SANS European Security Awareness Summit 2016

London 11th November, 2016
Chairman: Lance Spitzner

#SecAwareSummit @SecureTheHuman

securingthehuman.sans.org

info@securingthehuman.org

SANS EUROPEAN SECURITY AWARENESS SUMMIT 2016

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:
https://www.chathamhouse.org/about/chatham-house-rule.

EVENT NOTES

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

10TH NOVEMBER

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.

SANS EUROPEAN SECURITY AWARENESS SUMMIT 2016

FRIDAY 11 NOVEMBER
8:00–10:40 AM

8:00 – 8:45 am	**REGISTRATION & COFFEE**
8:45 – 9:00 am	**Opening Remarks** Lance Spitzer, *Research & Community Director, SANS Securing The Human*
9:00 – 9:20 am	**Roundtable Networking and Introductions** We know that the conversations among peers and the connections forged during these events are just as valuable as the case studies presented by leading security awareness practitioners. Kick off your day by getting to know the other attendees seated at your table and begin forging those meaningful connections and exchanging ideas right away.
9:20 – 10:00am	**Using Gamification to Transform Security Awareness** Human enabled exploitation is one of the most prevalent and dangerous security risks today. There is no easy patch to secure people. Securing humans requires behavioral change. Learn how to leverage behavioral psychology and gamification principles to drive positive, effective and measurable security engagement and behavior. We will discuss how harnessing the power of intrinsic and extrinsic motivations can help drive behavioral change. We will then discuss Salesforce security awareness program's application of these principles, resultant metrics, and some takeaways that will help you build your own program. Masha Sedova
10:00 – 10:40am	**Awareness with Impact:** **Making sure your awareness materials are seen, understood and acted on.** We all think that cybersecurity awareness is vitally important, and are dedicated to making our companies safer. But for our colleagues, our passion is just one more thing that they have to get through to be able to do their jobs. So how do we show them that security awareness is not just important, but also attractive? How do we make our materials stand out from the crowd? We'll look at 3 areas. In each one, we'll cover a bite-sized introduction to the field, identify an expert you can follow, a book or other resource you can read and a two-minute exercise you can carry out each day to improve your skills in this area. • Social Learning • Graphic Design • Influencing behaviour like a marketer John Scott, *Bank of England, Head of Information Security Education*

SANS EUROPEAN SECURITY AWARENESS SUMMIT 2016

FRIDAY 11 NOVEMBER
10:40 AM–2:20 PM

10:40 – 11:10 am	**NETWORKING BREAK**
11:10 am – 12:10 pm	**360 Lightning Talks** In this exciting hour, six 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! • Chris Boyd: *Tackling CFO Fraud* • Leron Zinatullin: *The Psychology of Information Security Culture* • Ido Naor: *Social Media Malware: Tag Me If You Can* • David Rimmer: *Lessons I learned from my dog* • Martine van de Merwe: *Improve your results by applying accelerated learning* • Dr. Simon Parkin: *Top Awareness Challenges and Solutions for SMEs*
12:10 – 1:40 pm	**NETWORKING LUNCHEON & SHOW-N-TELL**
1:40 – 2:20 pm	**But, I'm not a target!:** **How to combat the hidden bias that kills your awareness programme** One of the effective tools we have is to tie a desired action, a policy, or a behaviour to a real risk to the person or the organisation. Once we communicate that connection, people often agree with the risks but keep doing the same risky things they were doing before. Why? Do they not believe us? Do they not believe the risks? Do they believe something else? Using recent studies by Georgetown University researchers for NASA, I will explore "Near-Miss Bias" and how it can impact how the average user perceives risky behaviour in their day-to-day activities, and how managers and decision-makers make risky decisions that impact your programme. Most importantly, I will give you the techniques to slice through this stubborn bias so that you can make a lasting impact on your organisation. Jordan Schroeder

