The 2024 NorthEast Annual Cybersecurity Summit (NEACS) Detailed Summary & Notes

NORTHEAST ANNUAL

CYBERSECURITY SUMMIT

What follows is a detailed summary and notes from each discussion for the 2024 NorthEast Annual Cybersecurity Summit. It took place on Thursday 21 November 2024 at Quinnipiac University's North Haven Campus.

Start 09:36

Introduction: Michael Hiskey

- Emphasized rebuilding trusted relationships within the cybersecurity community.
- Leverage the **CxO Security Forum** for engaging discussions and interactive networking.

Partner Associations:

1. **(ISC)² Connecticut Chapter**
    - Volunteer-driven community fostering cybersecurity growth.
    - Exclusive custodian of the CISSP certification in Connecticut.
    - Activities: Monthly meetings, social events, conferences, and low-cost training (e.g., Capture the Flag).
    - Open to security professionals and like-minded individuals.
    - Actively seeking **speakers** and **presenters** for events.
    - **Contact:** ISC2CT.org.
2. **ISACA**
    - Mission: Promote trust through certifications like COBIT 5, COBIT 2019, and CMMI.
    - Member base: ~700 volunteers.
    - Events: Hosted 13 events with 107 CPE opportunities.
    - Upcoming Training (2024): Cloud fundamentals, blockchain, and more.
3. **CSA NY Metro Chapter**
    - Focused on cloud security; events and research groups actively seeking contributors.
    - January event in New York; Connecticut chapter holds robust yearly conferences.
4. **OWASP (NYC & CT)**
    - Advocates for secure application development.
    - 45,000 members globally.
    - Mission: Protect sensitive information while ensuring application functionality.

Agencies

1. **FBI New Haven Field Office**
    - Represented by Supervisory Special Agent Alexandra.
2. **IRS-CI (Carlo Nastasi)**
    - Specializes in financial investigations, including tax fraud, money laundering, and cybercrimes.
3. **Connecticut Information Center (CTC)**
    - Fusion center gathering intelligence; representatives include Tim Silva and Jon Hale.

The Whole Cybersecurity Industry: 4,155, 19, 660, 9,711, 14.052 Billion, and 973!

- **Key Statistics:**
  - 4,159 vendors worldwide, offering 9,722 solutions across 18 categories.
  - Emerging Category: **AI Security** (50 vendors).
  - U.S.: 1,909 vendors lead globally, followed by Israel.
  - Germany: Strong vendor-customer loyalty; oldest cybersecurity vendors.
- **Trends:**
  - $12 billion invested across 266 companies in 2024.
  - Average vendor age: 12 years.
- **Notable Insights:**
  - ~90% of Israeli vendors have IDF ties.
  - Consolidation of vendors is unnecessary due to the market's vast needs.

AI and Cybersecurity: Pamela Gupta

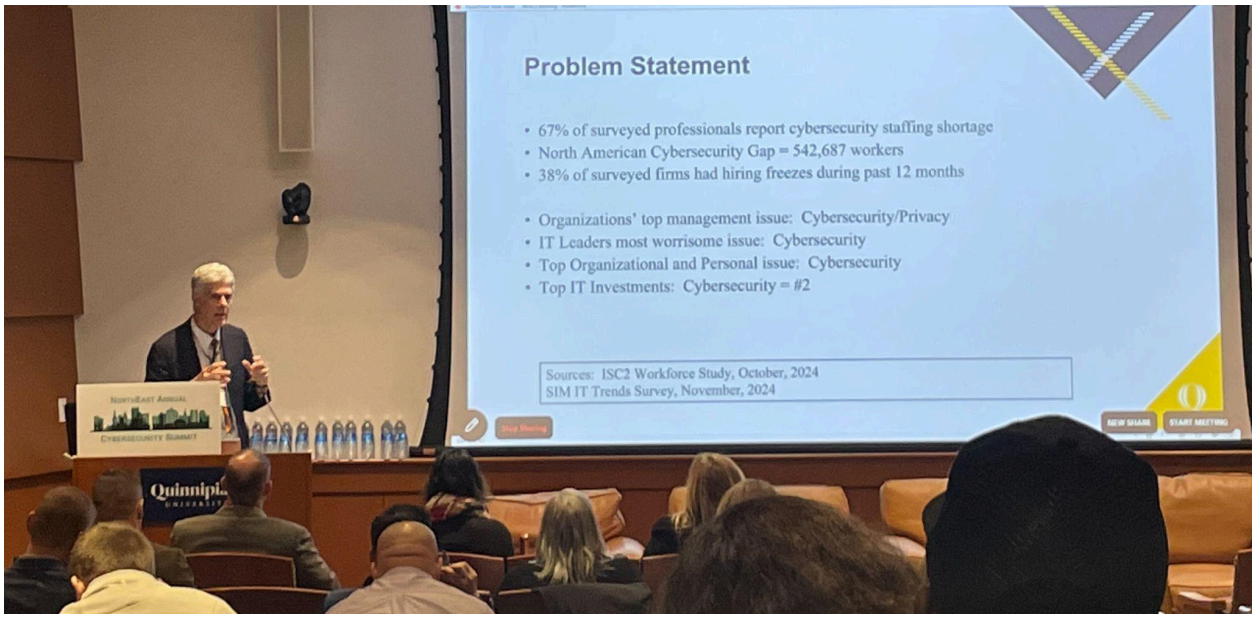
- **CEO of Trusted AI**, leading in AI Governance and Risk Management.
- AI Misconceptions: AI isn't one umbrella; it includes **predictive** and **generative** AI.
- Frameworks:

    - **NIST AI RMF**: Promotes responsible AI system development, emphasizing safety, resilience, and accountability.
    - AI Context Lifecycle: Data → AI Model → Task/Output → Application → People/Planet.
- **Key Statistics:**
    - By 2026, organizations using AI will achieve a 50% efficiency increase in adoption and business goals.

Industry and Academia

Quinnipiac University (Fred Scholl)

- Addresses cybersecurity workforce shortages.
- Students gain hands-on experience with tools and frameworks (IAM, resilient systems, blockchain).
- Promotes industry-academia collaboration to reduce the skills gap.



