Day 01 - Thursday, December 3	
9:30 – 9:45 am	**Opening Remarks** Lance Spitzner, @lspitzner, Director, SANS Security Awareness
9:45– 10:00 am	**Overview of Slack** We introduce you to Slack and how we will be making the most of it for interaction, networking and learning more.
10:00 – 10:45 am	**Keynote:** A Human Hacker Playbook: Account Takeover in 1 Day & How to Stop Me Rachel Tobac, **@RachelTobac**, Hacker & CEO, SocialProof Security At the world's largest hacker conference, DEF CON, a journalist asked Rachel Tobac to take over as many of his accounts as she could -- live. By the end of the day, Rachel had wreaked havoc on 10+ accounts, siphoned thousands of dollars worth of points into accounts she controlled, disrupted his travel plans, and was even ready to shut his lights off. Rachel did all of this without ever once contacting the journalist. Learn the playbook Rachel used to social engineer her way into her target's accounts in one day, and what you can do to stop attackers like her in their tracks, even during a pandemic.
10:45 – 11:00 am	**Break**
	Track 01 *Learn about managing human cyber risk with a focus on communication, influence, engagement, and culture.* **Track 02** *Learn about managing human cyber risk with a focus on data, reporting metrics, automation, and technology.*
	Track 1 **May the Horse be With You** **Perry Carpenter,**Chief Evangelist & Strategy Officer, KnowBe4, Inc. **Lisa Plaggemier,** Chief Strategist, MediaPRO

11:00 – 11:30 am	This session will guide the audience through a journey to create Trojan Horses for the Mind. We'll explore how to powerfully use images, sound, emotion, and stories to move beyond simple information delivery and create something that engages learners at a primal level. We'll illustrate how this is done by looking at examples from popular culture (advertisements, movie clips, stock images, and podcasts), and then discussing how the principles from those examples can be implemented in a security awareness program. The session is vendor-agnostic and will focus on thought leadership and advice that will work with any vendor solution or home-grown program.
	<u>Track 2</u> **Behavior and Risk Selection** **Oz Alashe,** Founder and CEO, CybSafe **Dr. John Blythe,** Head of Behavioral Science, CPsychol Many awareness and behaviou change programs often fail because they try to do too much, they jump straight to interventions or they haven't explicitly defined their cyber security risks in behavioral terms. Incremental change and building on small successes are key to effective behavior change, both at an organizational and individual level. But, identifying and prioritising security behaviors is a challenge for many organizations. This engaging presentation will explain why it's important to focus on intervening intensively on a few behaviors. It will also show attendees how to identify and prioritise security behaviors for your organization. You will learn how to apply four criteria: • impact (on security risks), • likelihood of change, • behavioral spillover • and ease of measurement As well as how free, open source research tools like the Cyber Security Behavior Database (SebDB) can help you to prioritise behaviors for intervention efforts.
	<u>Track 1</u> **Cybercrime insights and mitigating strategies from Sub-saharan Africa - Zambia** **Freda Mwamba-Brazle**, Chief of Staff and Initiative Project Leader, Anthem **Mark Mondoka,** Founder, SuperVeg Farms In January 2019, Bank of Zambia, the central bank, issued a public notice that monies paid to a company, Heritage Coin, would be reimbursed. The monies obtained from the public were going to be used to purchase cryptocurrencies and guaranteed a 38% return.

11:30 – 12:00 pm	Throughout 2018, Heritage Coin was operating in the financial sector without a license from the Bank of Zambia or other sector regulators. The company was offering attractive returns, too good to be true, and word got around. Members of the public, with limited to no understanding of bitcoins, were attracted to the opportunity of making money. Some took their retirement monies and gave it all to Heritage Coin. Later on, the directors of Heritage Coin were convicted and the judgment was viewed as a lesson to perpetrators of money laundering crimes and emerging cyber fraud. Dr. Freda Mwamba Brazle and Mark Mondoka invite you to join our session to learn more about the context and layout of cybercrime in Zambia and Africa. We will provide insights on Zambia's experience with cybercrimes, how she is addressing opportunities and challenges associated with these crimes, and share tips and best practices for doing work in Zambia / Africa.
	<u>Track 2</u> **Empower Employees: Nudging by Numbers** **Pooja Srivastava,** Senior Manager, Genpact Mandatory trainings, videos, awareness sessions, newsletters, rewards; we did it all, but were missing an important component - proactive employee behavior towards a cyber secure culture. Based on existing data, we created a score card for users. Users can now look up their individual scores, discover the scoring rubric, and identify specific measures to undertake to reduce their risk score. This customized approach has been much more effective than a one-size-fits-all program. In this presentation, you'll learn about of sources of data collection, the logic for the scoring rubric, how data was calculated for the pilot group, the results and feedback, and the planned next steps.
12:00 – 1:00 pm	**Lunch:** *Take a break and network with your peers as we host small 10 person breakout room for you to virtually meet, eat and greet with each other.*
	<u>Track 1</u> **The Pen Is the Mightiest Weapon of All** **Steffanie AK Schilling,** Information Technology Marketing & Communications, Steris Picture this: After embarking on your arduous journey of mitigating human cyber risk, the summit is finally in sight. A culture of security is sweeping the organization, you have allies in far-reaching corners and enthusiastic support from the highest reaches of leadership. Can you feel that? Are you yearning for that excitement,