SANS EUROPEAN SECURITY AWARENESS SUMMIT 2016

FRIDAY 11 NOVEMBER
2:20–5:00 PM

2:20 – 3:00 pm	**Building and launching the first iteration of your high-impact security culture program** Advancing from sporadic "security awareness training" efforts to a full-fledged security culture program may seem like a daunting task for a company of any size. How do you achieve C-level buy-in and funding? Where do you go from there to determine the maturity, actual needs, and appropriate engagement strategies for your company and its employees? And at the end of the day, how do you measure if your hard work has really caused the boost in risk resilience you – no doubt – will be asked to prove to ensure that the program lives on? In my talk, I'll provide you with a host of hands-on tips and tricks on what to do – and what to avoid – in your first attempt on creating an effective, structured, and measurable security culture program, based on my own hard-earned lessons from doing exactly this for one of the largest companies in the Norwegian Finance & Insurance sector. Magnus Solberg, *Security Manager, Storebrand Group ASA*
3:00 – 3:30 pm	**NETWORKING BREAK**
3:30 – 4:10 pm	**Passwords Like You Never Knew Them Before!** Passwords. No other security feature is used more often with more people on a daily basis. Everybody has an opinion about them; how to make them, use them, change them - and all the problems they are causing us. In this talk Per will show you some of the mistakes we've done with passwords since the 80's, and what we are still doing wrong today. More importantly he will show you how we can improve password usability, while also maintaining and improving your security. You have never heard a more passionate talk about passwords! Per Thorsheim, Founder Passwords Con
4:10 – 4:50pm	**Show-n-Tell Winners / Discussion**
4:50 – 5:00pm	**Closing Remarks** Lance Spitzner

SANS EUROPEAN SECURITY AWARENESS SUMMIT 2016

FRIDAY 11 NOVEMBER BIOGRAPHIES

JOHN SCOTT

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. John has been a software trainer for most of his career, meaning he has a strongly honed sense of the frustrations normal people feel when faced with new technology – training is, after all, mostly watching people make mistakes because of unfamiliarity. (And then helping them!) Passionate about explaining the 'why?' as well as the 'how?' and a strong advocate that if it doesn't look pretty (or at least professional) people will gloss over it.

MAGNUS SOLBERG:

I'm an infosec evangelist with a deep-rooted holistic approach to tackling the threats of our digital age. Working in IT most of my life, the last decade has been dedicated to information security in the private and public sectors: First as a techie and security architect, but for the last five years focusing on the "softer" aspects such as governance and ISMS's, policy frameworks, standards & compliance – and building security awareness and culture through training and motivation. Although a tech nerd at heart, I'm convinced that information security begins and ends with people, and love to spread the good word whether from the stage or over some craft beer! After being a consultant for most of my career, I'm now happily employed with the Storebrand Group, Norway's leading insurance and pension fund provider. Certifications: CISSP, CISM, ISO 27001 LI, ISO 27001 PA, ISO 27005 RM, ISO 22301 BCMF, CCSK

CHRIS BOYD

Malware Intelligence Analyst (Malwarebytes) Chris is a 7 time Microsoft MVP in Consumer Security and former Director of Research for FaceTime Security Labs. He has presented at RSA, Rootcon, VB, IRISSCON, and SecTor, and has been thanked by Google for his contributions to responsible disclosure in their Hall of Fame. Chris has been credited with finding the first rootkit in an IM hijack, the first rogue web browser installing without consent, and the first DIY Twitter Botnet kit. His work was also referenced in the People of the State of New York v. Direct Revenue, LLC.

SANS EUROPEAN SECURITY AWARENESS SUMMIT 2016

FRIDAY 11 NOVEMBER BIOGRAPHIES

LERON ZINATULLIN

(zinatullin.com) is an experienced risk consultant, specialising in cyber security strategy, management and delivery. He has led large scale, global, high value security transformation projects with a view to improving cost performance and supporting business strategy. He has extensive knowledge and practical experience in solving information security, privacy and architectural issues across multiple industry sectors. Leron is the author of The Psychology of Information Security book

SIMON PARKIN

Simon Parkin is a Senior Research Associate in the Information Security Research Group at UCL. His research has focused on employee security behaviours and attitudes within organisations, including use of security technologies and comprehension of policies. Parkin was a member of the Innovation Team at HP Enterprise Security Services until mid-2012, and a Research Associate at Newcastle University from 2007 to 2011. Parkin is currently collaborating with small organisations to understand related security investment and security skills challenges.

