SANS SECURITY AWARENESS

SUMMIT 2017

Nashville, TN | August 2-3, 2017

Chairman: Lance Spitzner

#SecAwarenessSummit @SecureTheHuman www.securingthehuman.org info@securingthehuman.org

EVENT RULES

To encourage honest and open dialogue amongst attendees, this event follows the Chatham House Rules. This means you are free to share what you learn with others, however you cannot attribute the source. In addition, there will be no media at this event. More about Chatham House Rules at:
www.chathamhouse.org/about/chatham-house-rule

SHOW-N-TELL

Back by popular demand, this event is a creative and interactive way for attendees to generate new ideas for their own security awareness programs. Attendees bring and display materials (posters, stuffed animals, give away items, handouts, etc.) they've developed for their security awareness programs, and share how they created the materials and their impact. Grab a cup of coffee, browse the wares, take some snapshots, and get ready to take your awareness program to the next level. If you want to share your own materials, there is no prior registration or coordination required, just bring whatever you would like to show from your own program. We will provide you with a table, you provide the rest. You are welcome to setup your materials the night before the summit, during early morning registration or during the first break. We have a separate room dedicated just for Shown-Tell. You are welcome to leave your materials during the whole event including overnight, however we recommend do not leave anything highly valuable such as electronics. Please be prepared to provide any vendor related information in-case other attendees want to do what you did.

SPEAKER Q&A

For this year, we are adding time after every talk for you to ask the speakers questions. In addition, we are adding time for you to discuss with members at your table one thing you learned from each talk.

EVENT BADGES

One of our goals is to maximize your ability to meet and network with other attendees. That is why when you pick up your badge during registration, be sure to select the industry sticker(s) that apply to your organization and stick them on your badge. This way you can easily identify others in the same industry as you, and vice-versa. In addition, we have colored stickers to represent the size of your organization so you can easily spot others the same organizational size as you. Finally, we will be providing red Sharpie markers at every table, use the red markers to write on your badge any topic you are passionate about or hoping to learn more.

AUGUST 1

Title: Pre-Summit Meet and Greet

This optional session offers the opportunity to meet and network with your fellow attendees the night before the Summit kicks off. We highly recommend you attend if possible. This is an amazingly friendly group.

EVENT NOTES

All approved presentations will be available online following the Summit at:
https://securingthehuman.sans.org/resources/summit-archives

DAY 01 8:00-10:40AM

8:00-8:45 am

REGISTRATION AND COFFEE

8:45-9:00 am

Welcome, Introductions & Rules of Engagement

Lance Spitzner (@lspitzner),
Director - SANS Securing the Human

9:00-9:20 am

NETWORKING & INTRODUCTIONS

We know that the conversations among peers and the connections forged during these events are just as valuable as the talks. Kick off your day by getting to know the other attendees seated at your table and begin fostering those meaningful connections and exchanging ideas right away. Not sure what to say? Start off by introducing yourself with your name, organization/industry, size of your organization, what you hope to get out of the summit, why you are attending the event. If you're lucky enough to be attending with colleagues from your organization, consider splitting up for the most benefit.

9:20-10:00 am

Know Your Enemy

To effectively defend against a threat from an enemy or malicious actor, you first have to understand who you're dealing with. What are the adversary's motivations, skills, and methods? In this talk, Rob Lee will walk you through how attackers select, research, and target their victims. As a result, you will be far better prepared to train and defend your organization against targeted attacks that focus on your employees.

Robert M. Lee (@RobertMLee),
CEO and Founder – Dragos, Inc.

10:00 – 10:40 am

What do Cars and Beer have to do with Security Awareness?

For years we've heard that people with the "soft skills" of marketing and communications make good security awareness professionals. But what if your background is more technical, and you didn't come to the world of security awareness via Madison Avenue? How can you learn to be a little more Mad Man, a little less Mr. Robot? This talk is Sales and Marketing 101 for Security Professionals. You will learn:

- The classic sales funnel and how to create "pull" through the funnel
- How to segment and target an audience, creating effective engagement
- Sell the sizzle: make 'em hungry, don't feed 'em lunch
- Madison Avenue resources to leverage (for free!)
- Marketing tactics for your next Security campaign: guerilla, viral, ambient, experiential, content, and grassroots

Real-world examples will include tactics from last year's Video Wars winner, Edna. We'll take a brief look at the whole campaign and the successful tactics used in addition to the videos. Before entering the world of security, Lisa's passion was filming car commercials in the Israeli desert and curating museum exhibitions about the life of Henry Ford. Lisa now brings that passion to security awareness, believing that "user behavior" and "consumer behavior" are one and the same.