1:00 – 1:30 pm	pride, and sense of accomplishment? You might be saying, “Yes! I want that! But how do we get there?” Facts and figures do not change minds; emotions do. Emotions not only affect our decisions, but even more fundamentally they determine whether or not we engage. By weaving stories into presentations, you have the power to engage the hearts of those around you, and in turn, capture minds. Join SANS Cybersecurity Difference Maker and Innovator Steffanie Schilling as she makes you into a master storyteller who creates allies and inspires action. You’ll learn to create a compelling vision and purpose, capture audience attention, facilitate understanding and memory recall, build support, and strengthen commitment to your initiatives
	<u>Track 2</u> **Using Security Operations Center Metrics to Develop Awareness Programs** **Chris Crowley,** Consultant, Montace LLC Security Operations Centers (SOC) are immersed in the day-to-day defense of computer networks. The visibility they provide on issues is likely the best security vantage point any organization has. This presentation will show what capabilities a SOC should have, the metrics that should be collected and delivered within the SOC, and the usefulness of these metrics for general organizational and executive awareness. We’ll examine the importance of leveraging SOC information to showcase the daily efforts to improve security capability – efforts that unfortunately become less visible as that capability become more successful. Attendees can expect to learn what every SOC should aspire to be, how an SOC can better present its performance and accomplishments to the organization, and how the SOC's data can be used to target general awareness within the organization. The net effect is an effective collaboration between deeply technical efforts with efforts to improve human awareness.
	Workshops: Time to Choose! Each of these workshops will be an intense, hands-on event where you actually develop solutions you can apply to your own program. Select and attend one of the options below. Remember, slides and handouts from both workshops will be made available to everyone.

1:30 – 3:00 pm	**Facilitated Social Engineering Sessions: Build Your Own!** **Jen Fox,** Security Program Specialist, Domino's Pizza This workshop demonstrates a short and effective social engineering exercise. Participants will walk through an example of the exercise, creating their own pretexts based on information that organizations frequently leave exposed. Sample materials are included. Participants will learn how to present this group exercise and customize it for your organization and/or different attack types. We'll examine which types of presentations and activities work best in certain environments, then run through the presentation and exercises. We'll also look at key questions that need to be answered in order to make presentations effective. What types of security attacks are common or problematic to your organization? What does your organization need to protect? Why does social engineering work? What is the process? How are pretexts developed? How or why did these work? The workshop features group exercises that involve reviewing research packets (everyone gets the same set), determining how to approach getting credentials, and having someone download a file or getting access to a physical machine the groups will share their ideas on how to customize/build Internal information sources.

Your Program is Awesome, Now Prove It
Masha Sedova, Co-Founder and Chief Product Officer, Elevate Security

The inability to measure the effectiveness of security awareness training usually leads to these programs being deprioritized. For too long, we've accepted training completion and mock phishing data as a sufficient way to measure the impact of our interventions. But is the training you're conducting actually reducing security risk for your organization? That remains a black box for too many teams. There is a way forward, as security teams have installed tons of security tooling that can provide insight into how our employees are behaving. However, we often just leave these data on the cutting room floor. For example, most enterprises have an endpoint solution that prevents malware from being run on a machine. Known malware execution attempts are blocked and logged, and the security team moves on. But wait! That's pure security-behavior-change gold! Wouldn't it be great to see who was running that malware, and how many times it happens? With that information you would know which employees need more malware training and who is good to go. Further, it would show you where your malware hotspots are for the future just in case your existing endpoint solution doesn't catch everything. Practice defense in-depth now with more people security! This presentation will show attendees where to get the data, how to prioritize those data, and how to use them to effectively change behaviors within their organization.

