CxO Security Forum

Atlantic City CyberSecurity & Fraud Forum

2024 Atlantic City CyberSecurity & Fraud Forum (ACCSFF)

Event Summary, Agenda, and Discussion Highlights

August 22, 2024 * Cape May, NJ

Introduction

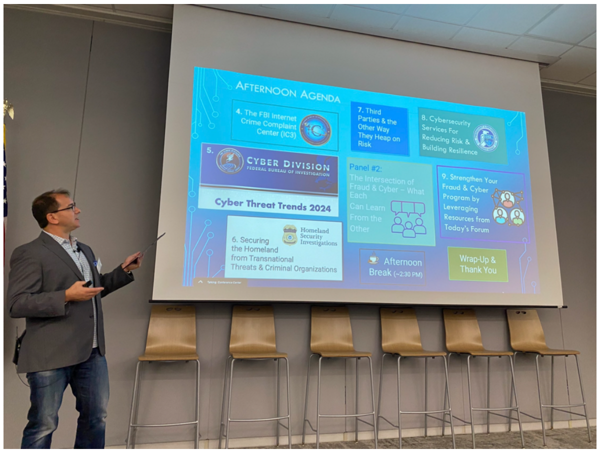
The 2024 Atlantic City CyberSecurity & Fraud Forum (ACCSFF), held on August 22nd in Cape May, NJ, brought together 150 cybersecurity, risk, fraud prevention, and compliance leaders from both private and public sectors. With over 2,000 professionals invited and discussions held under the Chatham House Rule, the event emphasized collaboration, operational insights, and peer-led dialogue.

Agencies
FBI Cyber Division
Identify • Pursue • Defeat
Federal Bureau of Investigation
IC3
Internet Crime Complaint Center
Cybersecurity & Infrastructure Security Agency
CISA
The United States Secret Service
CFTF
Cyber Fraud Task Force
NJ Cybersecurity & Communications Integration Cell
Department of Justice
Federal Bureau of Investigation
U.S. Department of Homeland Security
Homeland Security Investigations

Forum Themes and Focus Areas

The agenda addressed a number of key themes with high-level takeaways, including:

- The evolution and application of Zero Trust principles
- Cross-sector collaboration between government and enterprise
- Convergence of fraud prevention, risk management, and cybersecurity
- Current and emerging cyber threat vectors, including ransomware, AI, and supply chain risk
- Leveraging government resources to strengthen organizational resilience
- Real-world case studies and panel insights on risk, fraud, and cyber readiness



Afternoon Agenda

4. The FBI Internet Crime Complaint Center (IC3)

5. Cyber Division Federal Bureau of Investigation — Cyber Threat Trends 2024

6. Securing the Homeland from Transnational Threats & Criminal Organizations — Homeland Security Investigations

7. Third Parties & the Other Way They Heap on Risk

Panel #2: The Intersection of Fraud & Cyber – What Each Can Learn From the Other

8. Cybersecurity Services For Reducing Risk & Building Resilience

9. Strengthen Your Fraud & Cyber Program by Leveraging Resources from Today's Forum

Afternoon Break (~2:30 PM)

Wrap-Up & Thank You

Morning Agenda & Session Highlights

Welcome & Introductions

- Introductions by ISACA, ISC2, CSA, InfraGard, and other supporting associations
- Highlighted collaboration among agencies including CISA, FBI, NJCCIC, and DHS
- Encouraged participation and submission of questions via email or text

Keynote: Win the Cyber War with Zero Trust

- Presented by John Kindervag, creator of Zero Trust
- Introduced Zero Trust as a strategic model based on 'never trust, always verify'
- Discussed segmentation, micro-perimeters, and applying Zero Trust principles in layered defense strategies
  - Everyone is currently in a cyberwar: is a battle of wills – are you willing to win?
  - ***"No More Chewy Centers":*** Introducing the Zero Trust Model of Information Security (this was the original document from Forrester, authored by John that launched the concept of Zero Trust.
- "The Federal Government must adopt security best practices, advance toward Zero Trust Architecture…"
  - What is Zero Trust?
    - Not a product, "A strategy designed to stop data breaches & prevent other cyber attacks from being successful by eliminating trust from digital systems"
    - Data breaches occur when data is leaked into the hands of malicious hands and when no one is aware of what's going out: what goes out is more important than what comes in
    - Common denominator of all cyber attacks: trust
    - Dwell time: time that an attacker is in the system without being seen
      - Get rid of dwell time by use of zero trust

ZERO TRUST

A strategy designed to stop data breaches and prevent other cyber-attacks from being successful by eliminating trust from digital systems.

