We strive to present the most relevant, timely, and valuable content. As a result, this agenda is subject to change. Please check back frequently for changes and updates.

Monday, September 25	
8:30-8:45 am	*Welcome, Overview & Summit Roadmap* • **Matt Bromiley (@mbromileyDFIR), Senior Managing Consultant, Kroll; Instructor & Summit Co-Chair, SANS Institute** • **Benjamin Wright (@benjaminwright), Esq., Senior Instructor & Summit Co-Chair, SANS Institute**
8:45-9:30 am	*Keynote* **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. **Moderator: Benjamin Wright (@benjaminwright), Esq., Senior Instructor & Summit Co-Chair, SANS Institute** **SANS Institute** **Panelists:** • **Rick Kam, President/Co-Founder, ID Experts** • **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 & Vendor Expo**

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-Noon	**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**
Noon- 1:00 pm	**Lunch**
1:00-1:35 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**
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 & Vendor Expo**
2:30-2:50 pm	**Overview of Afternoon Exercise**
2:50-4:15 pm	**Exercise**
4:15-4:45 pm	**Group Presentations: Pulling the Lessons All Together** The plenary conference will reconvene for open discussion. Discussion groups will share lessons with all attendees. The goal is to improve practices in investigations, communications and compliance with law.
4:45-5:00 pm	**Summary/Closing Remarks**

Tuesday, September 26	
9:00-9:45 am	*Keynote* **Cyber-Readiness and the FBI** • **Scott Smith, Assistant Director – Cyber Division, Federal Bureau of Investigation** • **Trent Teyma, Section Chief, Cyber Readiness Section, Federal Bureau of Investigation**
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 & Vendor Expo**
10:50-11:45	**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 3rd 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. • **Kimberly B. Holmes, Esq., RPLU, Senior Vice President & Counsel, Cyber Insurance, Liability & Emerging Risks, IDExperts** • **Patrice Brusko, SVP/US Chief Privacy Officer, TD Bank** • **Ethan Harrington, Director - Insurance Risk Management, H&R Block**

11:45 am-12:15 pm	**Cyber Crises: Whether, When, and How to Engage the FBI** *Session description to come* **Todd Carroll, Assistant Special Agent in Charge – Chicago Field Office, FBI**
12:15-1:30 pm	**Lunch**
1:30-2:05 pm	**Paying the Price: Selling Your CFO on Cybersecurity** Cyber security 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… **Jason Christopher, CTO, Axio** *Additional speaker to be named*
2:05-2:40 pm	**Maintaining Confidentiality During an Investigation** *Session description to come* **Kristine Green, Chief Division Counsel, FBI Atlanta**
2:40-3:25 pm	**Managing Risk on a Global Scale** *Session description to come* • **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 & Vendor Expo**
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	*Session description to come* **Matt Bromiley (@mbromileyDFIR), Senior Managing Consultant, Kroll; Instructor, SANS Institute**
4:45-5:00 pm	*Closing Remarks* **Benjamin Wright (@benjaminwright), Esq., Senior Instructor & Summit Chair, SANS Institute**

Speaker Biographies

Matt Bromiley (@mbromileyDFIR), Senior Managing Consultant, Kroll; Instructor & Summit Co-Chair, SANS Institute

Matt Bromiley is a Senior Managing Consultant at Kroll, a major incident response and forensic analysis firm where he assists clients with incident response, digital forensics, and litigation support. He also serves as a SANS GIAC Advisory Board member, a subject-matter expert for the SANS Securing The Human Program, and a technical writer for the SANS Analyst Program. Matt brings his passion for digital forensics to the classroom as a SANS instructor for FOR508: Digital Forensics, Incident Response, and Threat Hunting, where he focuses on providing students with implementable tools and concepts. Matt fell into this career somewhat by accident, taking on a junior analyst role because the team was great and the work sounded exciting. Since then, Matt has built a wide-ranging career that gives him a broad perspective on digital forensics. He has helped organizations of all types and sizes, from multinational conglomerates to small, regional companies. His skills run the gamut from disk, database and network forensics to malware analysis and classification, incident response/triage and threat intelligence, memory analysis, log analytics, and network security monitoring. Along with traditional database forensics, Matt has experience deploying such tools as Elasticsearch, Splunk, and Hadoop to assist in large-scale forensic investigations, network security monitoring, and rapid forensic analysis on over 100 systems and over 10TB of logs. He has a particular interest in database and Linux forensics, as well as in building scalable analysis tools using free and open-source software. Outside of work, Matt loves spending time with his family, cooking Texas BBQ, and making his house as automated as possible in hopes that it will one day do work for him.

