Program Guide

@SANSInstitute #SANSBreachSummit

Agenda

All Summit Sessions will be held in the Astor Ballroom (unless noted).

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

Monday, August 20

7:00-8:30 am	**Registration & Coffee** (LOCATION: ASTOR FOYER)
8:30-8:45 am	***Welcome, Overview & Summit Roadmap*** ***Benjamin Wright****, Attorney in Private Practice; Senior Instructor, SANS Institute* ***Eric Zimmerman****, Senior Director, Kroll; Certified Instructor, SANS Institute*
8:45-9:30 am	***Keynote: Response to High-Profile Incidents*** A company often needs to minimize and control any immediate public comment on a data breach or security incident. But what if news of the incident hits the media outlets nearly immediately, requiring you to quickly develop public statements while simultaneously trying to figure out exactly what happened? Do you "spin" the story to protect the impacted organization or do you say "no comment" and leave everybody guessing, or do you do something else? This opening talk will look at a few recent high-profile incidents and how the impacted organizations responded when their incident became a lead news story. ***Marc Sachs****, CSO, Coventry Computer; Former CSO, North American Electric Reliability Corporation (NERC)*
	Investigation and Notification of Data Breaches: A Global Perspective Laws including the new General Data Protection Regulation (GDPR) require organizations to give notice of data breaches. This session will consider how those laws are interpreted and enforced in practice. It will consider procedures for authorities to discover details about how an organization investigated and evaluated a suspected breach and then decided whether notice was required. It will consider methods for maintaining confidentiality of investigations. The discussion will include the possibility for class actions, collective actions or other private lawsuits to enforce law related to data breaches. We'll examine the topic from three perspectives, with attorneys from continental Europe, the UK, and the US.
9:30-10:00 am	***Investigation and Notification of Data Breaches*** ***Alexander Blumrosen****, KAB Avocats Associés, France*
10:30-10:50 am	**Networking Break** (LOCATION: ASTOR FOYER)

Monday, August 20

10:50-11:10 am	***Investigation and Notification of Data Breaches: A U.S. Perspective*** ***Melinda L. McLellan**, Partner, BakerHostetler*
11:10 am – 12:10 pm	***Legal Investigation and Notification of Data Breaches: A Global Perspective*** After hearing each of the three perspectives on the topic, Ben Wright will lead an interactive panel discussion. MODERATOR: ***Benjamin Wright**, Attorney in Private Practice; Senior Instructor, SANS Institute* PANELISTS: ***Alexander Blumrosen**, Attorney, KAB Avocats Associés (France)* ***Melinda L. McLellan**, Partner, BakerHostetler* ***James A. Sherer**, Partner, BakerHostetler*
12:10-1:15 pm	***Lunch & Panel Discussion: Information Sharing: How ISACs Help with Incident Response*** Numerous industries have their own Information Sharing and Analysis Centers (ISACs). This panel of experts will share stories and opinions about best practices for drawing upon ISACs before, during, and after a cybersecurity incident. MODERATOR: ***Benjamin Wright** (@benjaminwright), Esq., Senior Instructor & Summit Co-Chair, SANS Institute* PANELISTS: ***Peter Falco**, Director of Broker-Dealer Services, FS-ISAC* ***Joshua Singletary**, CIO, NH-ISAC*
1:15-2:00 pm	***How Management Absorbs Information During a Cyber Event*** **The Analyst:** Here we go again. Another cyber event and the suits are interrupting the investigation and asking what IOC stands for. **The Leader:** Here we go again. Another cyber event and the techies are speaking Greek when I need information. Sound familiar? Of course it does; this isn't a unique scenario. Cyber events are fast-paced, high-stress scenarios where information is constantly evolving. Suddenly, the security team is in the limelight and being asked to provide technical information in business terms. Meanwhile, leadership is being pressured to provide answers to the Board, the customers, and the media. How can these two groups work together in this scenario to get leadership the necessary information without derailing the investigation? In this session, Sara Hall, the former CISO of the U.S. Department of Health and Human Services, will cover topics including: • Understanding perspectives from each side • What each side should be asking for • What each side should be prepared to provide • How to prepare before an actual cyber event ***Sara Hall**, Chief Operating Officer, NH-ISAC; Former CISO, U.S. Department of Health and Human Services*

