derived from commercial sources like ZoomInfo.
- **Automation & scale:** Buyers can plug this access into ransomware as a service platforms that automate lateral movement, exfiltration, and encryption.
- **Low barrier to entry**: With a cryptocurrency wallet and purchased access, operators of modest skills can execute large campaigns.

GroupSense's counter intelligence approach deploying thousands of multilingual personas to interrogate sellers and validate listings was cited as an effective way to verify claims and collect artifacts useful for preemptive

Closing Recommendations

- **Treat exfiltration as a strategic national risk.** Don't relegate stolen data concerns to post incident accounting there intelligence problems with national implications.
- **Invest in detection and resilience.** Faster detection and better recovery reduce attacker leverage and the need for ransom negotiations.
- **Prepare negotiation capability.** Combine legal, PR, and negotiation readiness with technical IR to improve outcomes.
- **Integrate intelligence and policy.** Ongoing monitoring of IABs, dark web markets, and crypto flows should be part of enterprise security programs.

We're From the Government, and We're Here to Help": Cybersecurity & Government Agencies - Leading the Fight!

[Discussion Pod #4]

In this talk, David Palmbach from the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) shared how they approach coordinated threat disruption with interagency collaboration alongside the US Secret Service, FBI and the Connecticut Intelligence Center (CTIC).

David Palmbach delivered a concise, practical briefing on CISA's recent activities, field observations, and ransomware insights. The session emphasized actionable guidance for organizations to improve cyber resilience, highlighting underutilized resources such as the Stop Ransomware Guides. Key topics included risk-based security, targeted controls, and emerging threats such as vulnerability exploitation by financially motivated actors. Palmbach stressed aligning security investments with operational risks rather than marketing trends or checklists.

Key Points & Takeaways:

- CISA's #StopRansomware Guide detail tactics of 21 ransomware groups and lists the open-source tools they use, enabling companies to ethically test their own systems.
- All examined ransomware actors use RDP or SMB for lateral movement, highlighting major exposure points.
- Software vulnerabilities have surged from 2015–2025, underscoring the need for secure-by-design/default development practices.
- Better coding standards and official compliance reduce exploitable flaws before deployment.
- CyHy (Cyber Hygiene) scanning continuously checks internet-facing systems for vulnerabilities and misconfigurations.
- Prioritize vendor evaluation, supply chain security, and intelligence-informed risk management
- Recognize that state actor threats, particularly PRC-linked campaigns, dominate the national cybersecurity landscape.

Field Observations: Common Gaps

- Organizations often underprioritize high-risk systems and lack strategic response planning.
- "Blind defense" is common: buying tools (EDR, XDR, AI-labeled products) without a

targeted plan.
- Small teams and limited budgets must prioritize high-leverage controls like MFA, patching, and segmentation rather than comprehensive tool coverage.

Emerging Threat: Vulnerability Exploitation

- 57% of initial access in ransomware incidents comes from exploiting vulnerabilities—a growing trend among financially motivated actors.
- Historically, zero-day exploitation was dominated by state actors (China, Russia).
- Financially-motivated cybercriminals increasingly discover and exploit zero-days themselves.

Recent trends
- ~80 zero-day vulnerabilities exploited in the wild per year, double the number from five years ago.
- **Published CVEs continue to rise;** 2025 forecast shows further growth.
    - Implication: vulnerability exploitation is a major and growing problem for both corporate and national security.

CISA Initiatives Against Vulnerability Exploitation

- Secure by Default / Secure by Design: Promotes secure coding in SDLC (Software Development Life Cycle).
- Cyber Trust Mark for IoT devices: Certification indicating devices meet baseline security standards.
- Focus on improving development practices and reducing attack surfaces.

Operational Recommendations

- **Adopt risk-based security**: prioritize assets by impact and likely attacker tactics.
- **Avoid "blind purchases":** assess whether products close real security gaps.
- Implement **high-leverage measures** for limited teams: MFA, patch prioritization, microsegmentation.
- Connect threat intelligence to mitigations and tabletop exercises.

Request CISA materials and assistance as needed; many organizations underutilize federal resources.

Supply Chain Security & Risk Mitigation

- Evaluate Vendor Security Practices
- Avoid vendors with repeated vulnerabilities.
- Review SDLC practices of new or small vendors.

Leverage Free Vulnerability Scanning

- CISA offers scanning for public-facing IPs and web apps, with weekly reports.
- Includes alerts on critical vulnerabilities exploited by state actors or ransomware groups.
- Government Intelligence as a Force Multiplier
- Early access to vetted intelligence allows rapid response.

Strategic National Priorities

In the recent past, CISA had multiple priorities. Under the new administration, the focus is very clear China. The “People’s Republic of China” (PRC) is the dominant focus due to national security implications. Organizations should integrate this perspective into risk and supply chain management.

Government Guidance & Intelligence Sharing
CISA guidance offers actionable insight into adversary motivations and TTPs (tactics, techniques, and procedures).

Reporting incidents helps build broader intelligence and informs defensive strategies.

