

<b>Day 00 – Tuesday, August 6</b>	
6:00 – 8:00 pm	<p><b>Pre-Summit Meet and Greet</b></p> <p>This optional session offers you the opportunity to meet and network with fellow attendees the night before the Summit kicks off. We highly recommend you attend if possible. In addition to free food and drinks, we will be hosting an interactive treasure hunt with an iPad as the top prize.</p>

<b>Day 01 - Wednesday, August 7</b>	
8:00 – 8:45 am	<p><b>Registration and Coffee</b></p>
8:45 – 9:00 am	<p><b>Welcome, Introductions &amp; Rules of Engagement</b>  <i>Lance Spitzner (<a href="#">@lspitzner</a>), Director, SANS Security Awareness</i></p>
9:00 – 9:20 am	<p><b>Networking &amp; Introductions</b></p> <p>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. Introduce yourself with your name, organization, industry, size of your organization, what you hope to get out of the summit, and one thing most people do not know about you. No more than two minutes per person.</p>
9:20 – 9:30 am	<p><b>Online Polling</b></p> <p>We introduce you to what online polling is and how it works, then kick things off with a couple of fun polls.</p>
9:30 – 10:10 am	<p><b>Keynote: Latest Techniques in Hacking the Human – Jake Williams</b></p> <p>Learn from the Incident Responder’s perspective what the latest human-based attacks are, how bad guys are getting in, what they are doing once they are inside, and what their tools, tactics, and motivations are. Join us as world-renowned security expert Jake Williams shares the latest attacks he’s seeing as he responds to some of the most fascinating and advanced cyber attackers on the planet.</p>
10:10 – 10:30 am	<p><b>Changing Culture: Lessons from Teaching Music – Jessica Chang, Robinhood</b></p> <p>Culture sets the guardrails for an organization’s shared values, goals, and practices, and it defines the attitudes and behaviors practiced over time. Outside the working world, our cultures also shape our values, perspectives, and habits as individuals within families, schools, and communities. During this talk, Jessica Chang will highlight the lessons learned from being a professional musician and teacher that</p>

	<p>apply to our profession as security education and awareness practitioners. While the world of classical music may be distinct from information security, music teachers are similarly tasked with using different learning theories and equally responsible for cultivating a mindset of growth and building informed behaviors that turn into lasting habits. Like security practitioners, music teachers use observation, analysis of behavior, and goal-setting to drive intended results. Learn how to foster meaningful results for your organization by assessing your organization’s culture of security, building complementary theories of learning for security, and designing a complementary hands-on curriculum to influence the formation of secure habits.</p>
<p>10:30 – 11:00 am</p>	<p><b>Networking Break:</b> Drinks and snacks will be served.</p>
<p>11:00 – 11:30 am</p>	<p><b>Using Appreciative Inquiry to Create a Network of Security Champions that Went Viral</b> – Sarah Janes, Layer 8 (@sarahkjanes)  In 2016, 40 operational security employees were put in a room and asked to imagine a future where employees demonstrated proactive security behaviors. Three years later, the team has over 600 security champions, all volunteers. The network, known as Openreach is able to demonstrate measurable changes in behavior and examples of real incident mitigation. This presentation will provide attendees with a step-by-step methodology to recruit, train, and sustain the momentum of champions, show how to use Appreciative Inquiry to engage stakeholders in self-determined change, and demonstrate how to use champions to measure behavioral change at the grassroots level (for example, what people are doing differently).</p>
<p>11:30 – 12:00 noon</p>	<p><b>Online Training Structure for Multi-generations</b> – Dr. Brenda L. Ellis, NASA  Today's cyber workforce is composed of members of five defined generations: traditionalists, baby boomers, generation X, generation Y, and millennials. These multi-generationalists are working together in a common setting and therefore must be trained in a manner that will effectively enhance knowledge and change behavior to reduce security risks in the workplace. Training such a diverse group across generations presents challenges in terms of different learning styles and educational practices, and those challenges only increase in online training. Learning is more effective when the learner is engaged and motivated. The ongoing question, then, is what is engaging to which learner? What motivates each generation? In answering these questions, this presentation will demonstrate the need for an integrated design solution for training. Attendees will gain a better understanding of the learning styles of each generation and see how to integrate effective training methods into risk-based cybersecurity training.</p>
<p>12:00 – 1:00 pm</p>	<p><b>Networking Luncheon:</b> 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.</p>
<p>1:00 – 3:00 pm</p>	<p><b>Tracks: Time to Choose! Select One of the Options Below:</b></p>

