



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.

No CLE	8:30-8:50 am	<p><i>Welcome, Overview &amp; Summit Roadmap</i></p> <p>Every day, the modern enterprises encounters security events that must be investigated. For a few of those events, full investigation finally reveals that the enterprise has suffered a data breach that entails legal and public obligations. Although experts like lawyers and investigators will have opinions, it ultimately falls to management to made decisions on the investigation and the response, including tradeoffs between legal confidentiality and public communication. This Summit aims to improve the wisdom available to management in its decision-making process.</p> <p><b>Benjamin Wright, Esq., Senior Instructor/Summit Chair, SANS Institute</b></p>
No CLE	8:50-9:25 am	<p><b>Two Truths and a Lie about Data Breaches</b></p> <p>Are <i>you</i> adequately prepared to handle a data breach crisis? Jeff will discuss the latest trends in enterprise data breaches and present a model for assessing your organizational readiness for a potential breach. Included in the presentation will be current spending patterns to address security (including insurance and breach preparedness) and a checklist of best practices for reacting to and communicating about a breach.</p> <p><b>Jeffrey Louie, Retired Director of Global Informatics Services, Agilent Technologies</b></p>
MO Yes IL/CA Maybe  25 minutes	9:25-10:00 am	<p><b>Incidents and Breaches: The Executive Management Decision-Making Process</b></p> <p>A large university system possesses many different types of sensitive data, including patient records, student records and financial data. It faces many legal and political expectations for securing data and communicating to the public if security is compromised. Mr. Segran will outline the challenges management faces as it evaluates input from experts about a possible compromise. He will share lessons learned in his experience as both a university CIO and a leader in state government cybersecurity.</p> <p><b>Sam Segran, CIO, Texas Tech University</b></p>

	10:00-10:20 am	<b>Networking Break &amp; Vendor Expo</b>
No CLE	10:20-10:45 am	<p><b>To Call or Not to Call?: Implications and Obligations of Involving the FBI</b>  As an enterprise discovers it has experienced a serious security incident, it must evaluate with legal counsel whether and how to contact law enforcement agencies such as the Federal Bureau of Investigation. Mr. Leatherman will address what it means in practice for the FBI to engage in a cyber security investigation at an enterprise such as a private corporation. Topics may include confidentiality of the investigation, process for cooperation between the enterprise and the Bureau, and what influence the enterprise may have over the direction and scope of the Bureau's investigation.</p> <p><b>Brett Leatherman, Section Chief – Cyber Outreach Section, Federal Bureau of Investigation (FBI)</b></p>
Yes 20 mins	10:45-11:05 am	<p><b>Legal Responsibilities for a Data Breach</b>  <i>Abstract to come</i></p> <p><b>Melissa Ventrone, Partner; Chair - Data Privacy &amp; Security Practice Group, Thompson Coburn</b></p>
No CLE	11:05am - Noon	<p><b>How to Determine the Significance of a Security Incident</b>  Security incidents are common. But only a few of them constitute “data breaches” or other significant compromises of security. These panel members will share the wisdom they have gained by evaluating incidents in healthcare and other industries.</p> <p>Moderator: <b>Benjamin Wright, Esq., Senior Instructor/Summit Chair, SANS Institute</b></p> <p><b>Panelists:</b></p> <ul style="list-style-type: none"> <li>• <b>Rick Kam, President/Co-Founder, ID Experts</b></li> <li>• <b>Meredith Phillips, Chief Information Privacy &amp; Security Officer, Henry Ford Health System</b></li> <li>• <b>Erika Riethmiller, Director, Corporate Privacy-Incident Program, Anthem, Inc.</b></li> </ul>
	Noon-1:15 pm	<b>Networking Luncheon</b>
No CLE	1:15-1:50 pm	<p><b>Breach Detectives: Gathering and Assessing Evidence of Incidents and Breaches</b>  Digital evidence can be tricky and subject to conflicting interpretations. The evidence of a possible breach can come from many sources, including third parties such as vendors or customers. This panel will examine how</p>

		<p>to find, preserve and understand the evidence.</p> <p><b>Moderator: Benjamin Wright, Esq., Senior Instructor/Summit Chair, SANS Institute</b></p> <p><b>Panelists:</b></p> <ul style="list-style-type: none"> <li>• <b>John Mohr, CSO, MacArthur Foundation</b></li> <li>• <b>Jake Olcott, VP, BitSight</b></li> <li>• <b>Hal Pomeranz, Fellow, SANS Institute</b></li> </ul>
<u>No CLE</u>	1:50-2:15 pm	<p><b>Relationship Management: Effectively Partnering with Your Cyber Insurer</b></p> <p><i>Session abstract to come</i></p> <p><b>David Hallstrom, Practice Leader - Information Risk, CNA</b></p>
<u>No CLE</u>	2:15-2:40 pm	<p><b>Real Breach Stories from the Trenches</b></p> <p>We often read or hear about data breaches in various news outlets, but by the time the general public learns of the incident, it is third- or fourth-hand news. In this panel discussion, listen first-hand to real-life incidents in varying verticals handled by front-line experts in forensics, public relations and remediation who assist breached entities every day.</p> <ul style="list-style-type: none"> <li>• <b>Rich Blumberg, Director, Data Breach Response, IDT911</b></li> <li>• <b>Ondrej Krehel, Digital Forensics Lead, CEO and Founder, LIFARS LLC</b></li> <li>• <b>Melanie Thomas, CEO, Inform LLC</b></li> </ul>
	2:40-3:00 pm	<b>Networking Break &amp; Vendor Expo</b>
<u>MO – Yes</u>  <u>IL/CA Maybe</u>  <u>20 mins</u>	3:00-3:20 pm	<p><b>Overview of Afternoon Exercise</b></p> <p>Learning comes from doing. The attendees will break into small discussion groups. Each group will be assigned a fact scenario and asked to develop a plan of action. The exercise will emphasize collaboration among experts such as CISOs, lawyers and risk managers. Speakers from earlier in the day will participate.</p> <p><b>Benjamin Wright, Esq., Senior Instructor/Summit Chair, SANS Institute</b>  <b>John Wurzler, President, OneBeacon Technology Insurance</b></p>
<u>MO – Yes</u>  <u>IL/CA Maybe</u>  <u>70 mins</u>	3:20-4:30 pm	<p><b>Ready...Set...Respond: Workshopping the Inevitable</b></p> <p>Attendees will work through a hypothetical but realistic breach scenario in small groups. Each scenario will raise legal, investigative, management and communications issues.</p>

<u>MO – Yes</u> <u>IL/CA Maybe</u> <u>30 mins</u>	4:30-5:00 pm	<p><b>Group Presentations: Pulling the Lessons All Together</b></p> <p>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.</p>
<u>MO Yes</u> <u>IL/CA Maybe</u> <u>15 mins</u>	5:00-5:15 pm	<p><b>Summary/Closing Remarks</b></p>