Business Continuity & Tabletop Exercises

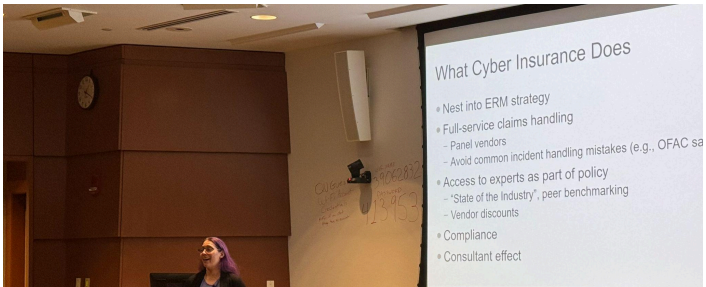
- Broaden Scope Beyond IT
- Cyber incidents affect entire operations; consider energy, communications, water, utilities.
- Effective Tabletop Exercises Include executives and department heads; small IT-only exercises are insufficient. Simulate real-world operational impacts, not just IT response.
- Focus on Business Operations:
    - Understand roles, responsibilities, and interdepartmental decision-making during incidents.
- Cybersecurity preparedness must be enterprise-wide; realistic, inclusive tabletop exercises improve readiness and resilience.

CISA Assistance - Tabletop Exercises & Organizational Support is available for organizations lacking experience: Remote guidance for small organizations, Onsite facilitation for large enterprises.

Cyber Insurance: What is risk transfer anyway? [Discussion Pod #5]

Amanda Draeger, Principal Cyber Risk Engineer, Liberty Mutual Insurance

Amanda Draeger offered a rare, insider-level look at how cyber insurance really works—demystifying underwriting, clarifying the mechanics of risk transfer, and dispelling the myth that “just buy insurance” is a cybersecurity strategy. Drawing from her experience inside one of the world’s



largest multinational carriers, she explained how cyber risk engineers bridge the gap between technical complexity and financial risk decisions, and why understanding your assets and exposures matters far more than most organizations realize.

This talk was not about selling insurance—it was about explaining its limits, its leverage, and how it fits into enterprise risk management. Amanda broke down the operational, financial, and governance implications for executives:

- Why cyber insurance transfers only financial consequences—not reputational loss, data value, or operational damage
- How brokers, underwriters, and risk engineers actually evaluate your environment
- Why outsourcing a function does not transfer risk—and sometimes creates new ones
- How exclusions (war, ransomware conditions, data valuation) shape the real boundaries of coverage
- Why reporting even “small” incidents below retention builds resilience and improves outcomes
- How current market conditions create a buyer’s advantage for organizations with mature controls

She also contextualized modern underwriting: the industry is moving away from binary yes/no questionnaires and toward maturity-based assessments reflecting how completely (and consistently) organizations apply security controls.

If you’ve ever wondered, *“What does cyber insurance really do for my security program?*”—this session provided the most candid and practical answer.

Executive Summary

Amanda provided a grounded, operationally realistic overview of cyber insurance as a financial risk transfer tool, clarifying its value, its limitations, and its place within enterprise risk management (ERM). She emphasized that insurance does not reduce cyber risk by itself; instead, it offers structured financial protection, access to vetted incident response partners, and expert guidance from cyber risk engineers.

Insurance can validate internal security priorities, accelerate stalled initiatives, and support crisis response—but it cannot replace core controls, governance, or investment in resilience. Coverage hinges on understanding exclusions, negotiating terms with knowledgeable brokers, and aligning policies with business needs. In today's soft market, organizations with strong controls are well positioned to obtain favorable terms.

The Role of Cyber Risk Engineers

- Translate technical realities into underwriting decisions
- Validate asset ownership, exposure, and control effectiveness
- Provide benchmarking across industries and peer organizations
- Navigate complex multinational legal and regulatory structures

What Insurance Actually Transfers

- Financial consequences of covered cyber incidents
- Access to full-service response teams (IR, forensics, negotiators, legal, crisis comms)
- Structured processes that help organizations avoid missteps

What Insurance Does Not Transfer

- Reputational damage
- Loss of intellectual property or intrinsic data value
- Operational disruption or loss of business advantage
- Responsibility for managing outsourced vendors

Policy Structure & Negotiation

- Policies are legal contracts; claims follow the written terms
- Brokers help match needs with carriers and negotiate endorsements
- Organizations must explicitly request coverage for specialized scenarios
- Exclusions matter: war, certain ransomware conditions, and data valuation are common gaps

Evolving Underwriting & Control Expectations

- The industry is shifting away from checkbox questionnaires toward maturity-based assessments, examining:
- Breadth and consistency of MFA
- Patch/vulnerability management effectiveness
- Open-port exposure and external attack surface
- Incident response readiness and backup testing

This reflects a more realistic evaluation of operational risk, not merely control presence.

Incident Reporting & Preparedness

Amanda strongly recommended reporting incidents even below the deductible:

- Builds familiarity with carrier processes
- Provides access to professionals who improve IR quality

- Strengthens response capabilities for future, larger events
- Creates internal awareness and improves documentation discipline

Current Cyber Insurance Market Conditions

- The current soft market favors buyers: Pricing, coverage breadth, and underwriting flexibility are better than in recent years
- Mature organizations can secure highly competitive terms
- Small and midsize organizations benefit disproportionately from full-service claims support

Strategic Takeaways

- Treat cyber insurance as one component of a broader ERM strategy—not a standalone solution
- Understand your assets and exposures before negotiating coverage
- Use brokers with deep cyber familiarity to avoid coverage gaps
- Scrutinize exclusions and understand what cannot be insured
- Report all incidents to strengthen organizational readiness and claims outcomes
- Leverage the current market to secure broader, more favorable coverage
- Carrier “nitpicking” perceptions usually stem from misaligned expectations or misunderstood policy language
- Minimal data collection and strong third-party governance reduce insurable exposure
- Insurance can indirectly drive risk reduction when organizations follow insurer recommendations

Amanda’s session reframed cyber insurance from a transactional purchase into a strategic tool for financial protection, crisis coordination, and organizational maturity—providing critical context for the CISO and professor panel that followed.