Academia & Corporate Panel Discussion Highlights:

- **Dennis Klemenz (CTO):** Graduates' unique strengths need industry recognition; COVID-19 impacted their direction.
- **Brian Kelly (InfoSec Director):** Students should apply directly on company websites instead of mass-applying.
- **Suzette Leal (CISO):** Sees a lack of communication and professionalism in the new generation.

- **Dr. Mekni (UNH):** Advocates for combining certifications with academic degrees.

Applied GenAI in Cybersecurity: Tim Rohrbaugh

- Key Insights:
  - GenAI is **Augmented Intelligence**, not true Artificial Intelligence.
  - **Strengths:** Advanced knowledge retrieval and reasoning capabilities.
  - **Challenges:** Data leakage via proprietary models; advocates for **internal/localized model use**.
  - Positive Hallucinations: Indicators of an effective model.

Cybersecurity Budgeting: Ira Winkler

- Key Idea: CISOs often receive budgets they "deserve," not what they "need."
- Advocates for data-driven decisions over intuition.
- Introduced **Risk Formula**:
    - Risk = Value × (Threat × Vulnerability) ÷ Countermeasure.
- Strategies:
    - Focus on reducing vulnerabilities near threats.
    - Leverage automation for incident detection and response.

Legal Perspectives on Breaches, Ransomware, & Incident Response: Trends & Predictions: **Gregory J. Bautista (Mullen Coughlin LLC)**

Greg is a DOUBLE Quinnipiac Alumni - undergraduate & law school!

- Expertise: Ransomware, data mapping/identification, acquisitions, business email compromise, and SEC disclosure rule compliance.
- Works closely with brokers, insurance companies, and directly with businesses.
- **Key Points:**
    - Cyber insurance now has requirements, aiding CISOs in securing budgets and resources.
    - Strong collaborations with the FBI and law enforcement.
    - Advised companies to assess recovery plans, downtime procedures, and notification timelines.
    - Increasing trend of companies switching to data mining.

CISOs & Cyber Agents: Government Agency & Private Sector Collaboration

Panelists:

- **Carlo Nastasi (Special Agent):** Expertise in money laundering investigations and inter-agency collaboration.
- **Jon Hale (Cyber Intelligence Analyst):** Works with the CT Information Center.
- **William Malik (Founder, Malik Consulting):** Former VP of Research at Gartner.
- **Justin Hickey (Deputy CISO, State of Connecticut):** Experience with phishing attacks and ISP takedowns.
- **Conor Phoenix (Former SSA, FBI):** Extensive background in incident response and collaboration with local agencies.

Key Points:

- FBI has 56 domestic offices and collaborates with local law enforcement and other agencies.
- Inter-agency relationships are critical; best built before incidents occur.
- Example Success: Collaboration with federal agencies to address phishing attacks via ISP letters.

https://docs.google.com/document/d/1gVHe8vPRgjNz02nit8YxrDlAalcRhuVWq86VWXVE96E/edit?tab=t.0#heading=h.s1krstuxmad7

Detail

Partner Associations:

(ISC)2 Connecticut Chapter - volunteers who collaborate to help grow the computer security community. Only CT chapter and are a Corporate entity & custodian of the CISSP certificate. Have monthly meetings, social events, & conferences throughout the year. Every chapter meeting has a speaker who specializes in a key area. Can get CPE credits. Want to do low cost training like Capture the Flag (CTF). Open to computer security professionals and like-minded individuals. Need speakers & presenters for monthly meetings and upcoming conferences. Can get into contact at SC2CT.org.

ISACA - Mission is to promote trust. Has globally recognized certifications and frameworks like COBIT 5, COBIT 2019, & CMMI. Chapter has around 700 members and are volunteers. Had 13 events and had up to 107 CPE opportunities. Also has in-person/online events. Training offered in 2024 cloud fundamentals, blockchain, etc.

CSA NY Metro Chapter - All volunteers can get CPE, and certifications. Research groups are always looking for contributors. Will hold an event in January in NY and the CT chapter has been robust, holding several conferences over the year. Great place to learn more about cloud security.

OWASP (NYC & CT) - Recently changed their name. Mindset is to get applications to work but also to be secure. It Has 45,000 members across the world. Goal is to make sure to protect our information.

Agencies:

FBI NEW HAVEN FIELD OFFICE - Alexandra is a supervisory special agent.

IRS-CI - Carlo Nastasi works a lot with the banking industry and is a part of the SAR Review Team. 16 years of experience in financial investigation. The IRS-CI investigates international tax fraud, abusive tax schemes, money laundering, cybercrimes, etc.

Connecticut Information Center (CTC) - A fusion center that collects information and provides intelligence. Tim Silva is a Fusion Center Manager and Jon Hale is a Cybersecurity Analyst.

The Whole Cybersecurity Industry: 4,155, 19, 660, 9,711, 14.052 Billion, and 973!

Richard Stiennon, Chief Research Analyst - IT-Harvest

> Richard Stiennon is Chief Research Analyst for IT-Harvest, the firm he founded in 2005 to cover the 4,036+ vendors that make up the IT security industry. He has presented on the topic of cybersecurity in 32 countries on six continents. He was a lecturer at Charles Sturt University in Australia. He is the author of Surviving Cyberwar (Government Institutes, 2010) and Washington Post Best Seller, There Will Be Cyberwar. His research appears on Substack. Stiennon was Chief Strategy Officer for Blancco Technology Group, the Chief Marketing Officer for Fortinet, Inc. and VP Threat Research at Webroot Software. Prior to that he was VP Research at Gartner. He has a B.S. in Aerospace Engineering from the University of Michigan, and his MA in War in the Modern World from King's College, London. His latest book Security Yearbook 2025 will be published by Wiley in May, 2025.

There are 4,159 Solution Providers in the cybersecurity industry today. Richard Stiennon is the former VP of Research for Gartner, and has spent decades analyzing the security industry. Since leaving Gartner, he has been an analyst, lecturer and industry pundit. More recently, his firm IT Harvest has set about cataloging and understanding the breadth and depth of the global vendor landscape.