Monday, August 20

2:00-3:00 pm	***Incident Response: From Basics to Best Practices*** Two seasoned incident responders will share case studies and hard-earned wisdom, and get you prepared to get hands on with a simulated incident. ***Lucie Hayward**, Managing Consultant, Investigations & Disputes, Kroll* ***Mike Quinn**, Director – Cyber Risk, Kroll*
3:00-3:10 pm	**Networking Break** (LOCATION: ASTOR FOYER)
3:10-5:30 pm	***Workshop: 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. ***Lucie Hayward**, Managing Consultant, Investigations & Disputes, Kroll* ***Mike Quinn**, Director – Cyber Risk, Kroll*
5:30-7:00 pm	**Networking Reception** (LOCATION: PROMENADE – 9TH FLOOR)

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.

Tuesday, August 21

8:00-9:00 am	**Registration & Coffee** (LOCATION: ASTOR FOYER)
9:00-9:45 am	***Keynote: Model-Driven Security: It's Closer Than You Think*** This session will offer an explanation of model-driven security, its implementations, and its implications. This model is not limited to large, sophisticated enterprises. You'll gain an understanding of why the growth of unconventional controls using models will continue. ***Jim Routh**, CISO, Aetna*
9:45-10:30 am	***Beauty & The Breaches: One Organization's Journey Towards a Culture of Confidentiality*** For the Henry Ford Health System, privacy and cybersecurity has been a journey of continuous quality improvement and team collaboration. As Henry Ford's Privacy and Security Team expanded its scope over the course of seven years, multiple incidents and response plans netted beautiful results. Join Meredith Harper for this engaging session that will review the beauty that can come out of each breach. Harper will share her perspective as a Chief Information Privacy and Security Officer, providing a window into how breaches have led to dramatic process improvements, and how people, processes, and technology were put into place to continuously develop a culture of confidentiality at the Henry Ford Health System. ***Meredith Harper**, Chief Information Privacy & Security Officer, Henry Ford Health System*
10:30-10:50 am	**Networking Break** (LOCATION: ASTOR FOYER)
10:50-11:45 am	***Getting Data Breach Right: Lessons Learned from Fighting in the Cyber Trenches*** The call comes in from the FBI. A customer. Your IT Director. You have a problem. Your data, your customers' data, has been exposed. For sale. Locked down. Two servers are impacted. No wait, it's forty-two... You've been breached. For years now, this story has been repeating itself in retail store chains, health care systems, fast food restaurants, and other enterprises. In response, enterprises have upped their game, investing billions of dollars to improve cyber defense towards becoming increasingly cyber resilient. But even the best-laid plans – the best IPS, the best end-point protection, the best employee anti-phishing training and awareness campaigns – aren't fool-proof. That's why it is so important to be prepared to get a data breach "right" if and when it happens to your organization. In this impactful session, John Ansbach will discuss the lessons Stroz Friedberg has learned over the years about how to get data breach response right, as a "first responder" in the US and globally. Through a discussion of real-world examples of fighting in the data breach trenches, John will reveal keys to a successful response while also highlighting some not-so-obvious not-to-do's and derailers to avoid. He'll also discuss the evolution of breach response and the ways in which companies are revising and innovating their approach to executing an effective response to cyber crises. This session is designed to be a focused discussion surrounding actionable insights and practical ideas for those tasked with managing and mitigating data breaches within their organizations. If you are trying to up your game and prepare for cyber crisis, you won't want to miss it. ***John Ansbach**, Vice President – Engagement Management, Stroz Friedberg, an Aon Company*