Building an AI Secure Software Development Lifecycle (AI-SSDLC)

[Discussion Pod #6]

Karun Rajasekharan, Global Product Security Architecture Leader at Honeywell understands how as artificial intelligence becomes deeply integrated into modern products and platforms, the traditional **Secure Software Development Lifecycle** (SSDLC) must evolve to address new risks introduced by AI models, data pipelines, and automation frameworks.

Karun delivered a fast, practitioner-focused overview of how he integrates security into every phase of its AI-enabled product development lifecycle. Speaking from the product engineering perspective—not as a CISO—he explained the practical realities of securing AI features inside building automation systems, sensors,

fire panels, and industrial IoT products. Effectively, large firms especiallyl must embed AI security systematically, not as an add-on.

Executive Summary

Karun outlined how he builds an **AI-Secure SDLC** grounded in OWASP [Software Assurance Maturity Model (SAMM)], ISA/IEC 62443, and NIST 800-218. He highlighted emerging risks such as data poisoning, prompt injection, unsafe outputs, and model manipulation—and the controls applied across planning, coding, testing, deployment, and maintenance. His core message: AI security must be built into the SDLC from the start, supported by strong data governance, continuous testing, and rapid incident response.

Key Points

1. Product Security Is Collective and Customer-Centric
    - Product teams must ensure their systems don't become attack vectors for customers—especially in HVAC, building controls, and safety-critical devices.

2. AI Introduces New Threats Across the SDLC
    - Data poisoning, supply-chain contamination, prompt injection, system prompt leakage, unsafe AI outputs, and excessive agent autonomy all require structured mitigation.

3. Secure-by-Design Processes
    - Karun applies a repeatable lifecycle:
        - Plan & Design: threat modeling, supply-chain validation, AI-specific requirements
        - Implementation: static code analysis, SCA, secure coding for AI pipelines
        - Testing:red teaming, prompt validation, automated and manual testing
        - Deployment: signed firmware, sandboxing, bounded AI behavior
        - Maintenance: rapid response ("P-cert mode"), continuous model hardening

4. Data Governance Is Critical
    - Track data origins, sanitize training inputs, version datasets, and rigorously vet external LLMs and APIs. Third-party risk increases significantly with AI.

5. AI Red Teaming and Safety Validation
    - Teams test model behavior, RAG pipelines, prompt resistance, and agent boundaries—an evolving capability given the novelty of AI-specific threats.

6. Customer-Facing AI Must Be Safe
    - AI-powered support tools must never issue unsafe instructions (e.g., fire panel resets). Human oversight and output verification remain essential.\

Strategic Takeaways

- Embed AI security into every SDLC phase

- Treat data governance and provenance as foundational
- Continuously red-team AI components
- Limit model autonomy and enforce guardrails
- Prioritize customer safety in all AI-enabled features.

Karun's session delivered a practical blueprint for securing AI in real-world products—providing essential context for the live demonstrations and panel discussions that followed.

The CVE Ecosystem Today & the AI Agents Burning Watts to Fix It

[Discussion Pod #7]

Tim Rohrbaugh, back at NEACS by popular demand, has taken a very deep look at the CVE pipeline (Common Vulnerabilities and Exposures), its 429 CVE Numbering Authorities (CNAs), timelines of reporting, and the ecosystem of scores, updates, and rankings.

News Flash: Everything we know about CVEs is wrong.

The CVE pipeline is bursting at the seams—and the downstream ecosystem that enterprises rely on to make sense of it (CVSS scores, vendor advisories, scanners, ticketing) is lagging, inconsistent, and noisy. Meanwhile, security teams are asked to do more with less while the volume of new "Published" and Updated CVEs are relentless.

Tim Rohrbaugh returned to NEACS with a deep, data-driven teardown of the **CVE ecosystem**—and a demonstration of how small teams can use locally hosted GenAI to fix what's broken. His core thesis: *"Everything we think we know about CVEs is wrong."*

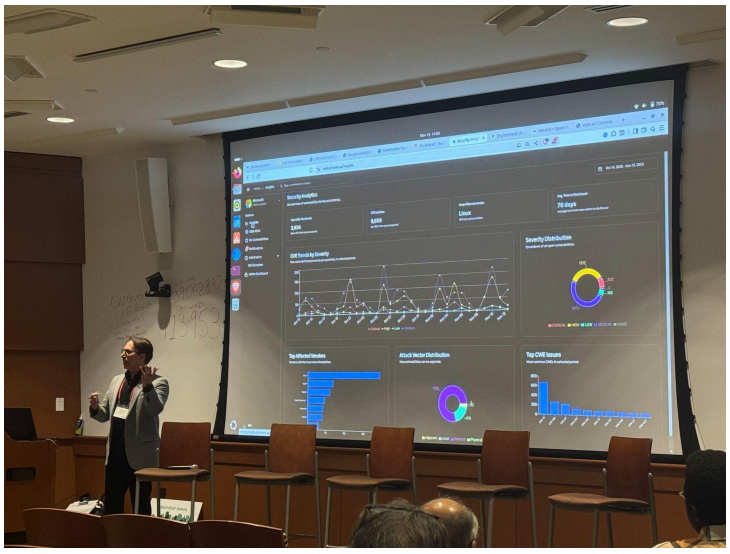
- The pipeline of Common Vulnerabilities and Exposures is overloaded, inconsistently maintained, and poorly scored, while defenders still depend on it to make patching and risk decisions.