He's neatly organized those vendors into 18 categories and 660 subcategories, which spans 9,860 product offerings. But there's even more to the story. In this discussion, Richard will share some of the key insights in his forthcoming book "The Cybersecurity Yearbook 2025," which follows successful updates since 2020.

Leaders will learn from this session how best to categorize and understand product offerings, helping them tune their thinking around which solutions and products will be most helpful to their cyber/information security, AML, KYC and third-party risk mitigation programs.

The Whole Cybersecurity Industry - Richard Stiennon

> There are 4159 vendors in the database. Hard to do research because vendors are hard to find in databases. Vendors do not say what they do on their website. They do tell you what they do in their product description. There are 18 categories based on a Layered Defense Model where they contain 600 sub-categories. With 4159 vendors there are 9722 solutions. The newest category is AI Security with 50 vendors. China has 1,126 cybersecurity vendors and for the most part they do not sell outside of China. The US has 1,909 vendors and sits at the top with Israel right below. In Germany the relationship between the customer and the vendor is so strong that they would rather shop with their own vendor and have them create a new product if need be instead of going to the USA or another country. The cybersecurity

vendor has the average age of 12 years and has made a chart for this. Germany has the record for the oldest cybersecurity vendor. So far in 2024, the total invested in 266 companies is $12 billion. Richard is watching AI Security but it is hard to keep track. IT-Harvest is the only platform for researching the entire cybersecurity industry.

Questions -

Q: Are there too many vendors? A: No, there is no need for consolidation.

Q: How many of the Israel vendors are from the IDF? A: About 90% of the vendors.

Safeguarding the Future: The Critical Role of Cybersecurity in AI Safety and Resilience

Pamela Gupta, CEO - Trusted AI

Pamela Gupta, a globally recognized AI Cybersecurity and Safety expert, is a C-level advisor, consultant, and professional speaker. As founder of Trusted AI, she helps organizations accelerate AI adoption by implementing Trustworthy and Responsible AI practices. Ranked among the top global experts in Risk Management and Cybersecurity by Thinkers360, Pamela combines technical expertise, leadership, and ethical AI skills to guide companies in leveraging AI for innovation while reducing risks.

Her groundbreaking AI Risk Management Framework, *AI TIPS (Trust Enabled Pillars for Sustainability)*, laid the foundation for holistic AI governance, addressing Security, Privacy, Transparency, Explainability, Ethics, Regulations, and Accountability—four years ahead of NIST's global framework.

A former executive at Unilever, Marriott, and Prudential Securities, Pamela offers invaluable insights into emerging risk landscapes. She is a LinkedIn Top Voice and sought-after speaker, known for demystifying complex topics and bridging strategy with actionable implementation.

As artificial intelligence (AI) continues to serve as a potent force propelling both prosperity and progress, the accompanying surge in its capabilities and integration brings forth significant challenges and risks. This keynote presentation will delve into the crucial importance of cybersecurity, safety, and resilience in AI systems, exploring how these elements are vital in preventing harms such as bias, discrimination, privacy breaches, and more.

AI's potential to influence nearly every facet of society is immense, but so is the responsibility to ensure it is safe, secure, and equitable. Businesses and entities involved in AI's sphere must adhere to strict standards of human rights and responsible business conduct, practicing due diligence to mitigate risks effectively.

Pamela is the CEO of Trusted AI. Leading AI Governance, Risk Management Consulting & Advisory. Wanted to bring the business to the security professionals instead of bringing the professionals to the business. CISOs are the MVP in your Cyber Security Program. More than 40% of leaders do not understand the cyber risks posed by AI, Virtual Reality, etc. AI is not one big umbrella. There are 2 different aspects of AL; One is predictive and one is generative AI. AI technology is accurate, resilient, security , safety & accountability. By 2026, organizations that will use AI will see a 50% efficiency increase in their AI Model in terms of adoption, business goals, & other acceptance. NIST AI RISK Management Framework (AI RMF) - manage AI Risks and promote trustworthy/responsible development and use of AI systems. Application Context -> Data & Input -> AI Model -> Task & Output -> Application Context -> People & Planet. AI Center of Excellence at Trusted AI contains Strategy, Governance, Technology, Skills Development, Operations, & Innovation.

Questions -

Q: Are there any certifications for AI A: No, there are none.

Q: What do you see Attacking or Red Team as a part of AI safety and resilience

A: It has to be contextual. It is going to be a very much iterative process right now.

Academia Cybersecurity: What's a Cyber Grad Do For Me?

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.

Universities (like our gracious host, Quinnipiac) offer both undergrad and graduate degrees in "Cybersecurity," Many CISOs are asking "What does a recent cybersecurity graduate do for me?" Do they work in the SOC? Are they prepared for leadership roles? How do I best fill those entry-level roles I need on my team? In this session, cybersecurity professors will discuss what is included in the programs, and how to best utilize these recent grads in your fraud-fighting or cybersecurity staff.

Academia - Fred Scholl

Professor Scholl is the MS Cybersecurity Program Director at Quinnipiac University. Presents a problem on a shortage of cybersecurity staff. 67% of surveyed professionals report cybersecurity staffing shortage. Organizations' top management and IT leaders issue is cybersecurity and cybersecurity is #2 in Top IT investments.

Students are not given the language of business and experience is needed. Quinnipiac is a CAE (Center of Academic Excellence) and has refined curriculums in IAM, Resilient systems, Blockchain, etc. Each course had 5-10 guest speakers and many hands-on labs. Students are trained to apply risk management concepts and be able to use some of the tools in the industry. Updated the NICE Framework with a total of 52 work roles needed. Hiring & internships is a many body problem.

This includes students, faculty advisors, HR managers, time, hiring manager, social media (handshake & indeed), skills (4000+ cyber vendors), & skills (52 work roles). How can we train students in all these skills? Ideas to reduce the gap by students needed to learn the language of business, bring guest lectures, on campus programs, mentor students, suggest community software, etc. Calling people to take action by starting an industry-academia group to help shrink the gaps in workforce and experience with tech talent accelerator course development.