Tuesday, August 21

11:45 am-12:30 pm	***Crossing Borders: Managing a Security Incident Across Multiple Collaborating Organizations*** How often does a security incident or breach response cover four different organizations? It can and does happen in university environments, where multiple stakeholders are involved in sensitive research. When it does happen, there are not just local security and privacy officials to coordinate but also the urgent question of who is in charge of the response. This presentation will provide the story of a real incident, the bumps, twists and turns, and, after the smoke clears, the lessons learned, both from risk management and regulatory compliance perspectives. You'll leave with key guidance on how to address this risk through relationships between information security professionals in the various collaborating entities involved. ***Thomas Siu**, CISO, Case Western Reserve University*
12:30-1:30 pm	**Networking Lunch** (LOCATION: ASTOR BALLROOM)
1:30-2:05 pm	***Global DFIR in a Fractured World: Challenges in Managing International Incidents*** Despite decades of efforts to foster frictionless global trade and finance, the truly vital currency of our global economy – data – seems harder to move across borders than ever. While data protection and privacy laws have always varied from country to country, Edward Snowden's revelations about data collection and mining by government intelligence agencies along with rising alarm regarding how global technology juggernauts like Facebook and Google are using (or abusing) personal data has given us a more fractured set of rules to follow as DFIR practitioners. Failure to recognize and heed applicable laws and restrictions when planning and carrying out an incident response protocol can put you in the cross-hairs of a local regulator that may not take kindly to you moving data across borders – even if your purpose is purely benign. The kinds of issues that can catch even seasoned first-responders off guard include export controls that can apply to certain forensic tools and technology, challenges getting specialized equipment and personnel into or out of certain countries (hint: Pelican cases can attract unwelcome attention at the airport). In other situations, even when you try to do everything "by the book" and work in cooperation with local law enforcement, unexpected problems can arise (and in some cases, guns can even be drawn). This talk will use specific examples and rely on the speaker's experience with cross-border incident response and forensics to illuminate pitfalls and try to provide some best-practices guidance on how to respond with necessary urgency and confidence while still staying on the right side of the law. ***R. Jason Straight**, Senior Vice President, Cyber Risk Solutions, UnitedLex Corporation*
2:05-2:40 pm	***Don't Panic! Tales from the Front Lines*** In a time of crisis, the last thing you should do is overreact. To determine if there was an actual breach, you need a plan, clear thinkers, and decisive advisors. ***Mary N. Chaney**, Esq., CISSP; Former Director – Worldwide Information Security, Johnson & Johnson*

Tuesday, August 21

2:40-3:25 pm	***Talking to the Techs: Asking the Right Questions*** If (when) you suffer a breach, you'll need to respond appropriately, and immediately. But you'll also have to retrace your steps to root out the causes. Every contact leaves a trace, and digital forensics professionals can unearth artifacts to help determine causes, fix the vulnerabilities to mitigate additional damage, and provide evidence you'll need if further legal action becomes necessary. But how can you collaborate with the digital forensic examiners when you don't have a deep understanding of the technology? Summit co-chair Eric Zimmerman, instructor of SANS's FOR508: Advanced Digital Forensics, Incident Response and Threat Hunting course, author of X-Ways Forensics Practitioner's Guide, and a former Special Agent with the FBI, will break it down for you. Learn the lingo, familiarize yourself with the kinds of forensic artifacts you'll need in a breach situation, and hone the skill of asking for what you need in a way that enables your cybersecurity team to deliver. ***Eric Zimmerman**, Senior Director, Kroll; Certified Instructor, SANS Institute*
3:25-3:45 pm	**Networking Break** (LOCATION: ASTOR FOYER)
3:45-4:30 pm	***Developing the Human Sensor*** Far too often we discuss breaches only in terms of technology. And yet people are often one of the most powerful tools organizations have in detecting a breach. Learn how you can create a trained workforce to quickly identify and report an incident, improving your ability to both respond to and manage a breach. ***Lance Spitzner**, Director, SANS Security Awareness*
4:30-5:00 pm	***Summary Remarks*** ***Eric Zimmerman**, Senior Director, Kroll; Certified Instructor, 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.