Lisa Plaggemier,
Security Awareness and Client Advocacy – CDK Global

SANS

SECURITY AWARENESS

SANS SECURITY AWARENESS SUMMIT 2017

DAY 01
10:40AM-3:00PM

10:40-11:00 am

NETWORKING BREAK

Drinks and snacks will be served.

11:00 - 12:20 am

Escape Rooms: Talk & Activity

The FedEx team will share how they created and executed security awareness escape rooms in their organization. They will then challenge each table to its own escape room. For those of you who are unable to complete all the locks in time or want to just learn more about escape rooms, the FedEx team will host a follow-on event later this evening after the Summit.

12:20-1:20 pm

NETWORKING LUNCHEON

Lunch is served onsite to maximize interaction and networking among attendees. If you finish lunch early, take a moment to review the show-n-tell tables or sign up for an evening activity.

1:20-2:00 pm

I've Got More Games Than Milton Bradley: Incentivize Positive Change in your Security Culture

Security awareness training is one of the last defenses against dastardly effective social engineering threats. Traditional vendor-purchased security awareness training is largely ignored by the workforce and can merely serve to ensure compliance without substantially reducing the risk. In fact, a 2016 Ponemon Institute survey found that 52% of organizations surveyed found their vendor-purchased security training product "somewhat or not effective." Using American Campus Communities, the nation's largest developer, owner, and manager of high-quality student housing, as a case study, this presentation will demonstrate the difference between traditional videos and a security awareness gamification program. Attendees will hear obstacles faced, and what worked and what didn't as we introduced a range of interactive games, contests, and rewards to motivate users to genuinely improve security.

Drew Rose,
Information Security Manager – American Campus Communities

2:00-3:00 pm

Lightning Talks - Phishing

In this exciting hour, five presenters will get ten minutes – and only ten minutes – each to share their stories and lessons learned on phishing. We will then follow the session with ten minutes of Q&A where you can beat up the speakers with your questions. This format jams tons of information into a short period of time. Don't blink!

- **Phish Me, Phish You –** Darren Lynch (@lynchdog24),
  Network Security Team/SOC – Lawrence Livermore National Laboratory
- **Phishing Program Tips & Tricks –** Tonia Dudley,
  Director, Security Awareness – Financial Services
- **Tailoring Lures to your Target Audience –** Ryan Cadwalader,
  Security Awareness Specialist – Zurich Insurance
- **Phishing High Value Targets –** JJ Rivera,
  VP, Cybersecurity Phishing Program JPMorgan Chase
- **Big Phish, Little Phish, How Should You Phish? –** Chrysa Freeman,
  Security Awareness & Education, Code42

DAY 01
3:00-5:00PM

3:00-3:20 pm	**NETWORKING BREAK**
3:20-4:30 pm	**Security Awareness Video Wars** Volunteers will show clips of 3 minutes of security awareness videos they've developed for their security awareness programs. Presenters will then share lessons learned, to include how the video was developed, how it was deployed, and the impact. Attendees will select the videos they think are the most effective, and winners will be awarded the coveted SANS Securing The Human security awareness coin.
4:30 – 4:50 pm	**Table Closing Discussion** Each member of table will share with everyone else one key learning from the day's agenda, and plans for applying that takeaway to their program when they get home.
4:50 – 5:00 pm	**Closing Remarks**

SANS SECURITY AWARENESS

SANS SECURITY AWARENESS SUMMIT 2017

DAY 02 8:45-10:20AM

8:45-9:00 am

Day 2 Kick Off and Coordination Items

Lance Spitzner (@lspitzner),
Director - SANS Securing the Human

9:00-9:20 am

Introductions & Networking

For the second day of the Summit, please sit at a new table so you can meet, network, and interact with a whole new group of peers.

9:20-9:40 am

Getting It Right the First Time; Avoiding the Costs of a Bad Cybersecurity Hire

Organizational leadership and cybersecurity management grapple with a talent shortage of unprecedented proportions. As CISOs race to build their information security teams, hiring managers face stiff competition for skilled professionals. Regrettably, employing the wrong person can drain a company of productivity, money, morale and negatively impact reputation. According to the U.S. Department of Labor, the cost of a bad hire is at least 30 percent of the employee's first-year earnings – for a security analyst, that's $27,000+. These challenges are even more profound when it comes to hiring cybersecurity professionals. A recent study conducted by the Center for Strategic and International Studies (CSIS) and Intel found that 82% of respondents reported a shortage of cybersecurity skills at their organization, and 71% percent say the talent deficit has hurt their organization. In an era driven by bottom line metrics, getting a hire right the first time is more important than ever.