Panel: Postulating a Better Connection for Industry & Academics

The biggest challenge to filling cyber jobs is the reluctance of industry to offer meaningful training opportunities to students, before they graduate. This is still an unsolved problem, even though people and groups are working on it. Moreover, some research suggests that the best education comes from shorter certificate-based programs, particularly beneficial to mid-career professionals. In this panel of local CISO Executives and University Professors, we will debate the issue and suggest solutions.

Panelists

Professors:

- Dr. Frederick Scholl, Cybersecurity Program Director & Associate Teaching Professor, Quinnipiac University
- Dr. Chad Williams, Chair, Computer Science - Central Connecticut State University
- Dr. Mehdi Mekni, Professor, Director of Computer Science Programs, University of New Haven

Cyber Executives

- Suzette Leal, CISM First Vice President, Chief Information Security Officer/Corporate Security Officer - Ion Bank

- Brian Kelly, Director of Information Security | CISSP, CISM - Community Health Network of Connecticut
- Dennis Klemenz, CTO - Jovia Financial Credit Union

Panel #1

Dennis says that it is unfair to provide a perfect fit for your industry needs. Every student is unique and every college is unique. In the industry we need to recognize that graduates were impacted by COVID and that they might not have a lot of direction and push the students in college.

Brian tells you to go directly to the company's website to apply instead of just dropping 500 applications. Not every student has a 4-year degree and I do see a lot of people

Suzzete says the new generation has a lack of communication, professionalism is not there, and the drive is not there as well. Ion bank is very high on hiring interns and likes to bring in them very often. When interviewing a lot of it comes from the drive and finding that a lot of students don't know exactly what cybersecurity is.

Dr.Mekni, we need to get both and not be exclusive to one or the other (certifications & 4-year degree). UNH has industry funded projects where we are funded by software by industry leaders.

Dr.Scholl, I do not have any tests but make them do labs with hand ons industry tools and make them do presentations. Healthcare, Fintech, Pentest all have their own certifications.

Dr.Williams, we collaborate a lot with high schools and do hackathons with them.

Applied GenAI for Cybersecurity: In-House LLMs

Tim Rohrbaugh

Principal/Founder: CISOsOnCall, LLM Strategic Solutions & 3x CISO

> Tim Rohrbaugh recently founded a new consulting start-up LLM Strategic Solutions, focused on applied GenAI/LLMs and the CyberSecurity mission. He is a senior security and data governance professional. He was most recently the CISO of JetBlue Airways for 3 years. Prior to his role at JetBlue, he was the CISO for financial services firm Intersection Inc (IdentityGuard) for 12 years. During this time, he was also the SVP for Product and Customer Experience for the product that started the Identity Theft protection space and grew to more than 35M subscripted consumers. His technical and cyber security experience started in the military, DoD and Federal Government. He holds two joint patents on Identity Verification.

In this discussion pod, Tim will demystify the overused term “AI,” and focus on what is really NEW. He will expand on where the hype is *real* and where it’s *not*. Participants will leave with better clarity: what this tech means, inherent risks, how to avoid the weaknesses and focus on using the strengths to positively affect security operations (and beyond). You may want to be an *Applied GenAI Engineer* by the end of this segment!

Applied GenAI for Cybersecurity, a discussion of In-House LLMs and demystifying “AI”, inherent risks, focus on using the strengths to positively affect security operations

Applied GenAI for LLM - Tim Rohrbaugh

Traditional AI has been around for a while. Tim has been a public company CISO and has been keeping track of ML. GenAI was added in 2017. “Artificial Intelligence *does not* exist but Augmented Intelligence does.” We have only scratched the service of AI.

Examples - Winter is Coming - BlackSwan (Nassim Taleb), 2010s was the first big leap: ML -> DL, etc. GenAI is the best text completion tool in human history. We can use it as an advanced google for long term knowledge and we can also give it knowledge and let it reason with it. Don’t fall into the trap of using AL, be specific with what you are using. If we have too much information in Cyber we can take GenAI and take identified agents to help you with your work; you must always stay in the loop.

> Hallucinations are a positive, if you don’t it means you broke the model. Never ask GenAI a specific question. Microsoft Copilot goes away from your device and does not do things locally. Need to put control on proprietary models because they are sending data away from our companies. Regulate the leak and not the models, use the models internally and locally. We need not security people, we need applied GenAI engineers.

Questions -

> Q: Are the open models as good as the proprietary models?
>
> Q: How do you feel about the companies that block AI?
> A: 100% block priority models but set up the other models

Your Budget is a Horse’s Ass

Ira Winkler, CISO - CYE

> Ira Winkler, CISSP is the Field CISO for CYE Security, former Chief Security Architect at Walmart, and author of You Can Stop Stupid, Security Awareness for Dummies, and Advanced Persistent Security. He is considered one of the world’s most influential security professionals, and has been named a “Modern Day James Bond” by the media. He did this by performing espionage simulations, where he physically and technically “broke into” some of the largest companies in the World and

investigating crimes against them, and telling them how to cost effectively protect their information and computer infrastructure.

He continues to perform these espionage simulations, as well as assisting organizations in developing cost effective security programs. Ira also won the Hall of Fame award from the Information Systems Security Association, as well as several other prestigious industry awards. CSO Magazine named Ira a CSO Compass Award winner as The Awareness Crusader. He was named 2021 Top Cybersecurity Leader by Security Magazine, and most recently 2022 Cybersecurity Champion of the Year by the Cybersecurity Association of Maryland.

Explore the historical influence of horse-drawn carts on railcar dimensions and how it relates to rigid cybersecurity budgeting. Join this session to learn how to apply machine learning and other mathematical concepts to justify budget allocation, optimize risk, and design effective cybersecurity programs for limited resources.

Your Cyber Budget is a Horse's Ass - Ira Winkler

It's easy to perpetuate things year after year. It is harder to innovate because of all of the new specifications, costs, etc. Keep things simple. We get firm numbers now to make decisions, but CISO do not. They go with their gut. This can now change because of better science/math, AI tools, and machine learning. We can now do automation of SOC decision making, better incident detections, etc. Other disciplines that are collecting hard numbers are operations, accounting, safety science, and supply chain. We have not applied business disciplines to cybersecurity and only some companies have data science programs in their cybersecurity department. The big problem is that CISOs get the budgets they deserve, not the budgets they need. Risk = value x (threat x vulnerability) / countermeasure. You do not want to mitigate value and threats are hard to mitigate. You can mitigate threats by not putting vulnerabilities near threats. You can either avoid, mitigate, accept, or transfer risk.