	<p><b>1. Beginner’s Track</b>  This track is for people new to the world of security awareness. The aim is to help attendees by discussing the foundations of security awareness and basic approaches to it. Each speaker gets 25 minutes to present, followed by a panel with all of the speakers together to answer your questions.</p> <ul style="list-style-type: none"> <li>- <b>Lessons Learned in Building an Award-Winning Phishing Program</b> – Dennis Legori, Total System Services, Inc.</li> <li>- <b>Security Awareness Recognition Program</b> – Nicole Jacobs, USAA</li> <li>- <b>Securing Leadership Support</b> – Janet Roberts, Zurich Insurance</li> <li>- <b>How to Use the Fogg Behavior Model, Nudge Theory, and More to Design Secure Behaviors</b> – Perry Carpenter, KnowBe4</li> </ul> <p><b>2. Metrics CyberScore Workshop (Advanced) – Jon Smiley, Highmark Health Solutions</b>  This hands-on, interactive workshop is for more experienced awareness officers and/or those who work in more mature awareness programs. Already have your CBT and phishing program rolled out? Is senior leadership looking for more detailed and useful measurements of the impact of your program? Join Jon and his team as they walk you through how they built a security awareness metrics dashboard both for their overall organization as well as at the business unit level. Then, through a series of interactive labs, you will build your own metrics dashboard for your own organization.</p>
3:00 – 3:30 pm	<b>Networking Break:</b> Drinks and snacks will be served.
3:30 – 4:00 pm	<p><b>The Creative Process Behind Fun, Low-Budget Videos</b> – Jill Barclay, Dignity Health  Video is one of the best visual tools you can use to convey complex information in an engaging way. But how do you actually make a video that is “engaging” in the first place? How do you come up with ideas for video content that would appeal to your audience? How do you make topics like cybersecurity consumable and entertaining? To be honest, it isn’t as hard as you might think. In this presentation I’ll showcase the creative process behind producing fun, budget-friendly videos and share surprising places to draw on for inspiration."</p>
4:00 – 5:00 pm	<p><b>Security Awareness Video Wars</b>  Volunteers will show short (no more than three minutes) security awareness videos they’ve developed for their security awareness programs. At the end of the video presentations you will be asked to vote on the videos you liked best and we will award the top winners. Videos will be shown in two categories: small budget (under \$5,000) and big budget (over \$5,000). After the videos and voting, we will ask the video submitters to sit down for an informal panel so that attendees can ask them questions.</p>
5:00 – 5:15 pm	<b>Closing Discussions at the Tables</b>

	Each person at a table will share with everyone else one key thing they learned from the day's agenda and how they plan to apply that takeaway to their program when they get home.
5:15 – 5:30 pm	<b>Closing Remarks</b>
6:00 – 8:00 pm	<b>SANS Fiesta by the Bay</b> <i>Join us for a taco and tequila fiesta at our Summit hotel, overlooking beautiful Mission Bay. We'll meet on the waterfront lawn for food, drinks, fun, and networking!</i>

Day 02 - Thursday, August 8	
8:00 – 8:45 am	<b>Networking and Coffee</b>
8:45 – 9:00 am	<b>Day 02 Kick-Off and Coordination Items</b> <i>Lance Spitzner (<a href="#">@lspitzner</a>), Director, SANS Security Awareness</i>
9:00 – 9:20 am	<b>Introductions &amp; Networking</b> 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 – 10:00 am	Keynote - TBD
10:00 – 10:30 am	<b>Partnerships &amp; Collaboration</b> – Alexandra Panaretos, EY Having worked in different industries, entities of various sizes, and a range of environments as both a consultant and practitioner, Alexandra Panaretos has seen the good, bad, and ugly ways that companies approach security awareness. The consistent theme in great programs is the willingness to collaborate with groups outside of the security team. Partnerships with physical security, corporate communications, human resources, legal, and yes, even employee health, can help build your program into a holistic approach to securing the human. Examples of successful campaigns and paths to partnership will be showcased, as will be a few of the frequent mistakes teams make along the way.
10:30 – 11:00 am	<b>Networking Break:</b> Drinks and snacks will be served.
11:00 – 12:00 noon	<b>Special Events</b> SANS has seen a growing interest in special events, so this presentation will provide two different perspectives on this approach to awareness training. Following the talks by each presenter, we will have them come together on the stage to answer your questions. <ul style="list-style-type: none"> <li>• <b>How to Build Your Own Escape Room</b> – Bob Hewitt (<a href="#">@infosecbobh</a>) and Justin Perkins, Stellar Technology Solutions</li> <li>• <b>Online Digital Scavenger Hunt: Engaging Security Awareness with Global Impact</b> – Laney Cannon, Citrix Systems</li> </ul>
12:00 – 1:00 pm	<b>Networking Luncheon:</b> 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.
1:00 – 3:00 pm	<b>Tracks: Time to Choose! Select One of the Options Below:</b>