In this session, we will:

1. Explore the workforce talent shortage and dangers of a bad hire
2. Discuss means to assess skills and best practices
3. Review case studies of successful innovative programs to develop new cyber talent pipelines

Max Shuftan,
Director of CyberTalent Solutions, SANS Institute

9:40-10:20 am

When is it Time to Reboot Your Awareness Program?

While the Lockheed Martin's The I Campaign™ has been extremely successful and includes our effective and impactful phishing program, it became apparent in early 2016 that we needed to advance and focus our mission and strategic vision by incorporating the tools and techniques of the future, working to be a step ahead of technology and rapidly changing adversarial techniques. The team received accolades but wanted to drive the statistics through improvements in overall metrics; emphasizing content updates and next-gen communication toolsets to provide enhanced integration of short, lighter awareness methodologies; tagline updates; and even a cybersecurity mascot persona. By definition, campaigns come to an end. The I Campaign™ team prefers to think we're morphing to a more advanced Awareness Crusade. This talk will include our initial assessment, planning cycle, expectations for overall employee engagement, actions taken to date, and leadership communications. Key takeaways include what's working (or not), leveraging diverse generations, and enabling non-IA professionals.

Cheryl Conley,
Security Education and Awareness – Lockheed Martin

SANS SECURITY AWARENESS

SANS SECURITY AWARENESS SUMMIT 2017

DAY 02 10:20AM-2:20PM

10:20-10:40 am — NETWORKING BREAK

10:40 -11:40 am

Ambassador Programs

Ambassador programs are one of the fastest growing and most effective methods organizations are using to effectively engage employees and change behavior. In this special one hour session, we'll have awareness officers from three different organizations (Salesforce, Dropbox, Adobe) share their lessons learned in building their awareness programs. We will then have an extended discussion period where you can both ask questions of the speakers and share ideas with people at your table.

- Cassie Clark, *Sr. Security Community Strategist – Salesforce*
- Julia Knecht, *Manager, Security and Privacy Engineering – Adobe*
- Jessica Chang, *Program Manager, Trust & Security – Dropbox*
- Christine Keung, *Chief of Staff to the General Counsel - Dropbox*

11:40am-12:20pm

Getting the Board on Board: Gaining Board Support for Your Awareness Program

Get the inside scoop on a board member's perspective on how to effectively frame risk and communicate program and training requirements to the board and CEO. In light of all of the high-profile breaches reported daily by the media, there is still a troubling tendency to view cybersecurity risk as being fundamentally different than and separate from other risks facing an organization, or as simply an "IT problem." This session will provide clear and actionable tips and guidance on clean and effective communication strategies to make sure your message resonates at the boardroom table and ensure security awareness is embraced as a strategic priority from the very top of the organization.

Kevin Magee,
Member Board of Directors - Brant Community Healthcare System

12:20-1:20 pm — NETWORKING LUNCHEON

1:20-2:20 pm

Lightning Talks

In this exciting hour, presenters will get ten minutes – and only ten minutes – each to share one powerful awareness initiative, idea, or best practice. This format jams tons of information into a short period of time. Don't blink!

- **Deploying a National Awareness Campaign –** Tiffany Schoenike (@STOPTHINKCONNECT | @StaySafeOnline), *Director, Campaigns & Initiatives – National Cyber Security Alliance & Ben Flatgard, Former White House NSC Director*
- **It Takes a Village: Hands-On Security Awareness –** Taylor Lobb, *Manager, Security and Privacy Engineering, Adobe*
- **How to Produce Funny & Engaging Videos –** Jason Hoenich (@jasonhoenich), *Manager, Information Security Awareness & Training, Sony Pictures Entertainment*
- **Is Your ePublication Just Another Castaway on Unread Island? –** Cathy Click, *Security Awareness Project/Process Advisor, FedEx*
- **Safe Outside the Walls - The Home Visit Programme? –** *John Scott, Head of Information Security Education – Bank of England*