3:00 – 3:15 pm	**Break**
3:15 – 3:45 pm	**<u>Track 1</u>** **Making Security Personal with Personas** **George Finney,** Chief Security Officer, Southern Methodist University This presentation will summarize the evolution of a security program over the course of 10 years to focus on creating culture change one relationship at a time. We'll look at a customized awareness program that used marketing personas, culture assessments, and personal interviews to meet the needs of a community, increase engagement, and change the organizational perspective from being compliance-focused to having a coaching mindset that meets individuals where they are and builds them up. After attending the session, participants should be able to create awareness personas based on the users in their environment, apply personas to tailor training outreach to multiple constituent groups, and use culture audits to identify strengths, weaknesses, and opportunities for outreach.
	<u>Track 2</u> **Automating Your Awareness Program** **Blair Adamson,** Cyber Influence - Senior Lead, Telstra Be honest; how much of your program is allocated to winning hearts and minds vs managing an Outlook distribution list and Excel spreadsheet? Your ambitions to keep growing your program are likely limited by the available resource or capacity within your team. But have you considered automating your program where it makes sense to do so? Over the past 18 months, Telstra's – Australia's largest telecommunications provider – Cyber Influence team has been using freely available automation tools in O365 to scale, optimise and now enhance their program; and the results speak for themselves.
3:45 – 4:00 pm	**Closing Remarks**

4:00 – 4:30 pm	**Coffee Chats with Cassie Clark –** Learn all about the world of growing, making, selecting and making the world's best coffee from self-professed coffee geek and guru. Sit back, turn on your video and interact with your peers from all over the world in this informal, relaxed and fun session.

Day 02 – Friday, December 4	
9:30 – 9:45 am	**Day 02 Kick-Off** Lance Spitzner, @lspitzner, Director, SANS Security Awareness
9:45 – 10:30 am	**Keynote: What 2020 teaches us about cyber security awareness, behavior and culture.** **Jessica Barker**, Founder & CEO, Cygenta The challenges of 2020 have brought with them many lessons. As security awareness professionals, what can we take from 2020 and apply in 2021 – and beyond – to make us more effective at planning, communicating and influencing cyber security in our organizations and communities? In this keynote, Dr Jessica Barker draws on research, case studies and reflections from the year to consider how we can help people better-protect themselves from an ever-evolving and often unseen threat.
10:30 – 10:45 am	**Break**
	Track 01 *Learn about managing human cyber risk with a focus on communication, influence, engagement, and culture.* **Track 02** *Learn about managing human cyber risk with a focus on data, reporting metrics, automation, and technology.*
10:45 –	**Track 1** **Comparing apples and oranges: how do we report on click rates when all our phishes are different?** **John Scott,** Head of Security Education, Cyber Security Division, Bank of England Phishing simulation companies promise massive reductions in click rates, but are those numbers reliable? How should you compare someone clicking on a badly spelled, obvious phish versus a spear phish? Can you draw any comparisons?

11:15 am	In this talk, John Scott will feed back to the SANS community on his MSc. thesis research into creating a useful and usable model for predicting the susceptibility of a given phish, based on the presence or absence of certain psychological triggers. He will discuss how he tested his models against his own organization, and will share the results.
	<u>Track 2</u> **Creating and Maintaining a Virtual Security Ambassador Program** **Nandita Bery,** Director, Security Engagement, Fareportal There are never enough awareness professionals to support the size of companies where we work. A growing trend is to establish a security ambassador program to leverage networks of employees to help spread security messaging, threat trends, news, and best practices. People get excited at first and sign up, but then you have to find ways to keep them engaged and coming back for more, because it's easy for them to get diverted by their "day jobs." How do you create excitement, so people want to join security awareness programs? How do you maintain that excitement past the honeymoon phase? What solid resource do you need to provide to keep them coming back? What reporting and metrics can be leveraged to demonstrate success? In this presentation, Nandita Bery will share success stories, failures, and lessons learned from creating new programs and transforming existing ones. She'll look at the key elements of a successful cyber champions program and how to avoid the pitfalls that lead to volunteer fatigue and boredom. Nandita will present strategy and specifics on how to roll out a program and support it with infrastructure such as a web portal, monthly calendars, speakers, activity kits, recognition, topic selection, reporting and metrics, and going global.
11:15 – 12:00 pm	**Plenary Session: Lightning Talks – Success Stories and Howtos for Virtual Engagement:** Don't blink! We will host five 8 minute lightening talks as people share their most successful virtual engagement tricks, stories and methods. **Madeline Howard**, Socio-Technical Engagement Manager, Cygenta **Dana Barka**, Senior Cybersecurity Awareness Program Lead, Kimberly-Clark **Jonelle Burns**, Firmwide Cybersecurity Education & Awareness, JPMorgan Chase & Co. **Melissa Misuraca**, Security Culture Lead, Kroll **Neaka Balloge**, Cybersecurity Awareness & Training Specialist, NYU Langone Health

