Dallas, TX
September 10

SECURITY AWARENESS
Summit 2014

Chairman: Lance Spitzner

AGENDA

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

All approved presentations will be available online following the Summit at https://files.sans.org/secaware14.
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Tuesday, September 9

6:30-8:00 pm — **Early Registration | Pre-Summit Meet & Greet** *(Location: Addison Grill)*

Join us for this optional opportunity to meet and network with your fellow attendees before the Summit kicks off. Gather at the Addison Grill in the Marriott lobby.

Wednesday, September 10

7:30-8:45 am — **Registration & Coffee** *(Location: Vista Ballroom)*

8:45-9:00 am

Welcome & Opening Remarks

***Lance Spitzner**, Training Director, SANS Securing The Human Program*

9:00-9:45 am

Ramping Up Your Phishing Program

Many organizations have recently started phishing programs as part of their overall awareness program. At Lockheed Martin we've been running intensive phishing assessments for 5+ years utilizing a rigorous, repeatable methodology. In addition to greatly reducing the risk associated of employees taking a "bad" action with suspicious e-mails we have identified numerous lessons learned on how to effectively use phishing to manage cyber security risk presented by human behavior. Examples include: how to structure a good phishing email, how to build a progressive and diverse training program, addressing chronic "clickers" and developing metrics that help inform risk management strategies and articulate risk reduction results to relevant stakeholders.

***Cheryl Conley**, Business Area Information Security Officer, Lockheed Martin*

9:45-10:05 am — **Networking Break**

10:05-11:00 am

Building An Awareness Conference

Employees bombarded with email information and online training can rapidly become deaf to important awareness messaging. To break through the communication "noise," FedEx Information Security Awareness hosts a security awareness conference every October in conjunction with National Cyber Security Awareness Month. Listen to the journey of how a one-day speaker engagement has grown into a three-day conference filled with informative sessions that employees can participate in at their discretion.

***Cathy Click**, Graphic Designer/Awareness Event Coordinator, FedEx*

11:00-11:45 am

The Human Risk Survey - A Human Vulnerability Scanner

The Human Risk Survey is a collaborative tool developed by the security awareness community over the years. This talk will discuss recent updates to the survey and how to use it to more effectively measure security knowledge, attitudes, and behaviors within your organization. Good surveys are harder than they look and this presentation will show you how to make them better. Takeaways for the presentation include:

- What makes a good survey?
- Developing the Human Risk Survey
- Using the survey – how do you do it and what does it tell you?
- Examples of data and analysis

***Lance Hayden, PhD**, Solutions Architect, Cisco Security Solutions*

11:45 am – 1:15pm **"Show & Tell" Lunch**

During this informal networking luncheon, attendees will have the opportunity to share examples of training materials they have developed and used in their awareness programs. Pick up tips and tricks, and share your own best practices, while enjoying lunch compliments of SANS Institute.

1:15-2:00 pm

Selling Enthusiasm

Communication is a critical part of security awareness. In order to help your audience be more security-aware, you must get your message to them, they must be receptive, and they must understand it. A brilliant message that no one reads will not help you achieve your goals.

A law firm is a challenging environment for effective communication. The audience is intelligent, interested, and engaged in the operation of the firm - but also determined, focused on their own productivity, and quick to dismiss anything they perceive as "wasting time." If you can get your messages heard here, you can get them heard anywhere.

We'll look at some of the most - and least - effective communications campaigns run by my office, including development, strategies, and how we measure the impact of our messaging.

***Matt Beland**, CISSP, Chief Security Officer, Davis Wright Tremaine LLP*

2:00-2:45 pm

Measuring Human Risk: What is Your Organization's Security Score?

This session will showcase the methodology and results of a multi-year human security risk assessment and security awareness initiative at Michigan Technological University. This discussion will include the risk assessment system, metrics, and scoring used to identify specific training needs by individual, department, and division, to uncover high-risk behavior, and to direct training and auditing where they are needed most. Multi-year data trends, combined with organizational structure data and training metrics are used to measure the actual impact of awareness training. As this process continues, it is used to focus Michigan Tech's security resources based on institutional risk and to help calculate the business value of security awareness programs.