Legal Perspectives on Breaches, Ransomware & Incident Response: Trends & Predictions

Gregory Bautista, Partner - Mullen Coughlin LLC

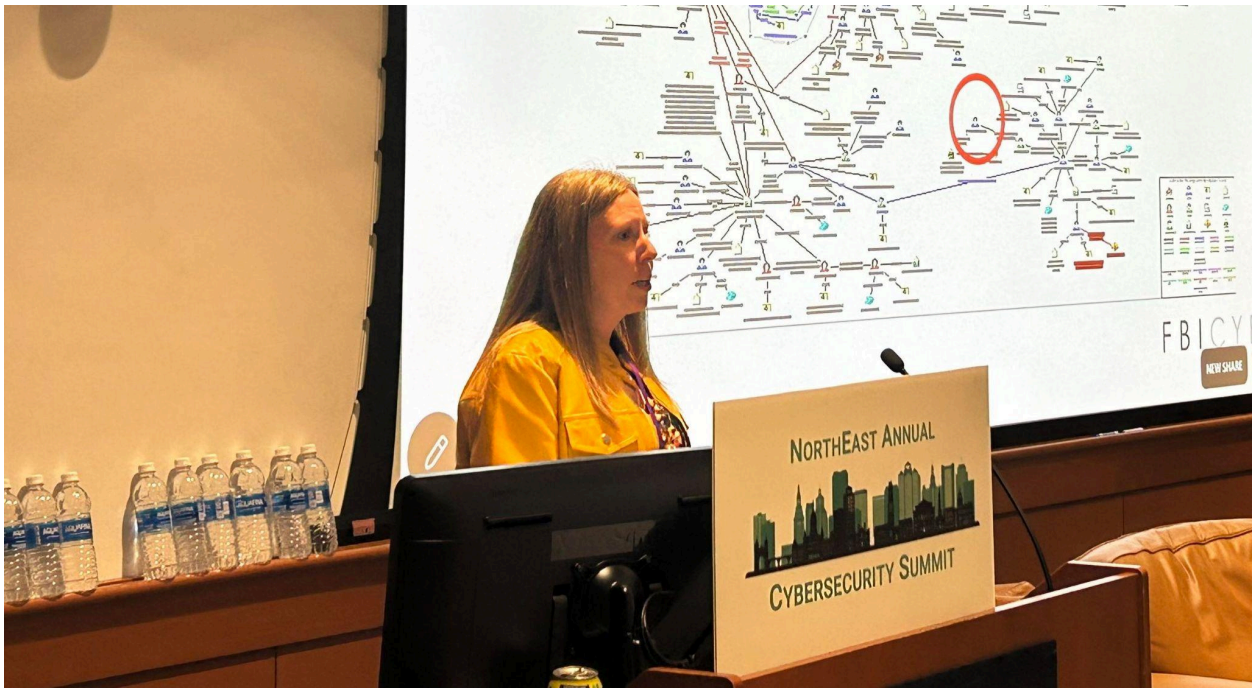
Greg Bautista is a seasoned cybersecurity attorney and civil litigator with deep expertise in data privacy and security. Over the past decade, he has guided hundreds of organizations through data breaches and security incidents, offering steady counsel during investigations, recovery, and communications to protect their financials, data, and reputation.

> Greg advises organizations on compliance with state and federal regulators, including the FTC, HHS, and NYDFS, and provides pre-incident planning services, such as incident response preparation and tabletop exercises. His clients span industries like professional services, financial services, healthcare, retail, education, and non-profits.
>
> A Certified Information Privacy Professional (CIPP/US) and International Association of Privacy Professionals (IAPP) member, Greg was named a "40 Under 40 Rising Star" by the Business Council of Westchester in 2017. He previously chaired the Cybersecurity & Data Privacy Practice at his former firm and now serves as a trusted advisor at Mullen Coughlin.

The legal perspective around ransomware incidents is discussed often, and NEACS invited an expert attorney in the field to share some fascinating and insightful data points that you will remember long after the agenda concludes today. Cyber is the singular focus for Mullen Coughlin, a law firm that handled over 14,000 incidents between 2020 and 2023. Gregory Bautista is a Partner, and brings a wealth of intelligence related to incident response, privacy litigation, and regulatory investigation defense.

When someone who can charge $900 per hour offers up some of their time for free, we should all probably listen.

> Mullen Coughlin LLC focuses on cyber. Experience ransomware, data mapping & identification, acquisitions, communications, business email compromise, & SEC disclosure rule. Introduced by the brokers or by the insurance companies but engage directly with the companies. Gregory’s firm follows the market value. Cyber insurance now does have requirements and this can help CISO’s get their budget and other needs. Gregory provided statistics on ransomware incidents, business email compromise incidents, and more. Coughlin LLC has very close relations with the FBI and law enforcement. Gregory cautions to evaluate your recovery plan and downtime procedures, notice timelines, etc. Most companies have switched to data mining.



Safeguarding Cyberspace: How the FBI Internet Crime Complaint Center (IC3) Protects and Partners for a Safer Internet

Melissa McBee-Anderson

Management and Program Analyst - Federal Bureau of Investigation, IC3

> Melissa has served with the FBI for 29 years in the Cyber, Human Resources, and CJIS Divisions. The IC3's core functions are to collect criminal Internet activity from victims, analyze the data submitted to identify emerging threats and new trends, post public service announcements for awareness of crimes and methods identified, and aggregate related complaints for referral to law enforcement. Melissa currently serves on the IC3 Criminal Team, which addresses criminal and cyber-enabled scams to include Investment, Romance, Tech Support, and the Elder Fraud Initiative. Melissa provides case support and analysis for FBI field offices, local and state law enforcement, international partners, and the private sector. In addition, Melissa works with public and private alliance partners to define growing schemes and coordinate involvement with all levels of law enforcement to ensure on-line activity continues to be safe for both consumers and industry.