	<p><b>1. OSINT Workshop</b>  At this hands-on, interactive workshop, you'll learn what open-source intelligence (OSINT) is, how it works, how you can use it in your awareness program, and even how to run an OSINT assessment of yourself. NOTE: Can't decide which course to take? <a href="#">SANS is also offering a full six-day course on OSINT right after the Summit.</a></p> <p><b>2. Communications &amp; Engagement Track</b>  Each speaker gets 25 minutes to present their point of view and experiences on the same topic – communications / engagement. Following their talks, we will have all of the speakers come together on a panel to answer your questions.</p> <ul style="list-style-type: none"> <li>- <b>Dashboard Confessions: Security Awareness Communication in Silicon Valley</b> – Brooke Pearson, Uber</li> <li>- <b>How to Transform Security Awareness Using Basic Marcom Methods</b> – Anett Stoica @annette_stoica, Paddy Power Betfair</li> <li>- <b>Shifting from FUD to Fun! How to Overcome Internal Obstacles for Program Success</b> – Mary Dziorny (@revsec), Revolutionary Security</li> <li>- <b>Cyber Agents for Change Leveraging Untapped Opportunities for Cybersecurity Awareness</b> – Diane Desauliners, Johnson &amp; Johnson</li> </ul>
3:00 – 3:30 pm	<b>Networking Break:</b> Drinks and snacks will be served.
3:30 – 4:30 pm	<p><b>Role-based Training Session</b>  SANS is seeing a growing interest in role-based training that ensures that the right people get the right training and no more. As such, this presentation will provide you with three different perspectives on this approach to awareness training.</p> <ul style="list-style-type: none"> <li>• <b>A One-Size-Fits-All Approach to Role-based Learning</b> – Jonelle Burns, JP Morgan Chase</li> <li>• <b>How Data-driven Personalized Journeys Are the Future of Security Training</b> – Aika Sengirbay, Autodesk</li> <li>• <b>Role-Based Awareness Training</b> – Joe Malec, Express Scripts</li> </ul>
4:30 – 5:00 pm	<p><b>Show-n-Tell Winners Announced</b>  Winners of the show-n-tell event will be announced, then make presentations about their materials, how they came up with and implemented the winning ideas, and the impact on security awareness as a result.</p>
5:00 – 5:15 pm	<p><b>Closing Table Discussions</b>  Each person at a table will share with everyone else one key thing they learned from the day's agenda and how they plan to apply that takeaway to their program when they get home.</p>

5:15 – 5:30 pm	<b>Closing Remarks</b>

<b>Optional Day 03 - Friday, August 9</b>	
<p>We are excited to announce a new event for the Security Awareness Summit: An optional third half-day! Yes, even more learning and interaction. Limited to only 160 people, this third day enables you to make the most of both the event and our amazing security awareness community.</p>	
8:00 – 8:45 am	<b>Networking and Coffee</b>
8:45 – 10:40 am	<p><b>Learning Theory/Instructional Design – Jon Portzline and Kevin Bennet, SANS Institute</b></p> <p>Spend the morning learning from several experts about the world of learning theory and instructional design. This hands-on workshop takes a deep dive as you develop learning objectives, leverage frameworks such as Blooms Taxonomy, ARCS and ADDIE, and engage in interactive team labs to help develop your own learning plans. Learn the science behind adult learning and apply those lessons learned to your own awareness program.</p>
10:40 – 11:00 am	<b>Networking Break:</b> Drinks and snacks will be served.
11:00 – 12:00 noon	<p><b>Birds of a Feather</b></p> <p>Complete the day by interacting with and learning from your peers through a series of “Birds of a Feather” sessions. These are informal table meetings where subject-matter experts, speakers, and attendees lead group discussions on the topics of their choice, ranging from metrics to learning theory, phishing, Ambassador Programs, gaining leadership support, and more. Pick the topic you want, jump in, then share with your peers and learn from them!</p>
12:00 noon	We wrap up the event at mid-day, allowing you to catch a flight home and still have time to spend your weekend with friends and family. What more could you ask for?