***Dan deBeaubien**, Director, SANS Institute*
***Ashley Sudderth**, Chief Information Compliance Officer, Michigan Tech*

2:45-3:05 pm	Networking Break

3:05-4:00 pm

Awareness Through Gamification

We are all familiar with the dread of yet another PowerPoint presentation in a drab conference room or another computer based training that is all text and limited engagement. Yet breaking out of this conundrum can be challenging with limited delivery times and budgets as well as compliance regulations to meet. How can we develop security awareness in which participants are actively engaged and even eagerly anticipate? Many whitepapers discuss the theories of gamification – the art of teaching through interactive games, simulation and engagement. In this presentation we will discuss the actual execution of a campaign actually conducted. With a focus on logic and empowered decision-making rather than compliance and regulation, this project represented one of the most successful and impactful experiences we have completed. We will also share lessons learned, implementation strategies, and tools to make gamification possible within any environment.

***Jonathan Homer**, SecAware Team, Idaho National Laboratory*

4:00-4:45 pm

Attendees' Choice: Speakers Weigh In

Throughout the day, speakers will share their viewpoints and experiences with attendees. In this session, we turn things around and pose the questions attendees most want answered, as determined through live crowdsourcing at the event. Don't miss your chance to ask your question and get direct feedback from these leaders.

Moderator:
***Alan Paller**, Director of Research, SANS Institute*

Panelists:
***Matt Beland**, CISSP, Chief Security Officer, Davis Wright Tremaine LLP*
***Cathy Click**, Graphic Designer/Awareness Event Coordinator, FedEx*
***Cheryl Conley**, Lockheed Martin*
***Dan deBeaubien**, Director, SANS Institute*
***Lance Hayden**, PhD, Solutions Architect, Cisco Security Solutions*

4:45-5:00 pm

Closing Remarks

***Lance Spitzner**, Training Director, SANS Securing The Human Program*

Thank you for attending the SANS Summit.

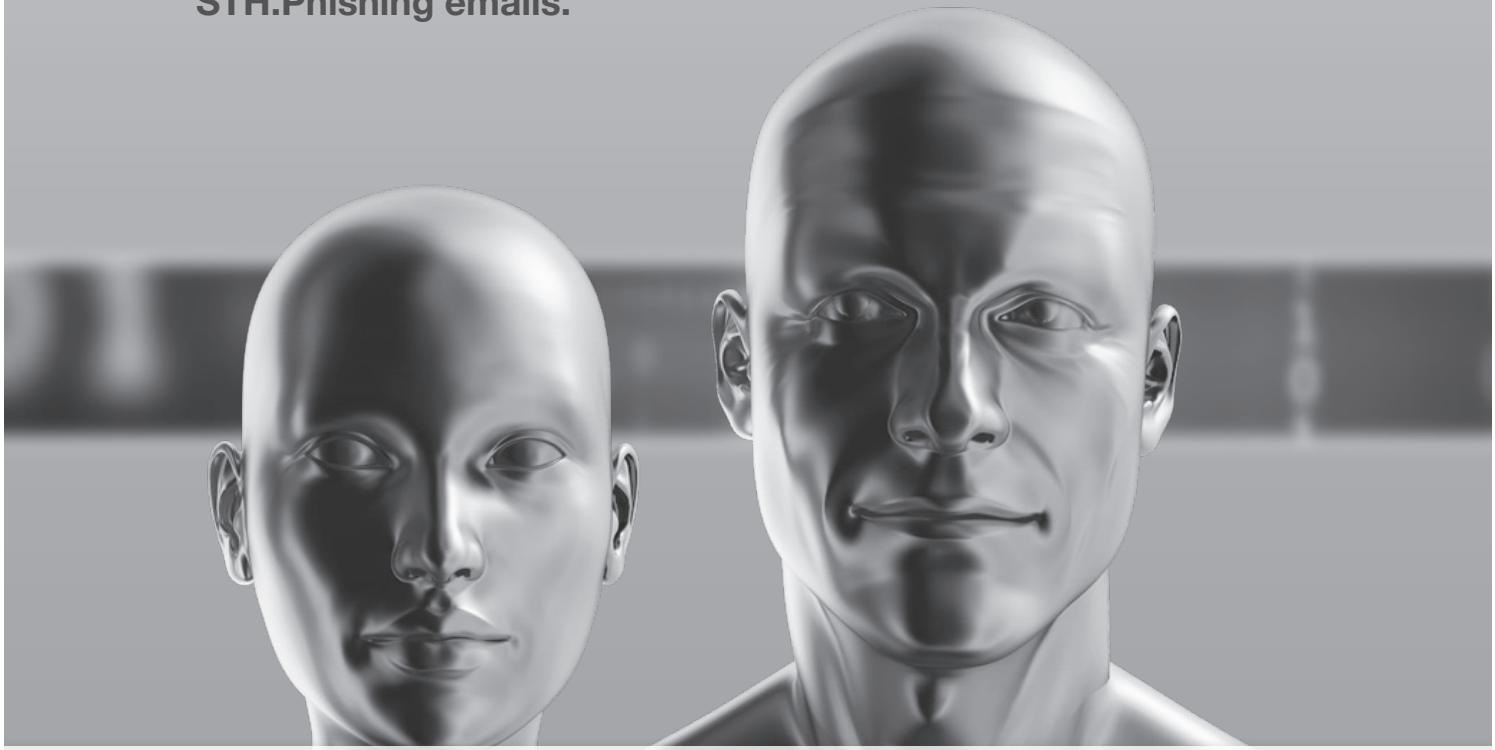
Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