Tim walked through how CVEs are created and updated across **~450 CVE Numbering Authorities (CNAs)** in 40+ countries, and showed that quality and completeness vary widely. In the last 12 months alone, **47,281 CVEs were published and 43,500 were updated**—yet a large backlog (~12,000) remains unscored.

- Many CVEs are updated repeatedly (some nine or more times), changing vectors, products, and risk profiles without most organizations noticing.
- Scanners struggle to keep up, teams tend to ignore unscored items, and critical changes (like a shift from local to network attack vector or the appearance of public PoC exploit code) often pass unnoticed.

Against this backdrop, Tim argued that **CVSS scoring is necessary but not sufficient**. Scores are often assigned once and rarely revisited, even when exploitation status changes. Temporal scoring exists on paper but is rarely used in practice. The result: organizations may treat actively exploited vulnerabilities as “medium” risk simply because the score never changed. His message to cyber leaders: stop blindly trusting NVD/NIST scorecards, and start questioning the underlying data, update history, and exploit context.

The second half of the talk showed a path forward: **AI-augmented vulnerability operations** built on *local* models for privacy and control. Drawing on Jevons’ Paradox, Tim noted that as AI becomes cheaper and easier to use, demand for analysis goes up—not down. Rather than replacing jobs, AI becomes a “synthetic employee” that handles the repetitive grunt work. Tim runs open-weight models (downloaded from Hugging Face) on an in-house GPU cluster and measures their workload in watts instead of labor hours.



He described a **real-time CVE pipeline** his small team built using Prefect for orchestration:

- Ingest all CVE publications **and every subsequent update**, preserving full revision history
- Automatically detect “high-signal” changes (PoC published, score changed, affected products updated)
- Use multiple GenAI models as a *team*—one to analyze exploitation paths, another to peer-review and fact-check, a third to synthesize a final, higher-confidence report
- Enrich public CVE data with private asset inventory to decide: *Is this relevant to us?*
- Generate concrete outputs for defenders: bash/PowerShell checks, EDR/SIEM queries, and retro-hunt playbooks tied to the PoC publication date.

Tim stressed a key operational assumption: **“Always assume IT can’t patch.”** In complex environments—airlines, legacy platforms, vendor-controlled systems—patches may be slow, expensive, or impossible in the short term. That shifts the burden to security teams to detect exploitation early and implement high-fidelity “tripwire” alerts. Inspired by the historic TripWire detection of the Solar Sunrise breach, Tim advocated for precise detections that only fire when a true exploit pattern appears, reducing noise while buying time for safe remediation.

Throughout, he positioned AI as a **force multiplier for analysts**, not a replacement. Each human (“carbon-based teammate”) should manage a small crew of named AI agents—Sally the scorer, Peter the analyst, Dale the documenter—who continuously rescore CVEs, track changes, and prepare verification artifacts. Interns and junior staff, he argued, should learn to manage these synthetic teams from day one: “My job isn’t being replaced by AI—my job is being promoted.”

Strategic Takeaways for Executives

- The CVE ecosystem is **noisy, incomplete, and in constant motion**; rely on scorecards alone at your peril
- Track **CVE updates and PoC releases in real time**, not just initial publications
- Assume patching will be delayed; invest in **tripwire-style detections, retro-hunts, and continuous monitoring**
- Use **locally hosted open-weight models** to preserve privacy while scaling analysis
- Build small, repeatable workflows where AI generates scripts, queries, and playbooks—and humans approve and act.

Tim’s session reframed vulnerability management as an AI-augmented, data-engineering problem—showing how even a small team can outpace the CVE firehose with the right synthetic reasoning agents “burning watts” on their behalf.

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

[Discussion Pod #8]

This panel discussion features a real-world exchange between cyber educators and industry leaders. Professors will share how they’re designing programs with hands-on labs, industry-funded projects, and even high school hackathons. CISOs and CTOs will weigh in on

the “last-mile” problem: grads with zero experience, mismatched expectations, and a professionalism gap that’s hard to ignore.

The big questions

- Are four-year degrees still the gold standard—or are certs and bootcamps the smarter play for mid-career upskilling?
- How do you hire interns *and* set expectations when “everyone is busy”?
- What can companies do (without breaking budgets) to actually shape the talent pipeline?
- And how can we close the generation gap without lowering the bar?

Come for the honest dialogue, stay for the practical takeaways—and leave with a few ideas for fixing a system that isn’t working for educators, employers, or students.

