

SANS

FOR CISOs  
OF TODAY AND  
TOMORROW



SECURITY  
LEADERSHIP

SUMMIT 2016

**Program Guide**

@secleadership



#SANSSecLeadership

Welcome to the Security Leadership Summit! As we come together as a community to discuss and share ideas all things security leadership, your participation is what makes our Summit the most comprehensive event of its kind. Over the next two days, you'll participate in discussions and hear from prominent information security leaders addressing key issues and challenges. Our goal is for you to take this information and use it to better protect your organization.



Frank Kim

Please take this opportunity to introduce yourself to those sitting around you, join one of the many conversations during breaks, and engage with our expert speakers during our networking events.

Attendees tell us time and time again that the greatest value of our Summit is the interaction with others and the newly forged connections they make during their time with us.

Looking forward to an amazing two days!

Frank Kim  
CISO, SANS



# Agenda

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

All approved presentations will be available online following the Summit at

<https://files.sans.org/securityleadership2016>

An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Tuesday, September 27	
8:00-8:45am	<b>Registration &amp; Coffee</b> (LOCATION: BLUEBONNET LOBBY)
8:45-9:00am	<b>Welcome &amp; Opening Remarks</b> <i>Kathy Fithen</i> , Chief Privacy Officer, The Coca-Cola Company; Summit Co-Chair <i>Frank Kim</i> , CISO, SANS Institute; Summit Co-Chair
9:00-9:45am	<b>Security to Privacy: How Did I Get Here?</b> As a chief privacy officer for a multinational beverage giant, Kathy must help Coca-Cola make good decisions on aligning with privacy laws around the world, while enabling the business. This role calls upon her background in business management, personnel management, information security, and privacy to help craft an effective privacy program. Kathy will enumerate how each role she held earlier in her career plays into her daily operations as well as long-term strategic planning. She'll also share lessons learned (some good, some bad) along the way to developing an effective privacy program. <i>Kathy Fithen</i> , Chief Privacy Officer, The Coca-Cola Company
9:45-10:30am	<b>How to Measure Anything in Cybersecurity</b> Security leaders must master analytics skills to compete in a data-defined world. We will cover research from <i>How to Measure Anything in Cybersecurity Risk</i> (Wiley 2016). Our thesis is that we compete with the "bad guys" on analytics. Security talent and technology are parameters to a larger, more strategic, decision-making model. <i>Rich Seiersen</i> , Former General Manager – Cyber Security & Privacy, GE Healthcare
10:30-11:00am	<b>Networking Break</b> (LOCATION: BLUEBONNET LOBBY)
11:00-11:45am	<b>So You Have Just Been Asked To Brief the Board of Directors on Cybersecurity</b> Situation: Your boss emails you to say that the Board of Directors is meeting next week and cybersecurity is on the agenda. The CEO wants you to brief the board. A big opportunity? Perhaps. A high risk moment? Most certainly. In this very practical briefing, Alan will share the results of five months of research on the most interesting and appropriate-for-the-audience techniques IT security managers have used in high-level gatherings and the most damaging errors that they continue to make. <i>Alan Paller</i> , Director of Research, SANS Institute



## Tuesday, September 27

11:45am-12:30pm

### **Cloud Security: Real-World Recommendations and Decision Making**

Is your organization obsessed with security risks around cloud solutions that are unsubstantiated? Navigating the array of decisions around cloud initiatives can be difficult, having a clear plan to address governance, regulatory compliance, monitoring and other barriers is crucial to making progress. Keys to discussing, security controls and obtaining both alignment and consensus among peers, as well as insight into varying risks and how to deal with them will be covered in this session for both private and public cloud. Matt Fearin, SVP CISO, Epsilon and Scott Savage, Enterprise Security Architecture, Capital One will share real-world experience and insights on traversing the path to cloud security decisions.