SANS SECURITY AWARENESS

SANS SECURITY AWARENESS SUMMIT 2017

DAY 02
2:20-5:00PM

2:20-3:00 pm

Rock the Boat: Transforming Security Culture Through Innovation

Traditional security education programs tend to live within the boundary of an organization's culture, emphasizing compliance and resisting radical ideas. At Geisinger Health System (GHS), we have opted to challenge this norm. Our goal is to transform the culture rather than work comfortably within the box. We contend that in order to create a security culture, an information security department must be innovative, creative and – to a degree – non-conformist. It is not enough to plug 'n play the latest security training solution. Security teams must employ unorthodox training methods and "rock the cultural boat" because, in the moments following the tilt, those aboard become simultaneously aware of their surroundings and uncomfortable enough to act quickly – two characteristics that help right the ship and chart new course. In security terms, this translates to a workforce capable of making sound technical decisions. In this session, we will present lessons learned from our own journey and hope to assist others who want to rock the boat and begin transforming their own security culture.

Graham J. Westbrook (@prescientwolf), *Cybersecurity Analyst – Geisinger Health System*

3:00-3:20 pm

NETWORKING BREAK

3:20-3:40 pm

Business E-mail Compromise

Special Agent Cavender will discuss the evolving threat of business e-mail compromise (BEC), findings from the most recent FBI Internet Crime Report, and how law enforcement is working to thwart the bad guys.

Special Agent Don Cavender, *Federal Bureau of Investigation*

3:40-4:00 pm

The Security Awareness Community Has Spoken: What's the Word and What Next?

The team at American University's Kogod Cybersecurity Governance Center (KCGC) had a blast analyzing the data for the 2017 SANS Security Awareness Report. The security awareness community had a lot to say in the survey responses and we learned a lot about what makes you tick, and what gets in your way. We'll share with you some of the challenges we faced and additional insights we uncovered while sifting and crunching the data for this year's report, including those related to KCGC's core mission – cybersecurity governance. In particular, what role do leadership, authority, responsibility and accountability play in implementing a successful awareness program? And because this work is ultimately all about you – the community – we'll open the session up for your input on next year's survey.

Rebekah Lewis, *JD, CISSP, CIPP/US, Director, American University's Kogod Cybersecurity Governance Center (KCGC)*

Taylor Heywood, *Research Assistant, KCGC*

4:00-4:30 pm

Show-n-Tell Winners Announced

Winners of the show-n-tell event will be announced. The winners will present on their materials, how they came up with and implemented the winning ideas, and the impact on security awareness as a result.

4:30-4:50 pm

Closing Table Discussions

Each member of table will share with everyone else one key learning from the day's agenda, and plans for applying that takeaway to their program when they get home.

4:50-5:00 pm

Closing Remarks

RYAN CADWALADER

Ryan Cadwalader is an Information Security Awareness Analyst at Zurich Insurance. Within his first year, Ryan supports the phish education training program for a global audience and has helped build a foundation that interconnects a variety of services to educate Zurich's employees. Ryan graduated from Cal State University Long Beach and obtained his bachelor's degree in marketing.

DON CAVENDER

Don Cavender is a 27 year veteran Special Agent of the FBI. He is currently the FBI Washington Field Office Business Email Compromise Coordinator for intrusion-related incidents and works major financially motivated cyber-crime in the NoVA and Washington DC area. In the 1990s, he investigated and disrupted Columbian and Mexican drug cartel organizations along the U.S. southwest border. During the late 1990's, he transitioned to cyber crime, later rising to manage programs in the FBI computer forensics lab and instructing at the FBI Academy, developing the first cyber crime curriculum taught in the FBI. Following the attacks of September 11, 2001, he applied his technical expertise for nearly 15 years, receiving numerous awards and commendations.

JESSICA CHANG

Jessica Chang is the Program Manager of Trust & Security at Dropbox, where she manages the security culture program and key team initiatives in trust, security, and privacy. She built and launched Dropbox's security awareness program in conjunction with National Cyber Security Awareness Month. She began her career as a professional musician and is passionate about building communities through her work.

CASSIE CLARK

Cassie Clark is Sr. Security Community Strategist at Salesforce. She encourages secure coding at Salesforce by engaging developers through training, initiatives, and incentives. She focuses on building community and infusing culture through her work. She is particularly proud of her use of outdated, nerdy pop culture references.

