



AGENDA*

8:00 a.m.	Registration and Breakfast	
8:30 a.m.	<p>CNI Security Benefits from SRE: How-to Guide for Success Sponsored by Amazon Web Services</p> <p>Gregory Herrmann, Senior Partner Security Strategist, Amazon Web Services Alexander O'Brien, DevOps Engineer, 6point6</p> <p>The goals of SRE and CNI security are well-aligned with reliability and protection. Both aim to avoid as many incidents as possible by creating resilient secure systems. SRE practices and tools can help complement security objectives. Join this 6point6 and AWS session to find out how you can succeed with SRE and CNI security.</p>	<p>Find It Before They Do: Being Proactive about IoT Risk Mitigation Sponsored by Keysight Technologies</p> <p>Scott Register, VP Security Solutions, Keysight Technologies</p> <p>In this session, we will discuss the techniques for understanding and coping with the increase in attack surfaces introduced by IoT. We'll touch on device-specific techniques, such as protocol fuzzing and vulnerability assessment, validation of surrounding defensive systems and the applicability of digital twins in validation scenarios.</p>
9:40 a.m.	Welcome Remarks James C. Packer, Board Member, (ISC) ²	
9:45 a.m.	Keynote Presentation National Cyber Security Centre	
10:40 a.m.	(ISC)² London Chapter Update Liz Banbury, CISSP, President, (ISC) ² London Chapter and CISO, Hiscox	
11:00 a.m.	Networking and Exhibit Hall	

*Subject to change.



<p>11:30 a.m.</p>	<p>Security Awareness: Planning and Delivering a Successful Program</p> <p>Laurie-Anne Bourdain, CISSP, Data Protection Officer & Awareness Program Manager, Isabel Group</p> <p>Humans are the weakest link in information security. Building their awareness and training them to detect and respond appropriately to threats should be among the top priorities of every CISO and organization. Find out how to define your training and awareness needs; identify and plan awareness-raising and knowledge-building activities; and put best practices in place now.</p>	<p>AWS, Azure or GCP Security?</p> <p>Paul Schwarzenberger, MSc, CISSP, CCSP, Cloud Security Specialist, Celidor</p> <p>Which of the three cloud platforms comes out on top? We'll look at everyday use cases and live demonstrations to compare their security architectures and features.</p> <p>Identity: Cloud customers create multiple AWS accounts, Azure subscriptions and GCP projects. How should a centralized source of identity be architected?</p> <p>Private Networking: Security-conscious cloud customers use private networking as a defense in depth strategy. How can we apply this approach in cloud services like storage or serverless functions, which are internet-facing by default?</p> <p>Content Delivery Network: How can we present web applications to global users with low latency and high levels of security?</p>
-------------------	---	---



<p>12:30 p.m.</p>	<p>How Should We Deal with Users Causing Cyber Breaches?</p> <p>Dave Cartwright, Head of IT Risk and Security, Standard Bank ICS</p> <p>People make mistakes. We can train them, write policies and procedures, and run phishing tests, but our organizations will still face human-induced cyber risk because eventually someone will do something they shouldn't. How should we react when this happens? Resign to the fact that we can't stop all attacks all the time and brush it off as "one of those things?" Go zero-tolerance on a cyber error and call it gross misconduct by default? Can we, for that matter, even have a set policy on how we deal with users when something goes wrong? We'll explore answers to these questions and more.</p>	<p>Supply Chain: Is It the Tail that Wags the Dog?</p> <p>Jon France, CISSP, CISO, (ISC)²</p> <p>We all know supply chains are getting longer and more complex as the world relies more heavily on them. When someone in the chain catches a cold, we all sneeze. Industries and organizations view supply chains as a way of reducing costs, building efficiency and getting access to goods and services - cybersecurity professionals view them as another threat surface. In this session, we'll explore the latest developments and impacts on supply chains and how they've changed cybersecurity practices in the face of COVID.</p>
<p>1:20 p.m.</p>	<p>Lunch and Exhibit Hall Lunch sponsored by ZeroFox</p>	



<p>2:00 p.m.</p>	<p>Panel: Cyber Resiliency and the Power of a Diverse Ecosystem</p> <p><u>Panelists:</u></p> <p>Andrew Elliot, Deputy Director Cyber Security Innovation and Skills, DCMS</p> <p>Dr. Sanjana Mehta, Advocacy Director, (ISC)²</p> <p>Laura Wellstead, President, Women in CyberSecurity (WiCyS) and Co-Founder, cyberexperts</p> <p>Richard Yorke, Managing Director, Cyber Cheltenham (CyNam); Chair, Co-Founder and Director, UKC3; Co-Founder & CEO, Deep3 Software</p> <p>In this session, you'll hear from leading cyber experts as they discuss what a diverse ecosystem means, who must be involved in this "all-hands-on-deck" inclusion effort, and how we must build diversity, equity and inclusion efforts into new and deeper partnerships to ensure a more inclusive cyber profession and a safer cyber world.</p>	<p>Crowdsource Security: For Better or For Worse?</p> <p>Alex Haynes, CISSP, CISO, CDL</p> <p>As crowdsourced security approaches its 10th anniversary, we'll look at how it has changed the pentesting landscape. We'll discuss the pros and cons of crowdsourced security compared to traditional pentesting and where it can be best leveraged within your business, if at all. We'll also dive into the recent weaponization of crowdsourced security in the Ukraine conflict as an example of how it can go wrong and the collateral damage it can cause to innocent bystanders.</p>
------------------	--	---



3:05 p.m.	To Be Confirmed	<p>Ransomware Incidents: How to Prepare, How to Respond</p> <p>Joseph Carson, CISSP, Chief Security Scientist and Advisory CISO, Delinea</p> <p>With cyberattacks on the rise, understanding ransomware is key to strengthening your organization's defenses. We'll look at a real-world ransomware attack — how it progressed from the initial credential compromise to escalated privileges, exfiltrated data and ultimately ransomware deployment and ransom demand. Watch a step-by-step example of how to effectively respond when an attack is detected; gather evidence to craft a contextual response that remediates the attack; and better secure your environment against future attacks.</p>
4:00	Networking and Exhibit Hall	
4:30 p.m.	<p>(ISC)² Insights</p> <p>Clar Rosso, CEO, (ISC)² Jon France, CISSP, CISO, (ISC)² Yiannis Pavlosoglou, CISSP, Board Secretary, (ISC)²</p> <p>As we wind down for the day with appetizers and drinks, join (ISC)² CEO Clar Rosso and CISO Jon France along with Board Secretary Yiannis Pavlosoglou as they take your questions about what's going on inside (ISC)², what's going on in the world of cybersecurity, industry trends and what it all means for (ISC)² and the way the association is supporting its members.</p>	
5:30 p.m.	Conference Concludes	