SECURITY AWARENESS

FOR THE 21ST CENTURY

End User - Utility - Engineer - Developer - Healthcare - Phishing

- **Go beyond compliance and focus on changing behaviors.**
- **Create your own training program by choosing from a variety of computer based training modules:**
  - **STH.End User is mapped against the Critical Security Controls.**
  - **STH.Utility fully addresses NERC-CIP compliance.**
  - **STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems.**
  - **STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.**
  - **STH.Healthcare focuses on security behaviors for individuals who interact with Protected Health Information (PHI).**
  - **Compliance modules cover various topics including PCI DSS, Red Flags, FERPA, and HIPAA, to name a few.**
- **Test your employees and identify vulnerabilities through STH.Phishing emails.**



SANS SECURING THE HUMAN

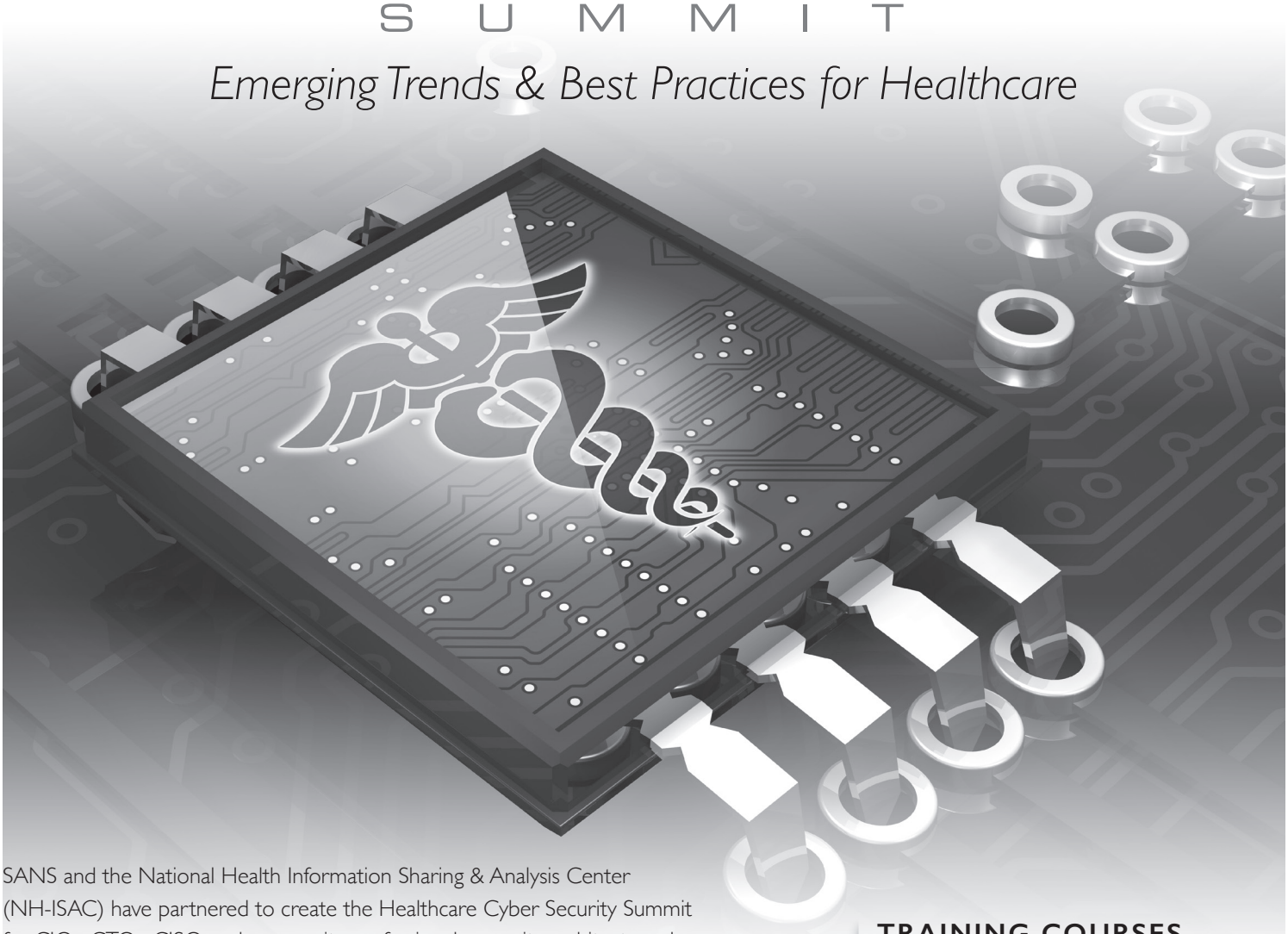
For a free trial visit us at:

www.securingthehuman.org

SANS San Francisco | December 3-10, 2014 | sans.org/event/healthcare-summit-2014

Healthcare CYBER SECURITY SUMMIT

Emerging Trends & Best Practices for Healthcare



SANS and the National Health Information Sharing & Analysis Center (NH-ISAC) have partnered to create the Healthcare Cyber Security Summit for CIOs, CTOs, CISOs, cyber security professionals, security architects and risk managers as well as compliance professionals. The ONLY event to discuss information sharing of cyber security intelligence specific to the health care industry to meet the ever growing need in securing health care.

New threats in health care (as recently revealed breach incidents show) are increasing and the most effective approach to better protect the industry is to share information regarding threats, threat actors and intent to better identify techniques, tools and best practices to protect intellectual capital and consumer health information.

The Summit will feature pioneering health care CIOs, CISOs and technology leaders who have faced issues head on and who will share the lessons they learned, combined with intensive training courses that will allow your technical staff to get up to speed quickly. Network among senior information security leaders, learn emerging and leading practices within cyber security and build relationships to promote more effective information sharing.

TRAINING COURSES

ICS410: ICS/SCADA Security Essentials **NEW!**

SEC301: Introduction to Information Security

SEC504: Hacker Techniques, Exploits, and Incident Handling

SEC542: Web App Penetration Testing and Ethical Hacking

FOR508: Advanced Computer Forensics Analysis and Incident Response

HOSTED: Health Care Security Essentials

Stay connected #HealthcareSummit

The sooner you register, the BIGGER the savings!

Register for a 4-6 day course, pay by October 22, 2014, and save up to $500 on tuition fees. Or reduce your Healthcare Summit registration fee from $1,495 to $495 when purchased in conjunction with a full-price 4-6 day course – SAVING $1,000! Secure your seat today **sans.org/event/healthcare-summit-2014**

UPCOMING SUMMITS & TRAINING EVENTS

2014

Pen Test Hackfest Summit & Training
Washington, DC | November 13-20

Healthcare Cyber Security Summit & Training
San Francisco, CA | December 3-10

2015

Cyber Threat Intelligence Summit & Training
Washington, DC | February 2-9

10th Annual ICS Security Summit & Training
Orlando, FL | February 23 - March 2

Digital Forensics & Incident Response Summit & Training
Austin, TX | July 7-14

Cyber Defense Summit & Training
Nashville, TN | August 11-18

For more information on speaking at an upcoming summit or sponsorship opportunities, e-mail SANS at **summit@sans.org**.

Visit **www.sans.org/summit** for detailed summit agendas as they become available.