Protect data assets with zero trust environment with 5-step methodology

1. **Define your protect surface -** Define the protect surface: what are you trying to protect?
   - Want to reduce the attacks to the protect surface especially
   - DAAS elements: Data, Applications, Assets, Services
2. **Map the transaction flow -** how does it work as a system?
   - Architect a Zero Trust environment
3. **Architect a zero trust network**
4. **Create zero trust policy**
5. **Monitor and maintain the network**

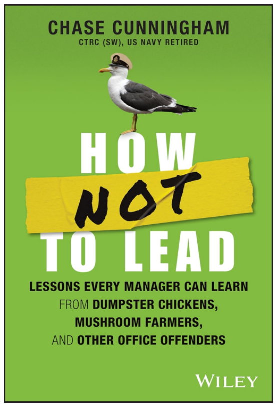
- Implement segmented networks; Zero trust defines network segmentation – questions to ask:
  - Why are you segmenting? What could go wrong? What has failed in the past?

  - How are you enforcing segmentation? Take a segmentation gateway to connect to the protect surface
  - Flat networks are dangerous: once attackers are there, they control the network
  - Zero trust limits the attacker's mobility through a network, which better secures data

- Designed to be strategic and to be using commercially available technology
- Learn from past mistakes: when networks are compromised, learn from those mistakes and see what can be done better, why did the network fail, how can it be improved and built upon, what should be prioritized, perform "cyber autopsies" – digital forensic investigation
- Proper network segmentation = more secure
- First person to follow shirtless dancing guy!! More incentive for other people to join along
- Trust, but verify": meant as a joke and is not literal - many don't verify as they may think it's rude, but these kinds of human emotions have been creeping their way into the ways workers enforce cybersecurity which is not ideal

Fireside Chat with John Kindervag

- Extended discussion of Zero Trust in practical deployment
- Reinforced segmentation as the cornerstone of secure architectures


CHASE CUNNINGHAM
CTRC (SW), US NAVY RETIRED
HOW
NOT
TO LEAD
LESSONS EVERY MANAGER CAN LEARN FROM DUMPSTER CHICKENS, MUSHROOM FARMERS, AND OTHER OFFICE OFFENDERS
WILEY

Leadership in Cyber: Dr. Chase Cunningham

- Explored leadership challenges and innovation in the face of persistent threats
- Touched on the psychology of cyber warfare and the role of behavioral insights

Reading material

- *Cyber Warfare - Truth, Tactics, and Strategies* by Chase Cunningham
- *gAbrIel* by Chase Cunningham
- *How Not to Lead* by Chase Cunningham
- *Rip Tide: A Narrative on Cyber Security Failures at the National Level* by Chase Cunningham
- *Project Zero Trust* by George Finney and foreword by John Kindervag

What implementation should look like:

- Who should be allowed to have access to what application and which protect surface does that application protect, and how are you going to look at it to make sure it's clean
- Each policy statement is a firewall

- Cybersecurity should fit you and your organization: do not implement something just because someone else did it… Always ask the question: who makes the money?
- Vendors will always try to sell their technology, make sure it is fitting for you first

Panel #1: Agency & Private Sector Collaboration

- Featuring leaders from the FBI, CISA, NJCCIC, CHOP, MGM Resorts, AtlantiCare, and Lowenstein Sandler
- Discussed how threat intelligence and education from government agencies are applied in the field

Afternoon Agenda & Session Highlights

Session: The FBI Internet Crime Complaint Center (IC3)
- Presented by FBI Special Agent Michelle Liu
- Shared data on increasing cyber complaints, ransomware statistics, and recovery efforts
- Highlighted elder fraud, BEC, and cryptocurrency-based scams