## Speaker Biographies

**Jill Barclay, Cybersecurity Communications Analyst, Dignity Health** Never afraid to take the path less traveled, Jill Barclay brings a fresh and innovative perspective to her communications campaigns. Jill has over 15 years of marketing/communications experience in health care and most recently transitioned to the fast-growing arena of Cybersecurity in health care IT. Jill's most recent claim to semi-fame is a series of award-winning videos she created to move employees toward better understanding of safer cybersecurity practices. She has a degree in Communications from Purdue University and was a guest lecturer for Liberal Arts Influentials course. Jill has a passion for all things odd, vintage, quirky, and unexpected—personally and professionally. And, if you ask, she might show you a picture of her retro toy Halloween costumes she created for her family. Spoiler alert: the Rock 'Em Sock 'Em Robots made an appearance.

---

**Kevin Bennet, Manager of Instructional Design, SANS Institute**

Kevin is a learning technology professional with 10 years of experience, and specializes in LMS integration, LMS administration, project management, interactive media development for online training portals, web standards such as HTML5, CSS3, and JavaScript, and graphic design. He creates highly interactive and effective e-learning courses, rich and engaging multimedia, simulations, user interfaces, and web portals. Kevin uses instructional design methodologies, industry best practices, need analysis, ADDIE model, rapid prototyping, and the Kirkpatrick model to develop effective training for instructor-led, blended and web-based training.

---

**Jonelle Burns, Vice President, Cybersecurity & Technology Controls, JP Morgan Chase**

Jonelle is passionate about learning and development and mitigating firm-wide risk through positive behavior change. As Program Manager, Global Cybersecurity Awareness, Jonelle partners with other Cybersecurity and Technology Controls (CTC) teams to identify valuable data and translate into consumable messages for the firm's employees. Jonelle then strategizes an awareness campaign and training strategy and partners across multiple teams and businesses to tell the story. In 2018, Jonelle was responsible for delivering the mandatory firm-wide Annual Cybersecurity Awareness course as well as developing the first-ever Data Loss Prevention remediation training assigned to policy violating employees. Jonelle also oversaw Cybersecurity Awareness Month, which included 88 events across 8 countries.

---

**Laney Cannon, @cannon\_laney, Program Coordinator, Citrix Systems, Inc.**

With a background in anthropology and marketing, Laney spends her days strategizing and communicating for the Product Security & Standards organization. Her love of culture and human behavior sparked her interest in security awareness. In her free time, she's obsessed with Citrix's Women's Inspirational Network, Raleigh's local music, people watching at airports and her foster dogs.

---

**Perry Carpenter, @perrycarpenter, Chief Evangelist and Strategy Officer, KnowBe4** Perry is KnowBe4's Chief Strategy Officer and the author of "Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors." Previously, Perry led security awareness, security culture management, and anti-phishing behavior management research at Gartner Research, in addition to covering areas of IAM strategy, CISO Program Management mentoring, and Technology Service Provider success strategies. He holds a Master of Science in Information Assurance (MSIA) from Norwich University in Vermont and is a Certified Chief Information Security Officer (C|CISO).

---

**Jessica Chang, @jessicatchang, Security Program Manager, Robinhood** Jessica is a Security Program Manager at Robinhood. Prior to Robinhood, she built and led the global security culture program and key company initiatives in trust and security at Dropbox as a Tech Lead for Security Culture. These programs included Trustober, a global celebration of safety, security, and trust held annually in conjunction with National Cyber Security Awareness Month, as well as over 130 talks and workshops on security and safety. She holds degrees from Yale, the Juilliard School, and the Curtis Institute of Music, maintains a dual career as a professional musician, and is passionate about building communities through her work.