**Matt Fearin**, CISO, Epsilon / Conversant

**Scott Savage**, Enterprise Security Architect, Capital One

12:30-1:45pm

### **Networking Lunch** (LOCATION: ELM ROOM – 2ND FLOOR)

1:45-2:45pm

### **Talent Representation: Building a Diverse Cybersecurity Team**

We can't talk about the dearth of qualified information security professionals without acknowledging that large segments of the population are vastly underrepresented in the industry. How can we work to build a more diverse workforce, including tapping into talented individuals from non-traditional career paths? What are the barriers to entry and advancement for female cybersecurity professionals and for people of color (of both genders)? What shifts in the organizational culture can create a more inclusive environment where diverse voices can contribute to the overall strength of the team? What do you want in a candidate, but also, what do candidates expect from employers? This panel promises a lively debate on this important topic.

**MODERATOR:** **Kathy Fithen**, Chief Privacy Officer, Coca-Cola

**PANELISTS:** **Kim L. Jones** CISM, CISSP, M.Sc., Director, Cybersecurity Education Consortium, Arizona State University

**Maureen Kaplan**, CISSP, GSLC, Executive Vice President, Business Development, Veris Group, LLC

**Juliet Okafor**, Strategic Advisory Board Member, International Consortium of Minority Cybersecurity Professionals; VP – Global Business Development, Fortress Information Security

2:45-3:30pm

### **Building a Successful Security Program**

What does a successful security program look like? There is no one-size-fits-all or magical formula, but there are some common themes to every successful program. Learn what one security leader has focused on while leading a large program over several years. There are five areas that will help define your program as a brand differentiator and business enabler. Back by popular demand as one of last year's highest-rated speakers, Gary will share his latest thoughts and experiences on what defines success in cybersecurity.

**Gary McAlum**, CISO, USAA

3:30-3:50pm

### **Networking Break** (LOCATION: BLUEBONNET LOBBY)



Tuesday, September 27

3:50-5:00pm

### **SANS Ones to Watch in Cybersecurity Awards**

We've searched far and wide to identify emerging cybersecurity leaders who:

- Show leadership and an ability to drive key elements of the security program.
- Institute and manage change within the organization.
- Understand and be able to articulate business drivers for information security.
- Develop process and technological improvements leading to new security innovations.
- Display an ability to lead, motivate, and inspire others.

Join us in getting to know the recipients of our first annual Ones to Watch in Cybersecurity Awards. You'll want to keep an eye on their careers.

**Cathy Click**, *Project/Process Manager, FedEx*

**Sandra Crosswell**, *Senior Manager, Security Red Team, VMware IT Security*

**Khash Kiani**, *Executive Director - Application and Product Security Trust and Assurance at Hewlett-Packard Enterprise*

6:00-8:00pm

### **Networking Reception**

Please join Summit speakers and your fellow attendees for an evening of networking at Union Park, 1311 Main Street. Be sure to wear or bring your Summit badge. Drinks and snacks will be served.

**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.*

@secleadership



#SANSsecLeadership

## Wednesday, September 28

8:00-9:00am	<b>Registration &amp; Coffee</b> (LOCATION: BLUEBONNET LOBBY)
9:00-9:45am	<b><i>10 Tenets of Security Success</i></b> <p>The era of CISO-as-dictator is at an end. The increased importance of cybersecurity as a vital component of business growth requires security leaders to find new ways to work with executive leaders, business partners, and their own team members. Learn 10 tenets that CISOs and security leaders can utilize to go beyond technical skills, successfully lead organizations through change, and ultimately get to “yes” with the business.</p> <p><b>Frank Kim</b>, CISO, SANS Institute; Summit Co-Chair</p>
9:45-10:30am	<b><i>The Three Ts of Cybersecurity: Talent, Technique and Tools</i></b> <p>Jim Routh will share his perspective on what's required for success in cybersecurity leadership given the evolving cyber threat landscape using specific examples of technology innovation and leadership techniques that his team has implemented successfully. Jim will share practical examples of methods and tools to change the ground rules for threat adversaries making it more difficult for threat actors to achieve success and ultimately improve enterprise resilience.</p> <p><b>Jim Routh</b>, CSO, Aetna</p>
10:30-11:00am	<b>Networking Break</b> (LOCATION: BLUEBONNET LOBBY)
11:00-11:45am	<b><i>Zen and the Art of Transformational Security</i></b> <p>Every security leader is a change agent. Whether making minor adjustments to well-established programs, responding to new regulations, or lifting and improving struggling programs, security leaders are constantly injecting transformation into the organizations they support. Unfortunately, the same technical skills and expertise we bring to our security roles does not necessarily prepare us for leading organizations through change. In this presentation, Kim L. Jones will share his insights and experiences on the skills and techniques necessary to successfully navigate an organization through security transformation.</p> <p><b>Kim L. Jones</b> CISM, CISSP, M.Sc., Director, Cybersecurity Education Consortium, Arizona State University</p>