12:00 – 1:00 pm	**Lunch:** *Take a break and network with your peers as we host small 10 person breakout room for you to virtually meet, eat and greet with each other.*
1:00 – 1:30 pm	**<u>Track 1</u>** **Meet a Culture: Security Awareness in Latin America** **Mora Durante Astrada,** Security Education and Awareness, Zurich Insurance Companies that operate in various countries sometimes face the challenge of the "one size fits all" approach: having a global concept or initiative and making it work everywhere. Security Awareness is no different. In today's talk, and under the umbrella of Zurich Insurance's global education and awareness program, we will see just how unique Latin America can be, and how aware we must be of certain particularities first, in order to successfully run a security awareness program –or campaign even! in the region. By the end of this talk, you will have gained some insight into Latin America, and what it takes to drive security awareness in the region: • Flexibility and adaptability (especially to political unrest –a sad fact of LatAm culture) • A bilingual person, preferably located in LatAm, or a very good translation service (Duolingo is not enough!) • The ability to create a sense of being a team and making decisions together (or they will make their own agenda and ignore yours)
	<u>Track 2</u> **How Non-Educators Educate Effectively: The Secret Recipe to Building Impactful Training Programs** **Dr. Mary Dziorny,** Senior Cybersecurity Consultant, Revolutionary Security As professionals in the security awareness space, we know that people join the domain from a variety of backgrounds that range from marketing and communications to cyber and technology. But rarely if ever are those tasked with designing training and education programs armed with a formal foundation in training or adult education. The SANS MGT433 course provides a comprehensive curriculum that covers all of the essential skills needed to develop and run an awareness program, including the Attention, Relevance, Confidence, Satisfaction (ARCS) model. However, there's a gap between where the ARCS model leaves off and the detailed planning and execution of training and education begins. This session will address that gap and provide program owners with a roadmap to create effective training and awareness activities. The trick is to design engagements that

	truly teach and motivate the audience. Attendees will learn nine critical components to designing effective instructional events and learning materials; how the instruction tools of Gagne and Briggs map with the ARCS model; and how to stimulate rapid, obstacle-free learning to achieve program goals and promote positive cyber behaviors. The remainder of the session will involve hands-on exercises to enable participants to work together and apply the design principles to the training and education challenges they face in their programs.
1:30 – 2:00 pm	**<u>Track 1</u>** **Culture Eats Strategy for Breakfast – Building Effective and Positive Behavioral Change** **Dean Chapman,** Director, People + Cyber Risk, Willis Towers Watson **Tom Finan,** Cyber Growth Leader, Willis Towers Watson This presentation will start by examining a fundamental problem, whether we want to hear it or not: most employees think cybersecurity is boring. How then can you achieve "buy in" and interest from those employees in a global business of over 45,000 personnel. Organizations with different cultures, a range of languages, and/or a largely displaced workforce first need to understand what the security awareness "problem" looks like. We continue to suffer incidents, and the traditional governance approach to people and training is not always effective. The underlying objective of this presentation is to better understand what the business cyber culture looks like and then develop a program to enhance positive behavioral change. The presenters will articulate the many challenges they've faced and the steps they've taken to address them. They'll provide a series of options to come to grips with defining what an effective training and awareness strategy looks like, supported by the collation of data (metrics) and a culture assessment framework Takeaways will include how to build a custom framework for the assessment of your people + cyber risk culture; how to identify and overcome the challenges you may face on this journey; and how to collect the data and metrics you need and ensure that they drive the development of a people-centric security strategy. Finally, we'll look at why your organizational culture is the key to everything we do and why it must be at the very heart of our activities. In short, culture eats strategy for breakfast.