---

**Diane Desaulniers, Manager, Governance Communications & Cybersecurity Awareness, Johnson & Johnson**

As a communications professional for 35 years, Diana has worked in corporate environments across many industries. Throughout her career, she has focused on representing the voice of the user in the typically complex environment of IT communications. In 2009, Diane joined Johnson & Johnson, and has been leading communications for information security for the last 7 years. However, her true passion is cybersecurity awareness; helping people to realize they have the power to protect their data and how to be cyber secure. She is a member of the H-ISAC Cybersecurity Education Awareness Committee, which is expanding awareness in the healthcare sector. She's also a musician, sailor and loves gardening.

---

**Mary Dziorny, @RevSec, Senior Cybersecurity Consultant, Revolutionary Security**

Mary Dziorny, PhD is a Senior Cybersecurity Consultant with over 9 years of experience in the cybersecurity field and over 20 years of experience in the education and training field. She has designed, developed, and implemented many training programs over the course of her career, including two comprehensive enterprise-wide security awareness programs.

---

**Dr. Brenda Ellis, @BrendaLEllis1, Program Manager, IT Security Awareness and Training, NASA**

Dr. Brenda Ellis is currently the Program Manager of NASA's IT Security Awareness and Training Center and has over 30 years of federal service working and managing in computing and various technical cyber security and education programs.

---

**Bob Hewitt, @infosecbobh, CIO, Stellar Technology Solutions; Instructor, SANS Institute**

Bob has been active in information security since 1994. He began his career as a Network Engineer in the United States Air Force and was first introduced into information security when he discovered malicious activities against the infrastructure he was managing. Through his Air Force career, he held various technical roles in which he was always able to implement controls, threat identification/management, and continuity. He eventually became a Lead Information Technology Instructor and developed and instructed courses related to systems and network administration and information security. Upon leaving Active Duty he entered the Air Force Reserves for 10 years where he continued instructing and worked as an evaluator for search and rescue and intelligence gathering exercises for State level agencies and Homeland Security.

---

**Nicole Jacobs, Information Security Officer USAA** Nicole is an Information Security Advisor, overseeing the Security Awareness Program for USAA, including the Fraud Fighter program. Her background includes fraud analysis, rule coding and supervising fraud teams. Nicole interned with the Secret Service Dallas field office, has a degree in Criminal Justice and is a Certified Fraud Examiner.

---

**Sarah Janes, @sarahkjanes, Managing Director, Layer8** Starting her career in BT and then running a security awareness practice Sarah has developed and delivered security awareness strategies to a wide variety of businesses of sizes and sectors. Frustrated with the slow progress in the human factor in security Sarah started Layer 8 Ltd in 2013.

---

**Dennis Legori, @DennisLegori, Senior Information Security Analyst Senior, Total Systems Services** Dennis has over six years of experience in Information Security and launched the Global Security Awareness Program at TSYS in 2013. He has a MBA, MPA, and is PhishMe Certified. Dennis implemented monthly phishing simulations in 2015 and his phishing awareness program won the 2018 Enterprise Defense Program of the Year.

---

**Joe Malec, Senior Security Analyst, Express Scripts** Joe is a senior security analyst with over 20 years of experience in information technology. He is responsible for the security training & awareness program for Express Scripts and has spoken at conferences and appeared on TV and radio to discuss IT security issues. He is also a Fellow with the ISSA.

---

**Alexandra Panaretos, @Cyber\_simple, America's Cyber practice lead for security awareness and training, EY** Alex is the Americas Cybersecurity Lead for Security Awareness and Training in the Advisory practice of Ernst & Young LLP. Alexandra's primary focus in awareness program design is the individual, which she showcases in materials that are relevant for multiple generational, cultural, and learning styles in an enterprise.

---

**Brooke Pearson, Staff Program Manager, Security Awareness, Uber** Brooke Pearson is a that Brooke was at Facebook developing policy and communications programs for Facebook's public policy and information security teams. Brooke joined Facebook after five years working in public diplomacy for the U.S. Department of State with responsibility for Afghanistan and Central Asia. At Facebook she leads internal communication, training and awareness efforts for Facebook's security team.