Panelists

- Dr. Frederick Scholl, Professor & Program Director Cybersecurity - Quinnipiac University
- Dr. Chad Wiliams, Chair, Computer Science Dept - Central CT State University
- Dr. Tirthankar Ghosh, Chair Professor - University of New Haven
- Mario Di Natale, CISO - Odyssey Re
- Michael Tetto, CISSP, CCSP, Director, Information Security - Eversource Energy
- Karun Rajasekharan, Global Product Security Architecture Leader - Honeywell

This panel tackled the disconnect between what cyber programs teach and what employers actually need from entry-level hires. With hundreds of thousands of open cyber roles in the U.S., panelists agreed the problem is not the volume of graduates—it’s whether they can do useful work on day one. The conversation focused on how degrees, certifications, and hands-on “grit” fit together in building real-world capability.

Professors described how they are modernizing curricula with the NICE Framework, NSA CAE designations, labs, CTFs, and industry-funded projects—but acknowledged that many programs still over-index on SOC roles and theory. Industry leaders stressed that **skills-based learning plus foundational knowledge** is the winning mix. Certifications (Security+, CSSLP, etc.) signal commitment, but employers put more weight on students who have built and administered real systems: Active Directory, Linux, networks, cloud labs, Raspberry Pi projects, and code.

Panelists repeatedly came back to **specialization and mindset**. “I want to do cyber” is now too broad; graduates should be able to articulate interest and aptitude in areas like product security, identity, GRC, AI, or incident response—and show work that backs it up. Mario Di Natale underscored integrity, ethics, and trust as non-negotiable; others highlighted curiosity, persistence, and an entrepreneurial mindset as differentiators in a fast-changing field.

A major theme was **industry–academia collaboration**. Michael Tetto shared Eversource’s model: their CISO has taught Intro to Cybersecurity at CCSU for seven+ years, turning the classroom into a direct talent pipeline where the strongest students become interns and, later, full-time staff. Karun Rajasekharan highlighted product security as a severely under-taught but high-demand area; He grew its product security team by upskilling internal engineers who showed interest and coding ability, then designating “security champions.”

Key takeaways

- Degrees and certs matter, but **hands-on experience and the ability to learn** matter more
- Employers can teach cybersecurity if students bring strong system fundamentals and grit
- Students should pursue **concentrations and visible projects**, not just course credits
- Universities need more guest teaching, internships, and joint projects with local employers

The panel closed with a shared challenge: educators and employers must co-design the early-career journey so that “cyber grad” translates into someone who can think critically, work ethically, and start adding value—while still learning—on day one.

The Next Mission: Turning Insight Into Impact [Discussion Pod #9]

In Closing - We've heard from the spies and the scientists. The agents and the analysts. The CEOs, strategists, and storytellers. Now, as we close the Summit, we return to the reason we came together in the first place: to make a difference.

In the final session, moderator **Michael Hiskey**, CSO and founder of the CxO Security Forum, closed the Summit reflecting on the day's most urgent lessons—from ransomware negotiation and AI-driven threats to CVE realities, fraud tradecraft, and law-enforcement collaboration models that showed real results. He thanked the speakers, universities, and solution providers, and urged attendees to continue networking before departure.

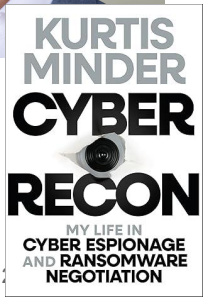
Rather than simply recap talks, the session served as a call to action: participants were reminded that whether they protected a global enterprise or a local college network, their mission was the same—to build trust, verify identity, out-think adversaries, and avoid going it alone. Hiskey noted that future gatherings were already being planned and encouraged attendees to share compelling speakers for next year. The event ended with appreciation for the community's engagement and a challenge to leave with purpose—and a plan.

Discussion Leaders

Kurtis Minder

CEO & Co-Founder, GroupSense
Author, *Cyber Recon: My Life in Cyber Espionage and Ransomware Negotiation*

Kurtis Minder is one of the world's foremost experts in ransomware response and cyber threat intelligence. As CEO and co-founder of GroupSense, he has led negotiations in some of the largest ransomware and data extortion cases globally, engaging directly with threat actors and nation-state affiliates.



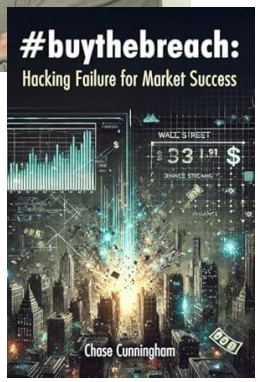
With over 25 years in cybersecurity—including roles at Fortinet, AT&T, and Citrix-acquired Caymus Systems—Kurtis has combined operational security, cyber reconnaissance, and real-world intelligence tradecraft into a uniquely effective digital risk strategy. His pioneering work and insights have been featured in *The New Yorker*, *BBC*, *The Wall Street Journal*, and *Fortune*.

Kurtis will deliver a TED-style keynote and participate in a moderated discussion on themes from his acclaimed new book, *Cyber Recon*, offering a rare behind-the-scenes look at the people, tools, and tactics behind today's cyber espionage and ransomware ecosystem.

Dr. Chase Cunningham, PhD

"Dr. Zero Trust" - Author, Speaker and Industry Thought-Leader

Dr. Chase Cunningham is a globally recognized cybersecurity strategist, bestselling author, and trusted advisor to both the public and private sectors. Widely known as **"Dr. Zero Trust,"** Chase pioneered the Zero Trust security framework during his time as a Senior Analyst at Forrester Research—an approach now adopted as a standard across government and Fortune 500 enterprises alike.