2:00 – 2:30 pm	**Track 1** **The Human Firewall - A multi-faceted approach to combating Social engineering** **Janet Maranga**, Chief Information Security Officer, University of Nairobi Social engineering is rife with the malicious actors utilizing covert and unique techniques such as SIM SWAP fraud and mobile money compromise. This session will focus on the social engineering attack lifecycle and creative ways to train people on these attacks and consequently foster a security aware culture that can be replicated successfully in other organizations. Key take homes for the attendees would be how to effectively issue advisories, best practice guides and creation of awareness in a bid to deter and contain the criminal and fraudulent activities. They will also learn how to improve their vigilance in relation to social engineering hacks. Overall, the mindset of the human element has to be changed by continuous creative sensitization and generating awareness to the people who are in harm's way.
2:30 – 3:00 pm	**Track 1** **The Art of Ethical Influence: Shaping the Decisions of Leaders to Support Security Awareness** **Luke Barnes,** Managing Partner, Fidelis Risk Advisory Getting business leaders and employees to buy into security training and initiatives is not only hard but also sometimes discouraging, since it requires people to change existing behaviors. What if you had tactics to deliberately target and influence leaders and employees into taking action? Like the term “ethical hacking,” which implies that hacking can be done unethically, the word “influence” today has become something of an expletive. Yet, like hacking, influencing can be done ethically for the good of the organization. This presentation will explore the art of ethical influence in information security. InfoSec professionals often get bogged down on the technical side and forget that one of their most powerful tools to get things done is the ability to influence others. Attendees will learn actionable methodologies to ensure that motives and actions are ethical. They’ll also learn

	about the dynamics of an organizational climate, culture, and context; how to define a target audience, how to ascertain the proclivities and biases of leaders that contribute to their decision-making; how to craft messaging themes and connect business objectives to them; how to map out information conduits and channels and determine success criteria; and how to effectively and ethically influence targeted leaders and employees.
1:30 – 3:00 pm	**Workshop – Choose Your Own Adventure Video** **Jill Barclay,** Enterprise Cybersecurity Communications and Engagement Lead, CommonSpirit Health **Roman Aguirre,** Digital Media Producer, CommonSpirit Health Video is one of the best visual tools you can use to convey complex information in an engaging way. In this workshop, participants will dive into the creative process – choosing the topic, theme, key messages and call-to-action. We will take you through the steps from script to screen using your input and participation to help create a short video that everyone will be able use for their organizations. Every adventure is different, which one will you choose!
3:00 – 3:15 pm	**Break**
3:15 – 3:45 pm	**Track 1** **Initial Findings and Results from the Annual SANS Security Awareness Report** **Dan deBeaubien,** Director, SANS Security Awareness **Lance Spitzner,** @lspitzner, Director, SANS Security Awareness
3:45 – 4:00 pm	**Closing Remarks**

Speaker Biographies

Blair Adamson
Blair leads Telstra's Cyber Influence team and has extensive experience across government, intelligence and private industry, having worked in various senior management advisory roles in the Department of Defence, the Australian Signals Directorate and the SANS Institute. Blair believes that cyber security is as much about people as it is about technology and, as Telstra's Cyber Influence Manager, sets the direction on delivering innovative programmes designed to foster a strong cyber security culture. Blair was also responsible for leading the application of Telstra's Five Knows of Cyber Security across the enterprise.

Roman Aguirre
Roman is the Digital Media Producer for CommonSpirit Health's Information Technology and Digital Team. Roman brings his 15+ years of experience from Independent Filmmaking to corporate communications, creating low cost and effect communications.

Mora Durante Astrada
Mora Durante Astrada has been leading security awareness in LatAm for Zurich for 6 years, first working in partnership with Zurich Security Education & Awareness (SEA) but reporting into various LatAm managers, and then, in 2019, coming full time to a combined global & regional role on the SEA team reporting to Janet Roberts. Mora is a member of a 100% virtual global team, but located in Buenos Aires, Argentina. She is fluent in Spanish, Portuguese, French and English and is the only person doing full time security awareness work in LatAm.

Oz Alashe
Oz Alashe MBE is CEO and Founder at CybSafe, a British cyber security and data analytics tech company based in London. A former UK Special Forces Lieutenant Colonel, Oz is focused on making society more secure by helping organizations address the human aspect of cyber security.He has extensive experience and understanding in the areas of intelligence insight, complex human networks, and human cyber risk and resilience. He's also passionate about reducing societal threats to stability and security by making the most of opportunities presented through advancements in technology.Oz was made an MBE in 2010 for his personal leadership in the most complex of conflict environments. He is an Expert Fellow at The Security, Privacy, Identity and Trust Engagement NetworkPlus (SPRITE+) and at the Royal United Services Institute (RUSI). He is also a member of the SANS Security Awareness Summit Advisory Board.