---

**Justin Perkins, Stellar Technology Solutions Systems Administrator/ Game Master** Justin is a Systems Administrator for a Software as a Service provider that services charitable foundations and financial institutions. He is a self-described nerd with a sizable video and board game collection, a nostalgic child of the 90s who has no interest in growing up any time soon.

---

**Jon Portzline, Director of Content, SANS Institute** Jon has over 13 years of experience combining technology, education and training. He possesses dual Masters degrees in Information Sciences and Educational Technology. Using instructional design principles along with adult learning and behavior

change theory, he creates training that is both engaging and effective. His education and experience allow him to develop holistic security awareness programs that help each member of an organization protect themselves from cyber attacks.

---

**Janet Roberts, @janetr12, Global Head of Security Education & Awareness, Zurich Insurance** In Greek mythology, Icarus' father gave him a pair of wax wings to help him escape. Icarus was warned not to fly too low so the sea's dampness would not clog his wings, nor too high or the sun's heat would melt them. Icarus could not resist getting closer to the bright light of the sun. His wings melted and he fell to the sea where he drowned. Four years ago, Janet came to Zurich to build their first security awareness program. No one outside of information security knew who he was or understood what I was there to accomplish. Slowly, she built relationships and projects one layer at a time, strategically. In 2017, her GCISO told her no one in Zurich leadership would clear their calendar to meet with her. Today, she has total support and has been asked to take our training and learn more about the program. She's been to Switzerland and, yes, leaders at several levels had held time on their calendars for her. She can show you the stepping stones, how to maximize luck, what types of slides and metrics to use - such as the SANS Roadmap - and how to make sure you don't have wax wings when leadership finally recognizes you and the heat of the spotlight is on you and your program.

---

**Aika Sengirbay, Senior Information Security Engagement Lead, Autodesk**

Aika is the Senior Security Engagement Lead at Autodesk. She is building an awareness program that is driving a secure mindset amongst all employees by using security behavior testing and data analytics. Aika and her team are building security simulations, company-wide campaigns, and custom lab environments to drive effective learning of key security behaviors. These efforts are enabling successful changes to the security behaviors company-wide in Autodesk. Prior to Autodesk, Aika was a member of the Incident Response and Red Team team at Gap. She holds a BS in Journalism.

---

**John Smiley, Information Security Strategy Consultant, Highmark Health Solutions** Jon has been at HMHS for 7 years, 3 of which are with the Information Security & Risk Management organization. He is an original member of the Strategy Execution (Security Awareness) team, which has seen an expansion in the past year. Jon has worked on several awareness campaigns including phishing enhancements, cyber score, CSAM, team-by-team outreach, and educational course overhaul.

---

**Lance Spitzner, @lspitzner, Director, SANS Security Awareness**

Lance Spitzner has over 20 years of security experience in cyber threat research, security architecture and awareness and training. He helped pioneer the fields of deception and cyber intelligence with his creation honeynets and founding of the Honeynet Project. In addition, Lance has published three security books, consulted in over 25 countries, and helped over 350 organizations build awareness programs to manage their human risk. Lance is a frequent presenter, serial tweeter (@lspitzner) and works on numerous community security projects. Before information security, Mr. Spitzner served as an armor officer in the Army's Rapid Deployment Force and earned his MBA from the University of Illinois.

---

**Annette Stoica, @annette\_stoica, Security Awareness and Training Lead, Paddy Power Betfair**

Annette began her security professional career as the accountable person for physical security and have progressively moved into infosec compliance. With some adventures in specialties such as 3rd party assurance, internal audit, business continuity and access governance, in 2017 I have met my match and stepped into the world of security awareness.

---

**Jake Williams, @MalwareJake, Principal Instructor, Rendition Infosec; Senior Instructor, SANS Institute**

Jake Williams is an expert in secure network design, pen testing, incident response, forensics, and malware reverse engineering. Cleared by various government agencies, he regularly responds to cyber intrusions by state-sponsored actors in the financial, defense, aerospace, and healthcare sectors. He developed a cloud forensics course for the U.S. government, the pentesting tool Dropsmack, the anti-forensics tool ADD, and builds other custom solutions at his company, Rendition Infosec.

---