Over a 20+ year career that spans the U.S. Navy, Department of Defense, and senior industry roles, Chase has led initiatives in cryptographic systems, threat intelligence, cyber forensics, and national cyber defense strategy. He holds a PhD in Computer Science and Cybersecurity, with research centered on insider threats and advanced detection algorithms. He also maintains CISSP and CEH certifications.

An engaging keynote speaker and regular contributor to leading cybersecurity forums, Chase is the author of several acclaimed books including *Cyber Warfare: Truth, Tactics, and Strategies* and his latest, *Buy the Breach: Hacking Failure for Market Success*. In *Buy the Breach*, he unveils a contrarian but data-backed strategy for turning corporate cyber failures into personal financial gains—arming cyber professionals with the tools to outperform hedge funds by investing in the inevitable post-breach market rebound.

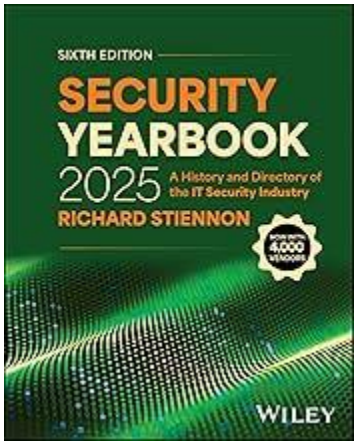
Chase is a rare voice who blends deep technical expertise with sharp financial insight. Whether briefing the Executive Branch or advising the boardroom, his mission is clear: empower defenders, demystify complexity, and challenge the status quo.

Richard Stiennon

Chief Research Analyst, IT-Harvest

Richard Stiennon is one of the most respected and provocative voices in the cybersecurity industry. As Chief Research Analyst at

IT-Harvest—the firm he founded in 2005—he leads the only comprehensive effort to map, track, and analyze the entire global cybersecurity vendor landscape. His research underpins the *Security Yearbook* series, offering deep data and sharp insight into the trends shaping the industry.



A former VP of Research at Gartner, Richard has held senior roles at Fortinet, Webroot, and Blancco Technology Group, and has advised government agencies and Fortune 500 companies alike. His past publications include *There Will Be Cyberwar*, a Washington Post bestseller, and *Surviving Cyberwar*. His thought leadership spans over three decades and 32 countries, blending strategic analysis with operational depth.

Richard holds a B.S. in Aerospace Engineering from the University of Michigan and an M.A. in War in the Modern World from King's College London. He is also an active commentator on LinkedIn, Substack, and X (formerly Twitter), where he regularly challenges assumptions and surfaces the next wave of cybersecurity innovation.

Tim Rohrbaugh

Founder - RadicalNotion.AI, 3x Public Co. CISO

Tim Rohrbaugh brings 20+ years of C-level cybersecurity leadership to the frontier of AI for security and applied engineering. As founder of RadicalNotion.AI and former CISO of JetBlue Airways, he has built and operated enterprise programs that protect high-value, regulated data— including responsibility for safeguarding more than 40 million consumer records at a public financial services company.

A career security architect and systems engineer, Tim advances a practical view of GenAI as "augmented intelligence": trustworthy, domain-tuned reasoning agents that reduce noise, challenge bias, and accelerate evidence-backed decisions without exposing IP. He has served as Vice Chair of the Airlines for America Cyber Security Council and as a board member of the Online Trust Alliance, where he contributed to national privacy and security policy. His work has been recognized with multiple awards, including Top Global CISO by Cyber Defense Magazine. Tim holds two

joint patents in identity verification and authentication and is a frequent speaker and advisor to boards and engineering teams alike.

Amanda Draeger

Principal Cyber Risk Engineer, Liberty Mutual Insurance

Amanda Draeger is an accomplished cybersecurity leader, with a distinguished career rooted in leadership, education, and technological excellence. As a Sergeant Major in the U.S. Army, Amanda exemplified these traits by not only educating and leading fellow soldiers, but by becoming one of the first four women to ever achieve the GIAC Security Expert (GSE) designation from SANS.

Now retired from the armed forces, she utilizes her expertise, knowledge, and passion for educating others in her role at Liberty Mutual as a Principal Cyber Risk Engineer. In this role she provides subject matter expertise to underwriters and insureds on critical cybersecurity topics, as well as presenting at major infosec conferences around the country. Outside of work, Amanda is a fiber arts enthusiast.

Prof. Frederick Scholl, Ph.D.

Program Director Cybersecurity, Associate Teaching Professor - Quinnipiac University

Frederick Scholl is a highly accomplished Global Senior Information Security Risk Manager. Dr. Scholl earned a BS and Ph.D. in Electrical Engineering from Cornell University. He is currently at Quinnipiac University, where he is MS Cybersecurity Program Director and Associate Teaching Professor. Previously, Fred founded Monarch Information Networks, LLC to enable trusted clients to protect their information. He also served as Senior Manager of Information Security and Control for Nissan Americas. His business experience also includes co-founding Codenoll Technology Corporation (NASDAQ: CODN) where he was Senior Vice President and Board Member. Career accomplishments also include 13 US Patents related to network technology and fiber optics. He chaired the IEEE committee that wrote the first standard for Ethernet communication over fiber optic links, now used world-wide.