Jill Barclay
Jill Barclay is the Cybersecurity Awareness and Communications Lead for CommonSpirit Health. Jill is best known for her creative communications campaigns and award-winning cybersecurity awareness videos. Prior to landing in Cybersecurity, Jill specialized in marketing and consumer engagement for major healthcare networks across the U.S. Her experience, along with her ability to connect with a variety of audiences, has helped move employees toward a better understanding of safer cybersecurity practices.

Dr. Jessica Barker
Dr Jessica Barker is an award-winning global leader in the human side of cyber security. She is Co-Founder and co-CEO of Cygenta, where she follows her passion of positively influencing cyber security awareness, behavior and culture in organizations around the world. She has delivered cyber security awareness sessions to over 40,000 people in over 23 countries. Jessica has been named one of the top 20 most influential women in cyber security in the UK and is the Chair of ClubCISO. She is a popular keynote speaker, including keynoting RSA San Francisco in 2020. Jessica is the go-to cyber security expert for many media outlets, appearing on BBC News, Sky News, Channel 4 News, BBC radio and much more. In September 2020, Jessica's book Confident Cyber Security was published by Kogan Page and became a number one Amazon best-seller within hours of publication.

Luke Barnes
Luke is an information security advisor, a long-time student of leadership, and a native of Austin, Texas. With over fifteen total (8 active & 7 reserves) years of service as a Marine Corps officer in both conventional and special operations units, he is trained in the art of combat leadership, high-stakes decision making, and information warfare. He holds an MBA with GCIH, GCED, GSNA, and PMP certifications.

Nandita Bery
As a technology professional with over 25 years in the software development world, Nandita has insider knowledge of the security world, which she has been applying in creative ways to raise awareness and understanding for both technical people and end users. She has established multi-faceted awareness programs from the ground up in various industries including media, entertainment, banking and healthcare.

Dr. John Blythe
Dr. John Blythe is Head of Behavioral Science at CybSafe and a Chartered Psychologist with the British Psychological Society. He has a PhD in psychology and over eight years' experience in researching the connections between people and cyber security. John is an Honorary Research Fellow at the Dawes Centre for Future Crime at UCL and has held positions at the Department for Digital, Culture, Media, and Sport (DCMS) in UK Government and the Centre for Behavior Change.

Dr. Freda Mwamba-Brazle
Active on two continents, Dr. Freda Mwamba-Brazle is a vastly experienced Zambian-American problem solver and change catalyst who uses her collaborative skills and network to drive community impact. Her purpose is to pursue and explore avenues to change and expand mindsets that will drive innovative growth for leaders in Africa and the United States.

Dr. Mwamba-Brazle brings to this mission more than 30 years of experience driving business transformation and collaborative culture change using data and risk management practices to exceed performance and organizational objectives. A specialty skill of hers is driving transformational change within organizations. Another forte is facilitating accelerated change

by utilizing disciplined process management methodologies, influence techniques and governance strategies. These are transferrable skills and expertise that she has developed working in executive positions in the healthcare, financial, consulting, manufacturing and nonprofit sectors.

In the nonprofit field, Dr. Mwamba-Brazle has successfully applied some of these strategies as Zambia's first Country Representative for the Unites States Attorney's General Alliance Africa (AGA Africa). She leads teams of American lawyers and criminal justice experts to Zambia, facilitating training and capacity building to combat transnational crimes such as money laundering, wildlife trafficking, human trafficking, and cybercrimes.

Dr. Mwamba-Brazle's involvement in engendering growth on her continent of birth goes beyond empowering Zambia's legal system. A 2006 alumna of Leadership Atlanta, the experience inspired her to establish her own nonprofit, Zambian Promoting Leadership in America (ZLA), in 2014. Its focus is to address leadership gaps focused on the youth across industries. Her other board experiences are from the YWCA Atlanta, AID Atlanta and Peak Performance Basketball. In addition, she founded Innovatus Zambia, drawing from her African roots, developed in corporate America, to address complex business opportunities and challenges. Her engagement on the continent also includes advising on the diaspora role on sustainable development.