The FBI's Internet Crime Complaint Center (IC3) provides a central platform for reporting internet-facilitated crimes, such as ransomware, phishing, business email compromises, and identity theft. It analyzes submitted data to identify emerging threats, publishes alerts to raise public awareness, and forwards actionable intelligence to law enforcement at all levels for potential investigation.

> While the IC3 does not contact complainants or provide status updates, it allows victims and their representatives to submit reports online and add supplemental information as needed. The IC3's mission includes fostering partnerships with industry and law

enforcement to combat cybercrime effectively. This presentation highlights how IC3 assists law enforcement by processing financial fraud kill chains and offering tools to understand and address internet crimes.

The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation (FBI) concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness. Some of the most common scams, frauds, and other matters reported to the IC3 are:

- Confidence/Romance Fraud
- Investment Fraud
- Tech Support Fraud
- Ransomware
- Business Email Compromises
- Data Breaches
- Non-Payment / Non-Delivery
- Phishing / Vishing / Smishing / Pharming
- Identity Theft
- Extortion
- Employment Fraud
- Credit Card / Bank Fraud

What does the IC3 do?

- The IC3 is the central point for internet crime victims to report and alert the appropriate agencies to suspected criminal internet activity.
- The IC3 reviews and analyzes data submitted through its website to identify emerging threats and new trends.
- Public service announcements, industry alerts, and other publications outlining specific scams are posted to the www.ic3.gov website.
- The IC3 aggregates actionable complaints to build referrals, which are forwarded to local, state, federal, and international law enforcement agencies for potential investigation.

What will the IC3 not do?

- The IC3 will not reach out to victims regarding a complaint.
- If additional information is obtained, victims are encouraged to file additional complaints with the new information and to identify the submission as a supplemental report.

Who can file a complaint with the IC3?

- Both victims and/or others on behalf of the victim can file a complaint on www.ic3.gov.

Other information about the IC3 submission process

• No complaint number will be provided during the submission process.
• You will have the option to print and/or save a copy of the complaint at the end of the submission process.
Presentation of above-listed objectives.

This presentation is an information session to provide LE with how the IC3 can assist LE and how the IC3 processes financial fraud kill chains.

Additional information about reporting to the FBI

• Information involving internet related fraud should be reported at www.ic3.gov.
• Information involving terrorism, threats to national security, or other violations of federal law should be reported to the FBI at 1-800-CALL-FBI or at www.tips.fbi.gov.
• If someone is imminent danger, call 911 or your local police immediately.
• Reports should be submitted as timely as possible.
• The information provided is vital in holding those responsible accountable.

Panel: CISOs and Cyber Agencies

Today, we will hear from numerous agencies from the federal and state governments, all charged with education, information and/or enforcement around fraud and cyber. Our tax dollars at work, they provide a plethora of services and direct help for private and public sector organizations.

In this discussion, we will hear from some of the CISOs who have been leveraging intelligence, education, and services from those agencies as well as leaders from within the FBI, IRS, DHS, and the CT State Fusion Center, CTIC. They will discuss how they have been working together in recent years, and suggest ways in which the private sector and government agencies can learn from each other.

Panelists

Cyber Agents

- Supervisory pecial Agent Alexandra Sevillano, FBI Field Office
- Special Agent Carlo Nastasi, IRS Criminal Investigations
- Jon Hale, Cyber Intelligence Analyst, CT State Intelligence Center

Cyber Executives

- William Malik, former CISO, Research VP, Gartner & Founder, Malik Consulting
- Justin Hickey, Deputy CISO, State of Connecticut
- Conor Phoenix, Manager of Incident Response, Hartford HealthCare

CISOs & CYBER AGENTS: GOVERNMENT AGENCY & PRIVATE SECTOR COLLABORATION

Conor, FBI domestically has around 56 different offices. Have had investigators from the local police department working with us and other agencies.

Carlo, was following money laundering cases. TD bank cases involved a lot of agencies. CISOs can be more collaborative and help with the investigation.

William, the biggest problem in the 90s was getting people to participate. When you bring in law enforcement they really do want to solve the problem. Worse time to try and build relationships is when the agents are in the middle of the investigation.

Justin, was getting phishing attacks every week. Decided to get the sites taken down and had a talk with an agent in New Haven and the federal agencies were able to write the letters to ISP.

AI in Cybersecurity: Balancing Innovation, Governance & Risk

Gavin Anthony Grounds, MBA, CEng, CITP, MIoD, FBCS, CRISC, CDPSE

CEO & Co-Founder, Mercury Risk and Compliance, Past President, ISACA Austin Chapter
Former: Meta, Verizon, HP/HPE/DXC, Bank of Bermuda (now HSBC)

Gavin Grounds is a pioneering figure in cybersecurity and risk management, renowned for his technical prowess and innovative strategies. With a rich history as a CISO and a leader in Cybersecurity Strategy and RiskManagement, Grounds has held executive leadership roles at Meta, Verizon, DXC, andHP/HPE. His tenure at these Fortune 500 companies was marked by groundbreaking initiatives and thought leadership in cyber security, risk quantification, payments processing, and cross-jurisdictional taxation.

Grounds is celebrated for his contributions to industry best practices, honed through participation in and speaking at various Security and GRC conferences including Gartner, ISACA, ISSA, RSA, amongst others. Beyond his professional achievements, he is deeply committed to philanthropy, supporting child safety, human trafficking prevention, and suicide prevention.Grounds embodies the blend of expertise, compassion, and visionary leadership, making him an able partner in navigating today's cybersecurity challenges and risks.

Grace Beason, MBA, CRISC, CISM, CISA,CDPSE

Director Of Governance, Risk and Compliance - Guidewire Software

Co-Founder & Board Member, Mercury Risk and Compliance.

Grace is a distinguished expert in Governance, Risk, and Compliance, with two decades of experience. She has built and led GRC programs in large-scale IT and OT environments, holding key leadership roles at Guidewire, DXC, HP/HPE, and the State Department of Mental Health. Beginning her career as a clinical social worker, Grace developed exceptional skills in understanding human behavior, enabling her to connect effectively with leaders, customers, and team members. Transitioning into legal compliance, she navigated complex regulatory frameworks, spearheading global GRC transformations for 3,000+ enterprise customers at HP/HPE/DXC Technology. As Director of GRC at Guidewire, she applies her expertise to SMB environments.

