CHICAGO | SEPT 25-26

Program Guide

@SANSDefense #SANSDataBreachSummit

Agenda

All Summit Sessions will be held in Chicago River Ballroom (unless noted).

All approved presentations will be available online following the Summit at
https://www.sans.org/summit-archives/cyber-defense

Monday, September 25

8:00-8:45 am	**Registration & Coffee** (LOCATION: CHICAGO RIVER BALLROOM)
8:45-9:30 am	***Data Breaches: The U.S. Secret Service Perspective*** Assistant Special Agent in Charge Chevraux will share insights from the Secret Service's experience of over 30 years of investigating and bringing to justice those responsible for some of the largest data breaches in history. Topics will include threat tactics, techniques and procedures (TTPs); best practices and lessons learned; working with law enforcement; and case studies that involved apprehending some of the most prolific data breach actors to date. ***R. Matthew Chevraux**, Assistant Special Agent in Charge, U.S. Secret Service, Office of Investigations, Cyber Strategy and Outreach*
9:30-10:15 am	***Panel: A Practical Perspective on Preparation and Response*** Security incidents are regular occurrences, but only a few of them rise to the level of "data breaches" or significant compromises. These seasoned security pros will share their hard-earned wisdom on a number of topics including: assessing risk; determining the magnitude of an incident; coordinating response across multiple departments; holding vendors accountable; the looming specter of ransomware; and fostering an organizational culture of security and privacy, and legal compliance. MODERATOR: ***Rick Kam**, President/Co-Founder, ID Experts* PANELISTS: ***Meredith Harper**, Chief Information Privacy & Security Officer, Henry Ford Health System* ***Erika Riethmiller**, Director, Corporate Privacy-Incident Program, Anthem, Inc.*
10:15-10:35 am	**Networking Break** (LOCATION: BALLROOM PRE-FUNCTION)

Monday, September 25

10:35-11:10 am	***Fighting Ransomware Blindfolded*** A ransomware incident paralyzed a large multinational company with subsidiaries in Brazil, India, and the US. Responders in Brazil discovered that the ransomware was new, unknown to the InfoSec community. All they had to start with was this phrase: "You are Hacked ! H.D.D Encrypted, Contact Us For Decryption Key (w889901665@yandex.com) YOURID: 123152." They possessed no malware sample, no encrypted files and no Google results. This session will describe how management in the Brazilian subsidiary made decisions each step of the way as the local response team analyzed and ultimately defeated the Mamba ransomware. ***Renato Marinho**, MSc, Morphus Labs (Brazil); Incident Handler, SANS Internet Storm Center*
11:10 am - 12:00 pm	***The Legal Intersection of IT and Privacy: Why IT and Legal Should be BFFs*** In this session, attorney Melissa Ventrone will explain why the legal team should be your new best friend. When should legal be involved in IT projects? How do you get them involved, yet not over-involved? Learn how creating a strong IT/legal relationship will help protect you should the worst occur. ***Melissa Ventrone**, CIPP/US, Thompson Coburn LLP*
12:00 -1:00 pm	**Lunch** (LOCATION: CHICAGO BALLROOM)
1:00-1:35 pm	***Maintaining Confidentiality During an Investigation*** What happens to our corporate information if we report a data breach to the FBI? The discussion will address the authorities upon which the FBI relies when accepting, requesting, and compiling information during a criminal investigation, and how the FBI maintains and protects the information it collects. The talk will include an introduction to the Freedom of Information Act and the federal regulations which apply to disclosure in civil and criminal matters. Finally, CDC Green will provide tips and advice as to how to work most effectively with cyber investigators while still maintaining the confidentiality of sensitive corporate data. ***Kristine Green**, Chief Division Counsel, FBI Atlanta*
1:35-2:05 pm	***It's Not If But When: How to Create Your Cyber Incident Response Plan*** A strong incident response plan is a key component of any organization's cyber defense. Many organizations, however, have an ineffective plan or no cyber response plan in place at all. We only need to look to the daily news to see the impact that an ineffective cyber response can have on an organization's bottom line. A strong plan can help you identify and respond quickly to a cyber incident, and mitigate the financial and reputational costs. This session will explore the difference between an event and an incident, and why the distinction is important. Learn how to build out your Incident Response Team (IRT) and who should be included. Understand the Incident Response Process - who does what, and when. Experience a walk-through of a Cyber Incident scenario and discuss possible actions and outcomes. ***Lucie Hayward**, Managing Consultant - Investigations & Disputes, Kroll* ***Mike Quinn**, Associate Managing Director, Kroll*
2:05-2:30 pm	**Networking Break** (LOCATION: BALLROOM PRE-FUNCTION)