In her fulltime role, Dr. Mwamba-Brazle serves as Chief of Staff and Initiative Project Leader for health care insurance provider Anthem. She has spent over 10 years there and her responsibilities include leading and executing enterprise projects that create shareholder value and overseeing the Enterprise Center of Excellence. Among the projects under her eyes are initiatives for 1) Future of Work 2) Electronic Medical Records data integration with providers, and 3) reducing medical costs of the top 1% members who drive 30-50% of cost of care.

Dr. Mwamba-Brazle's previous executive experience includes senior vice president positions, from 2002 to 2009, at Bank of America where she featured as a "world class leader" in the bank's annual report. As the Bank's Senior Vice President, Corporate Audit Director, Global Risk, she led teams of Six Sigma Master Black Belts (MBBs) and Black Belts (BBs) focused on driving process improvements and integrating Six Sigma methodology and tools into Audit. Earlier, as Senior Manager, Finance and Operations Business Solutions at Arthur Andersen Business Consulting in Atlanta, Dr. Mwamba-Brazle managed a team of consultants in analyzing and improving financial and operational business processes. She also served as Director of Quality for General Electric Corporation at various locations in the United States and Europe, and worked for Coca Cola in Greenwich, Connecticut. Overall, her description by managers and peers is "creative with extraordinary leadership skills".

Dr. Mwamba-Brazle graduated from Pace University in New York City with a BBA in Management Information Systems and a Master of Science in Accounting. She is a Certified Public Accountant, Master Black Belt in Lean Six Sigma and earned her Doctorate of Business Administration from the University of Maryland Global Campus. Her publication in Muma Business Review is on Big Data in Care Management for Healthcare Systems and is titled "What

is the impact of case management on medical cost reduction in healthcare insurance companies?"

Perry Carpenter @PerryCarpenter
Perry Carpenter (author of, "Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors" from Wiley Publishing) currently serves as Chief Evangelist & Strategy Officer for KnowBe4. Previously, Perry led security awareness, security culture management, and anti-phishing behavior management research at Gartner Research.

Dean Chapman
A Director and Consultant in our GB Cyber Team, Dean joined from the Royal Air Force where he was employed across the MoD cyber stream, notably as the Head of Cyber Threat Awareness. Specializing in People + Cyber Risk, Dean builds and manages cyber security training and awareness strategies.

Chris Crowley @CCrowMontance
Mr. Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area focusing on effective computer network defense. His work experience includes penetration testing, security operations, incident response, and forensic analysis. Mr. Crowley is a Senior Instructor and the course author for SANS Management 517 - Managing Security Operations and SANS Management 535 - Incident Response Team Management. He holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GMOB, GASF, GREM, GXPN and CISSP certifications. His teaching experience includes FOR585, MGT517, MGT535, SEC401, SEC503, SEC504, SEC560, SEC575, and SEC580; Apache web server administration and configuration; and shell programming.

Dr. Mary Dziorny
Mary Dziorny is a Senior Cybersecurity Consultant with over 10 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. Mary began her career in IT and technical training at Ericsson, Inc. and Richland Computer Training Institute. From there, she moved to The University of Texas at Dallas where she served as the University's Educational Technology Coordinator for 5 years before moving into the Information Security Office. There she created the University's first security awareness program, comprised of 11 security awareness classes in two certificate programs in addition to numerous outreach activities aimed at students, faculty, and staff. Six years later, she left the University to create the first comprehensive security awareness program for Southwest Airlines, encompassing 67,000 employees in all job roles across 100 locations in 7 countries. In addition to her industry experience, Mary is also an experienced teacher and instructor with over 10 years of online teaching experience and more than 20 years of experience as a classroom instructor. She has

taught for The University of Texas at Dallas, University of North Texas, and currently teaches for Texas A&M- Commerce. Her academic research focuses on online education, games and simulations, and working with students with dyslexia. Mary holds a Bachelor of Music with a Professional Education minor, a Master of Science in Applied Technology Teaching and Learning, and a Doctor of Philosophy in Educational Computing from the University of North Texas. She also holds Security+ and GSEC certifications.