Patrice Brusko, SVP/US Chief Privacy Officer, TD Bank

Patrice Brusko joined TD in 2011 and has been the US Chief Privacy Officer heading the US Privacy Office since September 2015. In this capacity, Patrice leads the US Privacy program including all activities related to the development, implementation, and adherence to the company's policies and procedures, federal and state laws, and industry best practices. Providing oversight to the overall program effectiveness, she manages a team of privacy professionals and serves as a liaison to regulatory bodies for matters relating to privacy.

Prior to this role, Patrice was a Senior Privacy Relationship Manager with the TD's US Privacy Office, covering the credit card businesses including acquisition due diligence. Patrice has also worked in various Financial Services marketing roles, both in-house and on the vendor side. She has lead in new product and channel development, and innovative uses of data.

Patrice maintains the Certified Information Privacy Professional (CIPP) designation, Certified Information Privacy Technologist (CIPT) designation, is a graduate of the ABA School of Bank Marketing and Management, and holds a degree in Political Science and Secondary Education from Gettysburg College.

Josh Bryant (@FixTheExchange), Cybersecurity Architect, Microsoft

Josh Bryant is a Cybersecurity Architect (Senior Consultant Cyber II) at Microsoft where he is currently focused on delivering Cybersecurity services ranging from Tactical and Strategic Recovery to Advanced Threat Analytics implementations, Risk Assessments, and more, to customers in a variety of industries around the world.

James Burns, Cyber Product Leader, CFC Underwriting Ltd. (UK)
James has nearly ten years' experience in the London Insurance Market, the last five of which have been spent focused on cyber, building up expertise and insight in this dynamic area. As Cyber Product Leader, James is responsible for ensuring that CFC's global suite of cyber products remain at the cutting edge of a class where threats continue to rapidly evolve. James travels extensively throughout the UK and North America to give presentations and speak at various events, from educational seminars to panel discussions and industry trade shows.

R. Matthew Chevraux, Assistant Special Agent in Charge, U.S. Secret Service, Office of Investigations, Cyber Strategy and Outreach
R. Matthew Chevraux is the Assistant Special Agent in Charge of the Cyber Strategy and Outreach Section within the Office of Investigations. His work in this assignment is to enhance the public/private partnerships within the Service's network of Electronic Crimes Task Forces, information sharing initiatives, and by regularly respresenting the USSS' cyber interests at both governmental working groups and private industry events. He has been an agent with the United States Secret Service for over 18 years; previous assignments include in the Los Angeles Field Office, the Presidential Protective Division, the Criminal Investigative Division at Secret Service Headquarters, and at the Department of Homeland Security's National Cybersecurity and Communication Integration Center (NCCIC), the Federal Government's 24/7 cyber and communication situational awareness, incident response and management center. During ASAIC Chevraux's career with the Secret Service, he has investigated counterfeit, financial, and cyber crimes, been a computer forensics examiner, and his presidential protective assignment was with both President George.W. Bush and President Barack Obama. Matt holds a bachelor's degree in business administrative studies from the University of California, Riverside.

Jason Christopher, CTO, Axio
Jason Christopher is Axio's Chief Technology Officer. His responsibilities include providing leadership on security issues relevant to Axio, its partners, and clients. Jason previously led cybersecurity research efforts across private sector and the federal government. He has worked in several critical infrastructure sectors, including power, energy, communications, and water.

David Derigiotis, Director, Professional Liability, Corporate Vice President, Burns & Wilcox
David Derigiotis is corporate Vice President and Director of Cyber & Professional lines with international wholesale insurance broker Burns & Wilcox. David has participated in cyber discussions with US Treasury Department in Washington D.C. and has appeared on networks such as Fox Business and CNBC discussing cyber risks and coverage solutions.