Wednesday, September 28

11:45am-12:30pm

### ***Crisis Communications for Incident Response: Five Keys to Getting it Right***

One of the parts of intrusion response that rarely gets attention in security circles – though huge attention outside them – is the victim companies' communication to their own customers. This is almost always the only real information the public gets about an intrusion, and communicating what happened effectively is crucial to minimizing damage, both to customers and to an organization's reputation.

Using lessons pulled from professional public relations specialists, combined with practical experience in operations and security incident response, we'll review the five keys to good crisis communications. We'll walk through multiple examples of good and bad crisis communications, and develop an understanding of what information people need when and why they should get it from you, not the media. We'll also discuss building a comprehensive incident communications plan.

**Scott Roberts**, *Bad Guy Catcher, GitHub*

12:30-1:45pm

### **Lunch & Learn** (LOCATION: BLUEBONNET A)

Presented by



1:45-2:30pm

### ***When Disaster Strikes: Managing Legal Risk in a Data Breach***

Let's be realistic: it's not whether your organization will suffer a data breach; it's when, and how bad the damage will be. The moment you become aware of a breach, you'll have to spring into action to notify affected customers. Right? Not so fast. In some cases, an in-depth analysis of the probability of significant harm can be more responsible than automatic notification. Furthermore, your legal adversaries, like regulators and plaintiff lawyers, will want access to the reports prepared by your incident response team. Are there ways to keep those reports confidential? Ben Wright helps you make sense of recent events and case law to help you prepare for the inevitable.

**Benjamin Wright**, *Esq., Senior Instructor, SANS Institute*

2:30-2:45pm

### **Networking Break** (LOCATION: BLUEBONNET LOBBY)

@secleadership



#SANSSecLeadership

Wednesday, September 28

2:45-3:30pm	<p><b><i>Managing M&amp;A Risks Whilst Building a World-Class Security Organization</i></b></p> <p>High-profile mergers and acquisitions present an excellent opportunity for hackers to take advantage of enormous organizational churn. Alan Daines, Dell's CISO, will talk about managing this risk as part of the biggest technology merger in history, how Dell went about rebuilding their cybersecurity program, and the benefits of a changing reporting structure to create a world-class cybersecurity organization.</p> <p><b><i>Alan Daines</i></b>, Chief Information Security Officer, Dell</p>
3:30-4:15pm	<p><b><i>Security Leadership For Everyone: Personal Authority and Beyond</i></b></p> <p>Leaders have followers because they have some sort of "authority." They may have positional authority because they are in charge, because of their position or title. They may have personal authority, which is earned through actions. Many leaders have both. In this talk, we look at leadership and authority, discussing both types of authority and concentrating on what it takes to establish personal authority in security. Security leadership is not reserved for those in charge. Personal authority can be earned by all of us, and ideally those with positional authority also have personal authority.</p> <p><b><i>Ted Demopoulos</i></b>, Certified Instructor, SANS Institute</p>
4:15-4:30pm	<p><b><i>Closing Remarks</i></b></p> <p><b><i>Kathy Fithen</i></b>, Chief Privacy Officer, The Coca-Cola Company; Summit Co-Chair <b><i>Frank Kim</i></b>, CISO, SANS Institute; Summit Co-Chair</p>

**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.*

@secleadership



#SANSsecLeadership