Renowned for innovation, Grace developed Automated Control Efficacy Testing (ACET) and co-founded Mercury Risk and Compliance, incorporated the Advanced Asset-Value Based Risk Quantification (AVRQ) methodology. Coupled with her dedication to humanitarian efforts, she is a transformative leader in cybersecurity.

Artificial intelligence (AI) is reshaping the landscape of cybersecurity governance, risk, and compliance (GRC), presenting both transformative opportunities and complex challenges. This session addresses the critical question facing executives: how can we harness the innovative potential of AI while managing its inherent risks and meeting regulatory demands?

Leveraging insights from leading industry analysts and research groups, this presentation explores the dual role of generative AI as a strategic asset and a governance challenge. Attendees will gain actionable strategies to establish governance frameworks that scale with AI's rapid evolution, manage third-party risks effectively, and align AI initiatives with organizational priorities.

Panelist Bios

Suzette Leal, CISM

First Vice President, CISO, Corporate Security & GLBA Officer - Ion Bank

Ms. Leal is a highly accomplished cybersecurity leader with over 20 years of experience in the financial services industry. At Ion Bank, Suzette has built an exemplary career at the intersection of information security, business continuity, and operational resilience.

She earned her Certified Information Security Manager (CISM) certification from ISACA in 2013 and joined Ion Bank in 2014 as Vice President of Information Security, quickly establishing herself as a trusted authority on regulatory compliance, technology risk management, and business continuity planning. Suzette is the Chairperson of the Bank's Information Security and Cybersecurity Council, where she leads efforts to safeguard sensitive information, strengthen cybersecurity frameworks, and implement robust vendor management practices.

Her expertise extends to conducting business continuity assessments, disaster recovery simulations, and developing comprehensive training and awareness programs. Suzette has been instrumental in introducing innovative tools like WolfPAC to align risk management strategies with the bank's overall risk appetite. She also plays a pivotal role in implementing physical security measures and overseeing operational security for premises and personnel.

Suzette is actively involved in the industry, serving on the board of the Connecticut chapter of the Association of Continuity Professionals (ACP) and as President of the WolfPAC User Group. Her passion for safeguarding organizations, coupled with her commitment to fostering collaboration and compliance, makes her a dynamic presenter and trusted voice in the cybersecurity community.

Brian Kelly, CISSP, CISM, CEH, MSIA

Director of Information Security, - Community Health Network of Connecticut, Inc.

In his current role Brian supports the safeguarding of information assets against unauthorized use, disclosure, modification, damage, or loss by developing, implementing, and maintaining methods to provide a secure and stable environment for data and related systems.

Before joining Community Health Network of Connecticut Brian was the CISO at Quinnipiac University and the Cybersecurity Program Director at EDUCAUSE. Brian is also an Adjunct Professor at CT State Community College (at Naugatuck Valley) where he has developed and teaches cybersecurity courses.

Brian has diverse experience in information security policy development, awareness training, and regulatory compliance. He provides thought leadership on information security issues across industries and is a recognized leader in his field.

Brian holds a bachelor's degree from the University of Connecticut and a master's degree from Norwich University. He has served in various leadership roles on the local boards of the ISSA, InfraGard, and HTCIA chapters. Brian is also a retired Air Force Cyber Operations Officer.

Prof. Mehdi Mekni, Ph.D.

Computer Science & Cybersecurity and Director of the Computer Science Program
Faculty Fellow, Connecticut Institute of Technology (CIT) - University of New Haven

Dr. Mehdi Mekni is a distinguished academic leader known for advancing workforce development and integrating industry-recognized credentials into academic programs. With expertise in computer science, cybersecurity, and software engineering, Dr. Mekni has contributed to R&D and technical project management in industry. He has held prominent academic roles at institutions like the University of Minnesota and St. Cloud State University, where he developed groundbreaking programs, including the BS in Software Engineering.

As Program Director for the Bachelor of Science in Computer Science at the University of New Haven, Dr. Mekni drives innovation in cybersecurity, system programming, and game design education. A Fulbright Specialist, he champions inclusivity in computing and fosters pathways for diverse participation in the tech sector. His research focuses on cybersecurity education, game development, mixed reality, and AI applications in software development.

Recipient of accolades like the AAG William L. Garrison Award, Dr. Mekni continues to shape the future of technology education, preparing the next generation of tech leaders.

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.

Alexandra Sevillano, Special Agent, FBI New Haven Field Office

Alexandra Sevillano is from St. Petersburg, Florida. She attended Florida State University on an athletic scholarship to play volleyball and graduated with a degree in Public Relations. She subsequently obtained her Juris Doctorate at Stetson College of Law in 2007 and became an Assistant State Attorney in Pinellas County, Florida. Alex joined the FBI in 2016 and was assigned to the Washington DC Field Office where she worked counterintelligence investigations. In February 2023, she was promoted to FBI Headquarters' Cyber Division and in November 2024 she joined FBI New Haven's cyber team.

Jonathan Hale, Cyber Intelligence Analyst - CT Information Center (CTIC)

Jon Hale is CTIC's Cyber Intelligence Analyst, coming from a 20+ year military career specializing in the neutralization of national security threats, intelligence collection and analysis, and cyber operations.

Carlo Natassi, Special Agent - IRS Criminal Investigations

Special Agent Carlo Nastasi began his career with the Internal Revenue Service Criminal Investigation (IRS-CI) in 2008. Prior to joining IRS-CI, Agent Nastasi was an Audit Senior at Deloitte and Touché and graduated from Pace University with a bachelor's degree in finance and accounting. He is currently the lead agent on the SAR review team and is the liaison to the private banking industry. His role includes leading high level money laundering and Bank Secrecy Act investigations and providing training to the BSA compliance industry.