Kristine Green, Chief Division Counsel, FBI Atlanta
Kristine Green has been a Special Agent attorney with the FBI for over 20 years. She has served as the Chief Division Counsel in Atlanta since 2014, and as the Chief Division Counsel in New Orleans from 2010-2014. She served as the Associate Division Counsel in New Orleans from 2009-2010. From 2006-2010, she was the Cyber Supervisory Special Agent and Cyber Program Coordinator overseeing National Security and Criminal Computer Intrusions, Child Exploitation, Theft of Intellectual Property and Internet Fraud violations. From 2000-2006, she was an agent assigned to Counterterrorism and Counterintelligence Cyber matters, and worked public corruption from 1996-2000.

Meredith Harper, Chief Information Privacy & Security Officer, Henry Ford Health System
Meredith joined Henry Ford Health System in 2003 as their first Chief Privacy Officer after completing a consulting engagement with Health Alliance Plan where she served as a HIPAA Project Manager beginning in late 2002. Over her 23 year career, she has emerged as a strategic leader who is not just interested in processes, goals and objectives but most of all she is passionate about her greatest assets…her human capital. Her success has been attributed to

her ability to manage large-scale complex projects that cross-functional areas within integrated delivery systems and health plans while advancing the skill sets of her team members.
As the industry has evolved, so has her areas of responsibilities and in 2012 her role was expanded to include leadership responsibilities for Information & Network Security, Privacy & Security Risk Management as well as Identity & Access Management. As Chief Information Privacy & Security Officer, she has responsibility for the protection of Henry Ford's provider, insurance, retail and research businesses. Her sensitivity to the operational needs of these various businesses helps her guide the objectives of her team to ensure that the operations are successfully married with the technology or regulatory requirements.
Meredith is an active member of the Health Care Compliance Association and the International Association of Privacy Professionals since 2004 where she has demonstrated her commitment to compliance by holding dual certifications in healthcare compliance and privacy. She is also certified as a HealthCare Information Security & Privacy Practitioner through the International Information System Security Certification Consortium, Inc.
Meredith is a member of HIMSS, Inforum, the PHI Protection Network, the Michigan Council of Women in Technology, Information Technology Senior Management Forum, Association for Executives in Healthcare Information Security, America's Health Insurance Plans, InfraGard and the Information Systems Audit and Control Association. She serves as a Governing Body Co-Chair for the Detroit CISO Executive Summit, the Chair of the Michigan Healthcare Cybersecurity Council and the President of the Medical ID Fraud Alliance.
Meredith is passionate about empowering women and minorities to embark upon careers in technology especially in information security where those populations are not very well represented. She serves on several advisory boards, one being Step IT Up America, in support of that passion and she has a unique perspective she enjoys sharing with others.
Meredith is a proud alumna of the University of Detroit Mercy where she received her Master's in Health Services Administration and her Bachelor of Science in Computer Information Systems. She is an avid supporter of her alma mater's mission and serves on the advisory boards for the Center for Cyber Security & Intelligence Studies and the Health Information Management program.

Rick Kam, President/Co-Founder, ID Experts
Rick Kam, CIPP/US, is president and co-founder of ID Experts. ID Experts delivers data breach response services, manages cyber risks, and is trusted by thousands of organizations. ID Experts is the largest provider of identity protection products to the federal government. Rick has extensive experience leading organizations in the development of policies and solutions to address the growing problem of protecting protected health information (PHI) and personally identifiable information (PII), and remediating privacy and security incidents, identity theft, and medical identity theft. Rick leads and participates in several cross-industry data privacy groups, including PHI Protection Network (PPN) and Medical Identity Fraud Alliance.

Renato Marinho, MSc, Morphus Labs (Brazil)
Renato Marinho is Director of Research at Morphus Labs. His journey in the area began in 2001, when he created Nettion, one of the first firewalls to use the contemporary UTM (Unified Threat Management) concept.
Experienced in cyber security, Marinho was internationally recognized in 2016 by his research that unveiled Mamba, the first full disk encryption ransomware. At Morphus Labs, he oversees research, innovation and development of new products. Master and Doctorate in Applied Informatics, he is also professor at University of Fortaleza teaching Computer Forensics in the post-graduate course. He is also a speaker having presented at BSides Delaware, BSides Vienna, WSKS Portugal and Brazilian CSIRTs Forum.
Certified ISC2 CISSP and ISACA CRISC professional, his research interests include malware and new threats analysis, OSINT, Honeypot, machine learning and automation of IR cycle.