JORDAN SCHROEDER

Jordan is a speaker, author, and security awareness blogger on gophishyourself.co.uk. He also designed and runs a fully automated phishing engine: SelfPhish. He has worked onsite with companies in the US, Canada, and the UK to implement and improve their security awareness programmes with teaching techniques he honed as an adult educator. His career has spanned the Canadian Coast Guard, stage acting, and running his own department at a technical college. These varied experiences give him unique insight into the challenges of teaching security awareness. He is kept busy in his free time by moderating the Security. StackExchange.com Q&A forum, and writing tabletop roleplaying game adventures.

SANS EUROPEAN SECURITY AWARENESS SUMMIT 2016

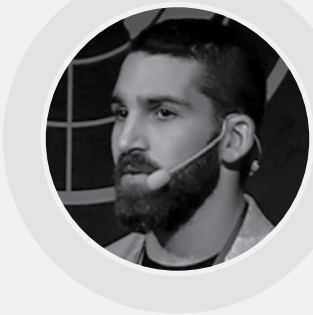
FRIDAY 11 NOVEMBER
BIOGRAPHIES

MARTINE VAN DE MERWE

trainer security awareness in healthcare / IT auditor, founder PrivacyLab. Martine believes privacy is essential to freedom. The more someone knows about you, the more power he has over you. People are key to ensure privacy. Although you can have a lot of technical controls, if the people don't get it, it won't work. That's why Martine decided in 2014 to focus on security awareness in healthcare and started her own business PrivacyLab. The PrivacyLab approach focuses on engaging training methods so people really get involved in information security. With some decades of experience in IT advisory and IT auditing Martine knows what she's talking about. Martine is co-founder of the Dutch security awareness community (with over 170 members) serving both the SANS Securing the Human community in the Netherlands and the Dutch Security Culture Framework User Group as well as any other security awareness professional who wants to be inspired by knowledge sharing colleagues.

DAVID RIMMER

Currently leading the European security function for Equifax, David has been involved in security leadership roles (focussing on culture change and security engagement) in public and private sector roles over the past 10 years. Contributing to industry programmes such as The Analogies Project, his passion is for making security transparent to the business and to employees – promoting common sense over Cyber jargon.



IDO NAOR

Ido is a senior security researcher at the Global Research & Analysis Team (GReAT), Kaspersky Lab. He joined Kaspersky two years ago and is leading the regional research in Israel. Ido specializes in malware analysis, penetration testing and software reverse engineering and has been credited for his work by major enterprises such as: Google, Facebook, Linkedin, Alibaba and more. Aside from research, Ido is a martial arts expert and a father of two daughters.

SANS EUROPEAN SECURITY AWARENESS SUMMIT 2016

FRIDAY 11 NOVEMBER BIOGRAPHIES

PER THORSHEIM

Founder of PasswordsCon

Per Thorsheim is the founder of PasswordsCon.org, the world's first & only conference dedicated to the most common computer challenge in the world - passwords. The conference seeks to improve the security as well as the usability of anything you could possibly connect with passwords, pins, multi-factor authentication and biometrics. He claims to know your next password.

MASHA SEDVOA

Masha Sedova is the Senior Director of Trust Engagement at Salesforce. She has built a team that drives a secure mindset amongst all employees using user security behavior testing and data analytics paired with elements of gamification and positive psychology. The scope of her work runs the gambit of general awareness such as phishing and reporting activity to secure engineering practices by developers and engineers. She and her team have built security simulations, company-wide competitions, and custom lab environments to drive effective learning of vital security behaviors. Her efforts have culminated in a security program that is altering the way Salesforce's employees, customers, partners, and large corporations approach security.

Prior to her work with Salesforce, Masha was the principal founder of Dymera Strategies Consulting where she conducted social engineering and security awareness training to international companies and government agencies based on tools, techniques, and methods of prominent cyber warfare actors. Masha has also worked for Northrop Grumman and BAE Systems as a cyber threat researcher.