Prof. Chad Williams, Ph.D.

Chair, Computer Science Department - Central Connecticut State University

Dr. Chad Williams is Chair of the Computer Science Department at Central Connecticut State University. Central has earned the distinction of being a National Center of Academic Excellence in both Cyber Operations (CAE-CO) and Cyber Defense (CAE-CD), one of only 18 institutions nationwide with both designations. Before transitioning to academia, Dr. Williams worked as a technical lead at Accenture, delivering secure software solutions for Fortune 500 clients in insurance, capital markets, banking, and credit reporting. Recognizing the importance of both theoretical knowledge and practical experience, Central's cybersecurity program was designed to ensure that graduates gain hands-on work experience prior to graduation, enabling them to contribute immediately to industry needs.

Tirthankar Ghosh, PhD.

Chair Professor, Department of Electrical and Computer Engineering & Computer Science
Director of Connecticut Institute of Technology, University of New Haven

Dr. Tirthankar Ghosh has 20+ years of experience in cybersecurity education and research and received and managed several grant-funded projects from National Science Foundation, National Security Agency / Department of Defense, Office of Naval Research, state governments including Florida department of Transportation, Florida Department of Education through CyberFL, and Minnesota IT, and private sectors.

Dr. Ghosh has experience working in the Minnesota and Florida higher education systems where he led several initiatives on research and education at the state and national levels before joining University of New Haven in the fall of 2023. Dr. Ghosh has published several papers on threat and anomaly detection, and scenario-based learning and competency assessment. Dr. Ghosh has a bachelor's degree in Electrical Engineering and a master's and Ph.D. in Computer Engineering.

Mario DiNatale

Chief Information Security Officer, OdysseyRe

Mario DiNatale is a recognized cybersecurity leader known for blending deep technical expertise with executive vision. As Chief Information Security Officer at Odyssey Re, he drives enterprise-wide resilience through pragmatic, risk-based strategy and a culture of accountability.

Previously CTO at Kyber Security and CIO for the Town of Hamden, Mario has earned a reputation for transformative leadership and trusted advisory work with governments, Fortune 50 CEOs, and federal law enforcement and intelligence agencies.

Born to blue-collar immigrant parents in New Haven, CT, Mario's passion for technology began early—legend says with a screwdriver in hand. He still keeps the shovel his father gave him "in case the computer thing didn't work out."

Outside of work, Mario enjoys building LEGO sets with his daughters, practicing Brazilian Jiu-Jitsu, and studying astronomy.

Karun Rajasekharan

Global Product Security Architecture Leader, Honeywell

Karun Rajasekharan is a seasoned product and security technologist with over two decades of experience in the field of security products. He currently serves as the Global Product Security Architecture Leader at Honeywell, where he spearheads a team of security architects dedicated to creating secure-by-design products.

In his role, Karun also focuses on the development of AI cybersecurity secure development practices. His previous experience includes leading Product Security at Dover Corporation, where he ensured the secure design and development of digital and IoT products. Additionally, Karun has managed product and engineering teams at Virima and Internet Security Systems, now IBM Security.

David Palmbach

Cybersecurity State Coordinator (CSC), Connecticut, Cybersecurity and Infrastructure Security Agency (CISA), Integrated Operations Division (IOD) Region 1

David Palmbach currently works for the U.S. Department of Homeland Security (DHS) within the Cybersecurity and Infrastructure Security Agency (CISA) a Cybersecurity Advisor in Connecticut. In his current role, David supports all 16 critical infrastructure sectors providing a variety of services ranging from assessments to workshops and exercises. Previously, David worked for the State of Connecticut in their fusion center, the Connecticut Intelligence Center (CTIC), as an Intelligence Analyst focusing on cyber.

During his time with the fusion center, he supported law enforcement investigations, provided technical analysis, and produced intelligence products on emerging threats. David graduated from the University of New Haven with a B.S. in National Security Studies and a M.S. in Cyber Security and Networking. During his time at UNH, David published research in the field of digital forensics.

Supporting Solution Providers

Blumira

Blumira (blumira.com) provides a cloud-based security operations platform that simplifies threat detection and response for small and mid-sized organizations. Its integrated SIEM and XDR solution deploys rapidly, offering automated detection, prioritized alerts, and guided response actions across cloud and on-premises environments.

By combining endpoint visibility, built-in integrations, and 24/7 SecOps support, Blumira enables IT and security teams to identify and contain threats quickly while reducing complexity and operational overhead. The platform's accessible design and automated workflows help organizations meet compliance and cyber insurance requirements, strengthen resilience, and enhance overall security posture.

CISOs within the CxO Security Forum Community have endorsed Blumira, citing a responsive account team and thoughtful, efficient pricing options.

ThreatLocker

ThreatLocker (threatlocker.com) provides a unified Zero Trust endpoint protection platform that enables organizations to control and secure their IT environments with precision. Combining application allowlisting, storage control, network access management, and privilege elevation, ThreatLocker delivers granular visibility and enforcement across servers, desktops, and cloud workloads.

Designed for enterprises, MSPs, and mid-sized organizations, ThreatLocker's "default deny" approach helps stop ransomware, data exfiltration, and insider misuse before they can execute—without disrupting operations. By centralizing policy management and automating threat prevention, ThreatLocker empowers IT and security teams to maintain strict control, meet compliance mandates, and reduce attack surfaces in real time.