Monday, September 25

2:30-2:50 pm	***Overview of Afternoon Exercise***
2:50-4:45 pm	***Data Breach Advanced Exercise*** When many smart people are in the same room, everyone can learn from everyone else. Leaders will walk the assembled Summit participants through a realistic, challenging case scenario for enterprise management that faces a cyber crisis. The scenario will raise a thicket of technical, practical, legal, and public communications issues. As these issues come up, the floor will be open for questions, discussion and debate. Participants will evaluate the options available to management and learn by living through a simulated experience with peers and experts.
4:45-5:00 pm	***Summary/Closing Remarks***
5:00-6:00 pm	**Networking Reception** (LOCATION: CHICAGO RIVER FOYER) *Sponsored by:* AIG axio
6:00-7:30 pm	VENDOR-SPONSORED @NIGHT TALK: *Sponsored by:* AIG axio ***Debunking the Myths about Cyber Insurance: How Security and Cyber Insurance are Actually Hitting It Off*** There are many myths when it comes to cyber insurance and the role the insurance industry plays in a holistic cyber resilience strategy. Insurance has not always been popular among the security community, however, to reduce cyber risk across the organization, security leaders are looking at cyber insurance as a key consideration in the overall cyber security strategy. In this session, we will debunk the common myths and focus on realities of cyber insurance and the positive role the insurance industry plays in managing cyber risk and supporting a holistic cyber resilience strategy. The Myths vs. Reality: • **Myth:** Cyber insurance policies force dubious security requirements and thresholds • **Reality:** False; The current insurance marketplace features nearly 75 providers of coverage, the vast majority of which do not feature such terms. • **Myth:** Cyber insurance policies don't pay claims. • **Reality:** False; most cited claim denial cases are cherry picked and sensationalized, or flat out misrepresented. Cyber policies have a strong track record of paying claims for all industry classes for losses such as forensics expenses, incident response costs, business interruption losses and bricked technology assets. • **Myth:** The only firms that invest in cyber insurance are those that are not confident in their cyber security; it's an admission of failure. • **Reality:** Firms that purchase cyber insurance view it as a valuable financial control to effectively complement their traditional control set. How many security leaders set aside hundreds of thousands per year in a 'rainy day' fund to pay for forensics and incident response? In this session, we will walk through a real-world scenario in which an organization in the critical infrastructure space successfully partnered with the insurance industry to achieve its intended insurance coverage and make cyber program and organizational improvements to support the security leader's strategy. ***Scott Kannry**, Axio CEO*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

@SANSDefense **#SANSDataBreachSummit**

Tuesday, September 26

8:00-8:45 am	**Registration & Coffee** (LOCATION: BALLROOM PRE-FUNCTION)
9:00-9:45 am	***#RUR34DY: The State of Cyber Readiness*** ***Trent Teyema**, Chief of Cyber Readiness, FBI Cyber Division, Washington, DC*
9:45-10:30 am	***The Hitchhiker's Guide to Data Breaches*** The results are in: you've been breached. It's officially the worst day of your career. How will you handle what comes next? Are you prepared to navigate the long road to recovery? Where do you even begin? Come, hitch a ride with me, I'll show you the way via lessons learned from dozens of compromise recoveries across a variety of industries from around the world. Get real-world advice on evicting your adversary, answering to executives, and recovering from the trauma of a cyberattack, to help you better prepare for the inevitable breach. Turn your worst day around; just don't forget your towel! ***Josh M. Bryant** (@FixTheExchange), Cybersecurity Architect (Senior Consultant Cyber II), Microsoft Consulting Services*
10:30-10:50 am	**Networking Break** (LOCATION: BALLROOM PRE-FUNCTION)
10:50-11:45 am	***The Financial Services Industry Speaks: Key Risk Management and Chief Privacy Officer Perspectives*** Key perspectives from the front lines in the financial services industry share successes, challenges, and what's next on deck for them as they lead their organizations in the ongoing march toward balancing privacy, security, and the need to be customer-centric in transacting business daily on a national and global scale. From evaluating, revising and monitoring ongoing partner relationships with third-party vendors and service providers to navigating the landscape of minimum retention and document destruction best practices, to motivating employee populations to come forward when they suspect a security or privacy issue is at hand – these industry leaders in corporate privacy and risk management share real stories from the front lines involving cutting edge issues in today's evolving cyber threat landscape. MODERATOR: ***Kimberly B. Holmes**, Esq., RPLU, Senior Vice President & Counsel, Cyber Insurance, Liability & Emerging Risks, IDExperts* PANELISTS: ***Patrice Brusko**, SVP/US Chief Privacy Officer, TD Bank* ***Ethan Harrington**, Director - Insurance Risk Management, H&R Block*