Session: Third Parties & Risk

- Presented by Mark Wolfrey (RKL LLP, ACAMS)
- Explored real-world case studies of third-party failures including PPP loan fraud and prepaid card oversight gaps
- Emphasized contract diligence, ongoing monitoring, and information security audits

Session: Securing the Homeland from Transnational Threats

- Led by Homeland Security Investigations (HSI)
- Outlined priorities including cybercrime, financial fraud, and border-related investigations
- Discussed tools like the El Dorado Task Force and cyber forensic capabilities

Session: CISA Cybersecurity Resources

- Presented by Christopher Kay, CISA Region II Coordinator
- Provided overview of freely available federal cybersecurity services: scanning, toolkits, tabletop exercises
- Emphasized resilience through CSET, WAS, SCuBA, and the .gov initiative

PANEL DISCUSSION: THE INTERSECTION OF FRAUD & CYBER

Increasingly, there is a coming together of these two areas. Fraud Fighters are the savvy professionals helping their organizations prevent Account Take Over (ATO), identity theft-related fraud, and the like… They are often thinking about Know Your Customer (KYC) and Anti-Money Laundering (AML) initiatives, as well as compliance in regulated industries. We have started to see more often financial fraud professionals merged into the teams that report to a CISO.

In this discussion, our panelists will debate this idea, and talk about what cybersecurity professionals can learn from each other.

Panel #2: The Intersection of Fraud & Cyber

- Panelists from InfraGard, FBI Atlantic City, IRS, and private sector risk leaders
- Discussed ATO, identity fraud, KYC/AML convergence, and aligning fraud ops with cyber leadership

Closing: Strengthen Your Cyber Program

- Presented by Ken Fishkin (ISC2 NJ, Lowenstein Sandler)
- Provided a practical roadmap to incorporating agency tools, peer networking, and best practices

Key Takeaways & Community Impact

The 2024 ACCSFF provided not just strategic insight, but a platform for regional collaboration. Senior leaders left with new partnerships, actionable intelligence, and access to federal resources. With a focus on leadership, community, and resilience, the Forum served as a model for how cyber and fraud leaders can address today's most pressing challenges—together.

Featured Speakers & Discussion Leaders

John Kindervag

John Kindervag is considered one of the world’s foremost cybersecurity experts. With over 25 years of experience as a practitioner and industry analyst, he is best known for creating the revolutionary Zero Trust Model of Cybersecurity. As Chief Evangelist at Illumio, he is responsible for accelerating awareness and adoption of Zero Trust Segmentation.

Previously, John served as Senior Vice President at On2IT, Field CTO at Palo Alto Networks, and as Vice President and Principal Analyst at Forrester Research, where he authored the foundational research on Zero Trust. In 2021, he was appointed to the President’s National Security Telecommunications Advisory Committee (NSTAC) Zero Trust Sub-Committee and co-authored the landmark Zero Trust report to the President. That same year, he was recognized as CISO Magazine’s Cybersecurity Person of the Year. John also advises the Cloud Security Alliance and NightDragon, a cybersecurity-focused venture capital firm.

Dr. Chase Cunningham

Dr. Chase Cunningham, widely recognized as “Dr. Zero Trust,” is an internationally respected cybersecurity strategist, thought leader, and keynote speaker. With more than two decades of operational experience, Chase has advised the U.S. Department of Defense, the Executive Branch, and Fortune 500 companies on advanced cyber defense strategy, threat intelligence, and Zero Trust security frameworks.

As a former Senior Analyst at Forrester Research, Chase helped define and popularize the modern Zero Trust approach. Earlier in his career, he served in the U.S. Navy, where he worked on advanced cryptographic systems and national cybersecurity operations. He is also the author of multiple books, including *Cyber Warfare: Truth, Tactics, and Strategies*—an industry essential that was inducted into the National Cybersecurity Canon Hall of Fame.

Chase holds a PhD in Computer Science and Cybersecurity and maintains both CISSP and CEH certifications. His dynamic, no-nonsense presentation style and practical insights have made him one of the most sought-after speakers in the cybersecurity community.