CATHY CLICK

Cathy Click, Security Awareness Project Manager, has more than 18 years of experience at FedEx with 16 years spent in IT and the last 10 years focused on Security Awareness for the corporation. Cathy was named in 2016 as "One to Watch in Cyber Security" by the SANS Institute, for her leadership in the security awareness community.

CHERYL CONLEY

Security Education and Awareness – Lockheed Martin

Cheryl has led the Security Education & Awareness Team in the Corporate Information Security organization, managing the development of an ad hoc initial user awareness capability to LM's awareness program trademarked The I Campaign®. Cheryl's accomplishments demonstrates her passion for the Security Awareness arena which has translated to the invaluable change in users' cybersecurity perceptions. The SANS Institute named Cheryl among its 2014 Difference Makers which complemented her Lockheed Martin Excellence in Leadership Award.

TONIA DUDLEY

Director, Security Awareness – Financial Services

What do you get when you mix 14 years of several Finance roles, transitioning into IT roles for 10 years and making my way into a few Security roles? A very passionate and diverse Security Awareness professional that can mix business, technology and security into a common language. Award: Challenger Award 2015 – building a robust Anti-Phishing solution to reduce risk to the business. Award: PhishMe Excellence Award 2016 – PhishMe Community Trailblazer of the Year

BEN FLATGARD

Ben Flatgard is the founder and principal of cycise, a security technology company. Ben served in the Obama Administration from 2009-2017. In his most recent post, as Director for Cybersecurity Policy on the National Security Council, Ben was responsible for leading policy development for the U.S. government in areas related to cybersecurity in the financial services and healthcare sectors, consumer security, and emerging technology.

CHRYSA FREEMAN

Chrysa Freeman lives in Minneapolis, MN. She has a B.A. in Communications from the University of Minnesota and an M.B.A. at St. Thomas. She currently leads the Code42 Security Awareness program. Code42 is a fast growing, Minnesota grown SaaS software start-up. Prior to that she was at Target Corp for eight years where she created a Security Awareness Program for a population of 18,000 end users, ran it single-handedly for two years and then managed the program with a team of four. During both those programs she interviewed training vendors, managed negotiations, then stood up and ran the phishing programs as well as all things Security Awareness.

TAYLOR HEYWOOD

Taylor Heywood is a Research Assistant at KCGC and an undergraduate student at American University, triple majoring in Computer Science, Applied Mathematics, and Business Administration. Outside of working at KCGC, Taylor also interns with the American University Information Security Team and is a competitive member of the American University Mock Trial Team. Taylor is also a member of Upsilon Pi Epsilon and Betta Gamma Sigma.

JASON HOENICH

(@jasonhoenich),
Manager, Information Security Awareness & Training - Sony Pictures Entertainment

Jason brings over 10 years of expertise, having built awareness programs for companies like Disney, Activision, and Sony Pictures Entertainment. His focus on user experience as being the foundation within awareness programs is helping to push the industry to Security Awareness 2.0. He wrote and produced several internal videos for The Walt Disney Company, an experience which has led him to start his own security awareness video series, Hashtag Awareness.

CHRISTINE KEUNG

Christine Keung is Chief of Staff to the General Counsel at Dropbox, overseeing cross-functional workstreams between trust, legal, security, and privacy. She started her career in Security Operations, where she built and scaled internal security training and awareness functions, including Dropbox's inaugural Capture the Flag competition, and security culture program.

JULIA KNECHT

Julia Knecht manages Product Security and Privacy Engineering at Adobe. She created and is responsible for the Secure Product Lifecycle of Adobe's Digital Marketing Business. An integral and invaluable piece of the Secure Product Lifecycle is her Security Champions program, which has been running successfully for three years.

ROBERT M. LEE

(@RobertMLee)

Robert M. Lee is CEO, Founder of the critical infrastructure cyber security company Dragos. He is also a non-resident National Cyber Security Fellow at New America and a SANS course author and Certified Instructor.

REBEKAH LEWIS

Rebekah Lewis, JD, CISSP, CIPP/US, is the Director of American University's Kogod Cybersecurity Governance Center (KCGC), a multi-disciplinary research initiative focused on the governance and management of cybersecurity. Rebekah previously served as a cybersecurity and information assurance attorney for the U.S. National Security Agency and practiced law in the Washington office of Latham & Watkins.

TAYLOR LOBB

Taylor Lobb is a Manager of Security at Privacy at Adobe where he leads a team of penetration testers and develops programs and training to raise security awareness. Previous to Adobe Taylor worked as information security manager for Clearwater Analytics where he created several security training and awareness programs.