Tuesday, September 26

11:45 am - 12:30 pm	***Now What? A Pragmatic Approach to Effective Breach Response for Leaders*** You read about it all the time, but now it's happening to you – the dreaded data breach. Fast forward to next Friday afternoon at 4:42pm. As a leader, your phone rings and your heart sinks as it is confirmed that you customer database has just been posted online for everyone to see. What intentional steps can a leader take in this moment to help ensure an effective breach response? ***Russell Eubanks*** *(@russelleubanks), VP & CISO, Federal Reserve Bank of Atlanta; Certified Instructor, SANS Institute*
12:30-1:30 pm	**Lunch & Discussion** ***Equifax: Get the Facts*** The most sensitive data of 140 million people has been comprised through the recent Equifax breach. That's bad; really bad. Should you panic? Lance Spitzner, the head of Security Awareness for SANS, will give you the real facts on the incident and what you can do to protect yourself, your family, and your organization. Spitzner also looks at the long-term ramifications on the Equifax incident on data security around the globe. ***Lance Spitzner*** *(@lspitzner), SANS Security Awareness*
1:30-2:05 pm	***Paying the Price: Selling Your CFO on Cybersecurity*** Cybersecurity insurance is an industry which, like technology, has matured over the past decade. Gone are the days of insurance companies not offering adequate coverage or paying for incidents. But that does not mean every insurance product is created equal. Just like any security control, insurance needs to be tailored to your environment and engineered for your organization. Learn from security practitioners who have applied insurance as a control and leverage those lessons learned for your own discussions with risk managers, brokers, and insurance companies. With real-world examples, attendees will hear about insurance covering forensics costs, data breach coaching, regulatory fines, and even how to make the case for more cybersecurity employees. A lot sure has changed since Y2K insurance. ***Scott Kannry****, CEO, Axio Global* ***John Mullen****, Partner, Mullen Coughlin*
2:05-2:40 pm	***Cyber Crises: Whether, When, and How to Engage the FBI*** When and how to engage law enforcement and the FBI when a breach occurs is the million dollar question. ASAC Todd Carroll will discuss engagement with the FBI in a crisis, and sustained engagement over time. He'll offer tips to prepare your organization for the inevitable Bad Day and outline the benefits of partnering with the FBI. You'll learn how to partner effectively with your legal department, the media, and the FBI to mitigate the business and reputational damage from a breach. ***Todd Carroll****, Assistant Special Agent in Charge – Chicago Field Office, FBI*

Tuesday, September 26

2:40-3:25 pm	***Managing Risk on a Global Scale*** For multinational organizations, managing cyber and privacy risks is becoming increasingly difficult in today's elevated threat environment. Regulatory pressures from evolving international privacy laws, well-funded attackers, and cybersecurity shortcomings are raising the stakes and consequences for every company when an event occurs. Both speakers represent international organizations and have advised clients on cyber risks and solutions located throughout the world. This in-depth session will cover: international privacy laws around Europe, North America, and Asia; the role of cyber insurance as more than financial risk transfer; cyber-loss case studies. ***James Burns**, Cyber Product Leader, CFC Underwriting (UK)* ***David Derigiotis**, Director, Professional Liability, Corporate Vice President, Burns & Wilcox*
3:25-3:45 pm	**Networking Break** (LOCATION: BALLROOM PRE-FUNCTION)
3:45-4:15 pm	***Stories from the War Room: Lessons in Breach Communications*** Data security incidents that are communicated poorly can quickly turn into reputational crises. Nearly three-quarters of consumers today say they'd switch brands after a company they rarely used suffer a data breach. Learn how to prepare and execute an effective communications strategy around a breach by examining real-world cases of organizations that got it right, and those that got it wrong. ***Jamie Singer**, Vice President, Edelman*
4:15-4:45 pm	***Breach Response in a Crazy World*** Suffering a breach is never easy. Response to a breach is likely to be one of the most stressful moments for any organization, and guaranteed to be a time of unwanted publicity and scrutiny. However, a breach does not necessarily mean that business is over. With the right mindset, breach response can morph into an opportunity for the organization to prevent future breaches. You can't change the past, but you can use it to make the business stronger. Through discussion of previous case studies, breach experience, and conference knowledge (yes, this presentation is dynamic!) we will examine ways to - and not to - respond to a breach. We will discuss handling a breach internally vs. externally, and how knowing your business is the best advantage you have in responding to a breach. Much more than just "handle the media," we'll also examine how to work with internal teams to make sure that information is being disseminated correctly. Lastly, we'll examine how to lay foundations to lessen the stress and reactionary time of a breach. Breaches are bad, but they are not the end! ***Matt Bromiley** (@mbromileyDFIR), Senior Managing Consultant, Kroll; Instructor, SANS Institute*
4:45-5:00 pm	***Closing Remarks*** ***Benjamin Wright** (@benjaminwright), Esq., Senior Instructor & Summit Co-Chair, SANS Institute*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.