Tom Finan

Tom Finan is a Cyber Growth Leader within Willis Towers Watson's FINEX Cyber/E&O Practice. In this role, Tom advances the company's integrated approach to cybersecurity across all aspects of people, capital, and technology risk. Tom previously worked as the Chief Strategy Officer of Ark Network Security Solutions. He also served as Senior Cybersecurity Strategist and Counsel with the Department of Homeland Security's National Protection and Programs Directorate. While at DHS, Tom established and led the agency's cybersecurity insurance initiative in support of implementation of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." To advance that effort, he created DHS' Cyber Incident Data and Analysis Working Group (CIDAWG), a private-public engagement forum that examined how a cyber incident data repository could help meet the information and analysis requirements of the insurance industry and technical cybersecurity professionals. Tom previously served as the Staff Director and Counsel for the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment with the U.S. House Committee on Homeland Security. During his time with the Committee, he authored two major reports that informed many of the statutory provisions that he helped develop for Title V of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) and the Reducing Over-Classification Act of 2010 (P.L. 111-258). Tom is a former Assistant General Counsel at the FBI. He has also worked in private litigation practice. Tom earned his J.D. from the University of Minnesota Law School and B.A. from the University of Virginia.

George Finney

George is a CISO that believes that people are the key to solving our cybersecurity challenges. Because of his passion for education, George teaches cybersecurity at SMU and is the author of several cybersecurity books including the upcoming book Well Aware: Master The Nine Cybersecurity Habits To Protect Your Future.

Jen Fox @J_Fox

Jen Fox holds the DEF CON 23 Social Engineering Capture-The-Flag black badge. As a security consultant, she provided social engineering tests, awareness training, risk management, and compliance services to clients. She now helps Domino's Pizza to secure its brand and is a two-time guest editor for the SANS OUCH! newsletter.

Mark Mondoka

Mark Mondoka helps startups take the guesswork out of building their ventures. He has supported over a hundred startups in launching their businesses. He focuses on educating people on how to create economic value and leverage technology in the process.

He is the founder of VENIVI, a technology strategy organization supporting enterprise and small, medium businesses. He is also the founder of SuperVeg Farms that grows and supplies microgreens to hotels and restaurants fifty-two weeks a year.
He is actively involved in the UNCDF Fintech4U startup accelerator program in Lusaka and Bongo Hive Innovation Hub where he teaches design thinking and produces learning content. He is also a board director for the Impact One Initiative, which focuses on supporting literacy in community schools in low-income communities.
He worked as a Technical Account Manager at Microsoft supporting banking, mining, tax authorities, and telecommunications enterprise accounts across east and southern Africa in his previous experience. He worked at IBM as a Service Manager and Transformational Projects Manager. He also worked at Airtel and Zain in Lusaka as a Product Manager, Technology Projects & Governance Manager. He shipped multiple mobile technology solutions used by millions of Zambians.

Lisa Plaggemier @LisaPlaggemier
Lisa Plaggemier is Chief Strategist at MediaPRO. Lisa is a trailblazer in training and awareness. Lisa uses her diverse experience to fuel an innovative approach that engages learners and influences behavior. Lisa's background includes International Marketing with Ford Motor Company, Director of Security Culture and Risk for CDK Global, and Chief Evangelist at InfoSec.

Steffanie AK Schilling @SAKSchilling
Steffanie AK Schilling believes in empowering individuals to better protect their data and the lives entangled within. A SANS Cyber Security Difference Maker and Innovator, she marries a keen understanding of human behavior with the technical of cyber. Steffanie holds a B.S. in Marketing and B.A. Communication from Miami University.

John Scott
John Scott is the Head of Security Education, Cyber Security Division, at the Bank of England. For nearly 30 years, he has been working in IT Training and Management not only teaching, but also designing and producing materials for both face-to-face training and e-learning. John specializes in security awareness and cultural change and can be found speaking internationally on the subject. He is an instructor for SANS MGT433: Managing Human Risk: Mature Security Awareness Programs

Masha Sedova @modMasha
Masha Sedova is the co-founder of Elevate Security and is an industry-recognized expert in measuring and influencing employee-risk. In her previous role, Masha built a world-renowned security culture program at Salesforce. Masha sat on the Board of the National Cyber Security Alliance and continues to share her expertise with the broader community.

Pooja Srivastava

Pooja is part of the cyber security awareness and training team at Genpact, a 90,000+ global organization. Moving from training to security awareness domain, Pooja has led several projects in driving right security behaviors. She has a post graduate diploma in computers and is an Oracle Certified Associate. She is also ISO 27001 LA, LI and CISM certified. At present she is helping Genpact Information Security team to look at the problem from a people perspective. She has also worked with Barclays PLC in the past.