Abnormal

Abnormal Security (abnormal.ai) is an AI-native cybersecurity company specializing in protecting enterprises from advanced email and collaboration-based attacks. Its Behavioral AI platform analyzes identity, context, and communication patterns to establish a baseline of

"normal" user behavior—enabling precise detection of anomalies that indicate social engineering, phishing, and account compromise.

By leveraging large-scale behavioral data and machine learning, Abnormal Security stops sophisticated inbound attacks and detects compromised accounts across Microsoft 365, Google Workspace, and other connected applications. The platform's autonomous, adaptive defense helps organizations reduce risk from human-targeted threats while minimizing false positives and operational burden.

Palo Alto Networks

Palo Alto Networks (paloaltonetworks.com, NASDAQ: PANW) is a global cybersecurity leader advancing intelligent, automated defense across cloud, network, and endpoint environments. Through its **Cortex** platform and **Unit 42** intelligence team, the company delivers a powerful fusion of technology and expertise designed to prevent, detect, and respond to modern cyber threats.

The **Cortex** portfolio integrates extended detection and response (XDR), automation and orchestration (XSOAR), AI-driven analytics (XSIAM), and attack surface management (Xpanse) to streamline and accelerate SecOps. Complementing this, **Unit 42** provides world-class incident response, threat intelligence, and managed detection services—helping organizations strengthen resilience and translate insights into action. Together, they form the backbone of Palo Alto Networks' proactive security operations ecosystem.

GuidePoint Security

GuidePoint Security (guidepointsecurity.com) is a leading cybersecurity consultancy providing expert advisory services, advanced solutions, and hands-on technical support to help organizations assess, mitigate, and manage cyber risk. The company is distinguished by its practitioner-led model—many of its consultants are former CISOs—offering pragmatic, experience-based guidance rooted in real-world operational insight rather than product sales.

GuidePoint's Digital Forensics and Incident Response (DFIR) and Threat Intelligence practices are widely recognized for their expertise in rapid breach response and complex threat investigations. The firm also supports enterprise clients in designing and operationalizing secure

cloud and Zero Trust architectures through a vendor-agnostic approach, ensuring objective recommendations and sustainable security outcomes.

Bridgesoft

Bridgesoft (bridgesoft.com) is a provider of technology, consulting, and information security management solutions focused on IT-powered risk management and identity governance. The company partners with enterprises to develop and implement secure, efficient, and scalable solutions that align with business objectives while maintaining acceptable risk levels.

With extensive experience supporting global organizations across industries, Bridgesoft combines technology leadership with a strong customer-centric philosophy to deliver measurable results. Its core expertise in identity governance and risk-driven IT strategy enables clients to enhance operational efficiency, strengthen compliance, and maximize return on investment with products like Bridgesoft Identity Gateway.

Robert Half

NEACS 2025 Recruitment Firm Partner

Robert Half (roberthalf.com, NYSE: RHI) was founded in 1948 and is considered the largest specialized talent solutions and business consulting firm. They connect professionals and employers for both permanent and contract positions, spanning disciplines.

Through its consulting subsidiary **Protiviti,** Robert Half also delivers internal audit, risk, business, and technology consulting solutions. In the last 12 months, Robert Half has been recognized as one of America's Most Innovative Companies by Fortune and, with Protiviti, has been named one of the Fortune® Most Admired Companies™ and *100 Best Companies to Work For.*

Within its technology practice, Robert Half's Full-Time Engagement Professional (FTEP) Program provides clients with access to experienced IT and cybersecurity professionals who are full-time Robert Half employees, available for long-term or project-based engagements.

Demo-Force

Demo-Force (demo-force.com) delivers a next-generation cybersecurity simulation and validation platform designed to help enterprises **operationalize Zero Trust strategies** and continuously test the effectiveness of their defenses.

By emulating real-world attack paths, insider threats, and adversary behaviors, Demo-Force enables organizations to identify security gaps before attackers exploit them. Its cloud-native platform integrates with existing EDR, SIEM, and identity tools to validate controls, prioritize remediation, and provide clear, data-driven insights to leadership.

With automated testing cycles, customizable scenarios, and continuous performance scoring, Demo-Force empowers security teams to move from **assumption to assurance** — strengthening resilience, improving ROI on existing security investments, and aligning cyber operations with strategic business goals.

CISOs and security leaders within the CxO Security Forum Community have praised Demo-Force for its **practical Zero Trust validation approach**, responsive support, and measurable impact on risk reduction.

Conatix

Conatix (conatix.com) is pioneering *cyberomics*, like genomics in biology – streaming massive granular data in real time to map and monitor the whole and the parts simultaneously: not tissues, cells and DNA but the network, the endpoint and the code that powers them, all at once, to spot pathologies, anomalies and security issues.

Conatix applies deep learning AI, patented anti-encryption, 3D network visualization and other advanced technologies to help CISOs and MSPs analyze an organization's entire IT estate, in order to detect and prevent malware, ransomware, insider and supplier fraud on business computers and enterprise and virtual networks.

Advanced technologies countering the toughest cases, including adversarial AI threats: Preventing problems before they start and detecting what others miss.

Tab 2