DARREN LYNCH

(@lynchdog24)

Information Technology Professional with 17 years of experience in System Administration, Cyber Security Education, technical support in high-tech, software, and banking industries.

Effective team leader with strengths in team building, customer relations and problem solving. Organized, take-charge professional with exceptional follow-through abilities and able to plan and oversee projects from conception to completion. He has a canny ability to make people laugh and have a good time.

KEVIN MAGEE

Member Board of Directors - Brant Community Healthcare System

Kevin Magee is one of Canada's leading authorities on cyber security cyber risk governance and security awareness. He is a cyber security executive with Gigamon Canada, Board Member at the Brant Community Healthcare System and guest lectures and advises on curriculum development for several Canadian Colleges Universities and Industry Associations.

LISA PLAGGEMIER

Security Awareness and Client Advocacy – CDK Global

Lisa has spent her career branding and marketing cars and trucks, software and data, and now security. She's combined her passion for the automotive industry with a fervor for security awareness to help CDK, OEMs, and dealers manage their risk and grow their businesses securely. Lisa worked for marketing for Ford Motor Company in the US, Europe, Africa and the Middle East. She is currently the Director of the Client Security Advocacy Office for CDK's Global Security Organization. Lisa graduated from the University of Michigan and currently lives in Austin, TX.

JJ RIVERA

JJ Rivera is a Vice President and the lead for the Cybersecurity Phishing and Operational Drill Programs at JPMorgan Chase. He joined JPMC after eight years in the United States Air Force as an Information Security Manager. He received his Bachelor of Arts in History from Columbia University. He currently resides in New Jersey.

DREW ROSE

Information Security Manager – American Campus Communities

Drew Rose earned a BS in Cybersecurity from the University of Maryland and holds the following certifications, CISSP, CEH, GCIA, and CCNA-Security. At his current position Drew handles everything from security architecture and operations to policy building and enforcement. His true passion lies in building progressive security awareness programs.

TIFFANY SCHOENIKE

Director, Campaigns & Initiatives, National Cyber Security Alliance

Tiffany Schoenike started with NCSA in 2012 and serves as director of campaigns and initiatives, promoting privacy and online safety awareness and education. Tiffany provides strategic direction for the STOP. THINK. CONNECT.™ campaign and works with diverse stakeholders to develop and execute national privacy and security campaigns. In 2016, Ms. Schoenike worked with the Obama White House to coalesce 40 government, industry and nonprofit stakeholders to develop and launch Lock Down Your Login, a STOP. THINK. CONNECT.™ campaign to educate Americans about strong authentication.

JOHN SCOTT

Head of Information Security Education – Bank of England

John is an established Information Technology trainer, with many years' experience in Further and Higher Education and training in both the private and the public sector. He has been integral in the implementation of the Bank of England's current security training programme, and is focused on the transition from passive compliance to active security.

MAXWELL SHUFTAN

Director of CyberTalent Solutions – SANS Institute

Max leads the CyberTalent division of SANS Institute. In this role, he directs business development and external stakeholder engagement to support the various SANS CyberTalent programs and develop strategic partnerships. He also oversees CyberTalent program operations and staff management. SANS CyberTalent helps organizations in both the public and private sectors address their cybersecurity human capital needs through initiatives such as VetSuccess, the Women's Immersion Academy, and the CyberTalent Assessments, among others. Max joined SANS Institute as its' CyberTalent Business Development manager in 2015.

LANCE SPITZNER

Summit Chair & Director, SANS Securing The Human

Summit Chair & Director, SANS Securing The Human

Lance Spitzner has over 20 years of security experience in cyber threat research, awareness and training. He invented the concept of honeynets, founded the Honeynet Project and published three security books. Lance has worked and consulted in over 25 countries and helped over 350 organizations plan, maintain and measure their security awareness programs. In addition, Lance is a member of the Board of Directors for the National Cyber Security Alliance, frequent presenter, serial tweeter and works on numerous community security projects.

GRAHAM J. WESTBROOK

(@prescientwolf)

Graham J. Westbrook (Sec+, C|EH) is a cybersecurity analyst with Geisinger Health System's Information Security Office. As an intelligence analyst by training and cybersecurity analyst by trade, Graham merges the disciplines to run the Threat Intelligence and User Awareness programs at Geisinger. Past experience includes time with a Defense Contractor, Foreign Policy firm and Nashville-based tech. company, Five Iron Technologies.