During his time with IRS-CI, Agent Nastasi worked various tax evasion, money laundering, and Bank Secrecy Act investigations relating to financial institutions, OCDETF, international tax, Securities Fraud, Ponzi Schemes, Political Corruption, and Mortgage Fraud. Many of these investigations involved tracing funds globally including, fiat currency, crypto, foreign currency, TBML, and informal money transfer systems. Agent Nastasi also served as a Task Force Officer with the Federal Bureau of Investigations assisting the white collar and political corruption divisions from 2011 to 2016.

William J. Malik, CISA

Former Research Director at Gartner & Founder, Malik Consulting

I can make complex ideas clear – but not simple, because some of this stuff isn't simple. I help clients achieve an effective information security posture spanning endpoints, networks, servers, cloud, AI, supply chain security, privacy, and the Internet of Things. This involves technology, policy, and procedures, and impacts acquisition/development through deployment, operations, maintenance, and replacement or retirement.

Currently working on SBOM and AIBOM schema.I worked as an application programmer with the John Hancock Insurance company; an OS developer, tester, and planner with IBM; a research director and manager at Gartner for the Information Security Strategies service and the Application Integration and Middleware service, and served as CTO of Waveset, an identity management vendor acquired by Sun. At Trend Micro, I provided research and analysis of the current state and future trends in information security. I participate in the ISO/IEC 62443 standards body, the Cyber-Informed Engineering work group, and the CISA ICT security Work Group. Over 180 publications, speaker at numerous events worldwide. Attended MIT, majoring in Mathematics. CT InfraGard/ ISACA member.

Justin Hickey, Deputy CISO - State of Connecticut

Justin is certified, experienced, and educated in many facets of network security, compliance, and security architecture. Justin is passionate about security and privacy and has served as an advisor to various boards and committees.

For the past 30 years he has designed, implemented, supported and secured a variety of different platforms. Sample projects spearheaded include; multiple firewall layer Internet Infrastructure;

Network Access Control, Mobile Device Management, Penetration Scanning and Testing, PKI, URL Filtering and Reporting, Wireless Networking, Network Monitoring and Alerting, Remote Access with IPSec and SSLVPN's, Load Balancing and Fault Tolerance, In-line Virus Scanning, Disaster Recovery and BCP Planning, Traffic Shaping and Reporting, and much more.

Dennis Klemenz, Chief Technology Officer - Jovia Financial Credit Union

Dennis Klemenz is a highly regarded technology expert and accomplished academic with over 25 years of experience in diverse industries, including academia, aviation, manufacturing, law enforcement, healthcare, emergency services, cybersecurity, technology, and financial services. This extensive background gives him a unique perspective on technology and business practices across multiple critical infrastructure sectors. Dennis is the Chief Technology Officer at Jovia Financial.

In addition to his professional endeavors, Dennis has dedicated the past 15 years to teaching at various universities, where he imparts knowledge on cutting-edge topics, including data and AI strategies, distributed/cloud computing, cybersecurity, mobile development, operating systems, secure computing, and cryptocurrencies/blockchain. Throughout his academic career, Dennis has been recognized for his excellence in teaching, earning distinctions at multiple institutions and receiving nominations for teaching awards at each university where he has taught.

Outside of his professional pursuits, Dennis supports local charities, including Habitat for Humanity and Shepherds Mentors, where he mentors high school students at his alma mater, Notre Dame of West Haven. A passionate Buffalo Bills fan, he brings his enthusiasm for the Bills wherever he goes. Hide the folding tables when he's around…Go Bills!

Conor Phoenix, Manager of Incident Response, Hartford HealthCare & former Supervisory Special Agent, FBI New Haven Field Office

Conor Phoenix, the current Manager of Incident Response for Hartford HealthCare (HHC), was hired by HHC in June 2024, following his retirement from the Federal Bureau of Investigation (FBI) after 25 years of service. Conor spent nearly his entire career focused on cyber investigations, covering such areas as crimes against children, violations of intellectual property rights, internet fraud and computer intrusions committed by criminals, nation-states, and terrorists.

While most of Conor’s time as a Special Agent was spent in New Haven, Connecticut, it was not his only posting. In 2011, Conor spent three months working in Driebergen, Netherlands alongside the Dutch Police’s National High Tech Crime Unit. Upon his return, Conor spent the next three years working at the FBI Headquarters’ Cyber Division in Washington, DC. Then, in 2014, Conor moved to London, England and spent the next few months working

with the United Kingdom's Security Service (MI5). Conor subsequently returned to Connecticut, and in 2019 he was promoted to the position of Supervisory Special Agent for the FBI's cyber squad in New Haven. He remained in that position until his retirement.

Conor's investigations have led to the arrest of numerous individuals throughout his career, both in the US and abroad, including the 2017 arrest of a Russian botnet operator in Spain and the 2019 arrest of Russian cryptors in the US and Estonia.

Conor lives in Hartford County with his three teenage sons.

Moderator: Michael Hiskey, Founder - CxO Security Forum

Michael Hiskey is an author, blogger, moderator and speaker who has been in enterprise B2B strategy for more than 20 years. His articles have been in Forbes, Information Week, WSJ.com, InfoWeek, ITProPortal, and he has made appearances on CNBC and C|Net.

He has run hundreds of cybersecurity conferences, and having worked in cyber, fraud, AML/KYC, digital identity and data/analytics, he started the CxO Security Forum to change the way executives connect for education, mentoring and networking.

Michael has primarily worked for software and services solutions providers, who solve for the challenges in the realms of cybersecurity, FinTech, data, analytics, cloud computing and AI. He has held Chief Marketing Officer (CMO) roles at Avanan, Semarchy, Socure, Kognitio, Trifacta, Chief Strategy Officer (CSO) Roles at CISO ExecNet, Data Connectors and Engagez, and executive leadership roles at MicroStrategy and IBM.

After starting his career in finance, Michael spent almost 10 years at IBM. Some notable efforts there included leading Subject Matter Expert (SME) Teams for Analytics, Data Warehouse Product Development, and Advanced Customer Support. Michael returned to the US in 2010 after a successful assignment in Brasil, where he helped grow the Software Lab and connected sales, partners and clients supporting Cognos, DB2 & Informix products.

Michael is a graduate of the Columbia Business School in New York City. He is the husband of one current, and GirlDad to two future women in technology.