Jamie Singer, Vice President, Edelman
A senior account supervisor with Edelman's Corporate Reputation & Risk Management practice, Jamie Singer provides issue management, crisis preparedness and crisis communications counsel to clients across an array of industries, including food & beverage, health care and higher education. She provides strategic counsel and support to companies and non-profit organizations facing reputational risks such as data security & privacy

vulnerabilities, product quality issues, and human safety and health concerns. Jamie's expertise includes leading risk and vulnerability assessments, crisis plan and playbook development, as well as crisis trainings and simulations. As part of Edelman's Data Security & Privacy Team, Jamie has led breach response efforts for one of the largest insurers in the U.S. as well as other companies in the health care, retail, higher education and technology industries. She also works with clients to enhance their data security & privacy crisis preparedness through plan and process development.

Prior to joining Edelman, Jamie served as the Assistant Director of Internal Communications at the Kellogg School of Management at Northwestern University. At Kellogg, Jamie led development and execution of the school's internal communications program as well as the school's crisis communications planning efforts. Prior to Kellogg, Jamie worked in Cone Communications' Crisis Prevention and Management Group. At Cone, she supported risk analysis and mitigation, communications strategy, message and materials development, as well as media relations for clients including Nestle Waters North America, Green Mountain Coffee Roasters and General Mills. Prior to Cone, Jamie worked at FTI Consulting, performing crisis and issues management work for clients in industries ranging from entertainment/gaming to health care IT to professional services. Jamie has authored several published bylines on crisis and reputation management topics, including for *NCAA Champion Magazine* and *The Detroit News*. EDUCATION: University of Michigan, BA, graduated Phi Beta Kappa and with Highest Distinction.

Melissa Ventrone, CIPP/US, Thompson Coburn LLP

When a cybersecurity incident strikes, affected parties need a swift and strong response to manage their situation and minimize damage. As chair of Thompson Coburn's cybersecurity practice, Melissa Ventrone leads teams of first responders, including lawyers and forensic investigators, in jumping head-on into a crisis. Melissa and her team work around the clock to control a breach situation and manage
any public or regulatory fallout. When not in urgent response mode, Melissa represents her clients in cybersecurity litigation and proactively managing data privacy and security risks.

Melissa has led cybersecurity incident response teams in connection with small breaches impacting a few hundred people to larger breaches impacting millions on behalf of merchants, financial institutions, medical providers and educational institutions. Melissa and her team work with clients to preserve evidence, determine a breach's scope, document the response and craft communications that both
meet legal requirements and protect a company's brand. She also advises on establishing incident call centers and staff training, in addition to formulating other methods to protect impacted individuals from potentially negative outcomes.

Melissa has attained considerable success in defending companies facing data security and privacy litigation, including class actions. She represents numerous clients in litigation and arbitration, including disputes related to privacy, invasion of privacy, contracts, consumer fraud, statutory claims and other matters. She has litigated cases of first impression establishing favorable law, including
obtaining summary judgment in a class action case alleging damages from the theft of a hard drive.

Melissa advises clients on compliance with state, federal and international laws and regulations.

Education: Chicago-Kent College of Law-J.D. (2003); Northern Illinois University-B.S. (2000)

Benjamin Wright (@benjaminwright), Esq., Senior Instructor & Summit Co-Chair, SANS Institute

Benjamin Wright is a practicing attorney based in Dallas, Texas, focusing on technology law. He serves as a senior instructor at the SANS Institute, teaching its 5-day course titled 'Law of Data Security and Investigations.' Through that course Mr. Wright has taught thousands of students from throughout the world. He chairs SANS Institute's annual Data Breach Summit. Mr. Wright advises diverse clients, both in the US and outside the US, on privacy, electronic commerce and data security law.