












Agenda & Speakers

10.00 – 10.10	<p>Welcome and Introduction Siân John & Lesley Kipling</p> <div data-bbox="300 465 587 831"></div> <div data-bbox="300 835 587 987"><p>Siân John Director of Security Business Development and Strategic Growth</p></div> <div data-bbox="300 1032 587 1339"></div> <div data-bbox="300 1344 587 1417"><p>Lesley Kipling Chief Security Advisor</p></div> <p>Siân John MBE is Director of Security Business Development and Strategic Growth at Microsoft. She leads a team focusing on developing opportunities for Microsoft to deliver new security, compliance, and identity offerings to market. Siân is a Fellow of the Chartered Institute of Information Security and was awarded an MBE in the Queen's 2018 New Year's Honours List for services to Cybersecurity.</p> <p>Previously lead investigator for Microsoft's detection and response team (DART), Lesley Kipling has spent more than 17 years responding to our customers' largest and most impactful cybersecurity incidents. As Chief Cybersecurity Advisor, she now provides customers, partners, and agencies around the globe with deep insights into how and why security incidents happen, how to harden defenses and more importantly, how to automate response and contain attacks with the power of the cloud and machine learning. She holds a Master of Science in Forensic Computing from Cranfield University in the United Kingdom.</p>
10.10 – 10.30	<p>Keynote: Secure operating models for a digital economy Edna Conway</p> <div data-bbox="300 1563 587 1870"></div> <div data-bbox="300 1874 587 1980"><p>Edna Conway VP, Chief Security and Risk Officer, Azure</p></div> <p>Edna Conway currently serves as VP, Chief Security & Risk Officer, Azure at Microsoft. She is responsible for the security, resiliency, and governance of the cloud infrastructure upon which Microsoft's Intelligent Cloud business operates. She has built new organizations delivering trust, transparency, cybersecurity, compliance, risk management, sustainability, and value chain transformation. She is recognized domestically (U.S. Presidential Commissions) and globally (NATO) as the developer of architectures delivering value chain security, sustainability, and resiliency. Prior to joining Microsoft, Conway served as Cisco's Chief Security Officer, Global Value Chain, driving a comprehensive security architecture across Cisco's third-party ecosystem.</p>






10.30 – 10.45	<p>How Microsoft responds to security threats Scott Miller</p>  <p>Scott Miller Microsoft Security Response Center – SOC Manager</p> <p>Scott Miller is a Manager in the Microsoft Security Response Center and is responsible for teams in the UK and India, performing Security Monitoring and Response primarily for Azure. Born and bred in Newcastle upon Tyne, Scott qualified from Northumbria University with a degree in Computer Forensics. The 9 years following he worked for the UK Government in a variety of Cyber Security roles which included performing incident response for the London 2021 Olympics, managing teams in GovCertUK, and building the NCSC's Incident Management function. In 2018 he moved to protect Microsoft and its customers on a global scale.</p>
10.45 – 11.00	<p>Windows 11: Principles of building a secure system David Weston</p>  <p>David Weston Director of Enterprise and OS Security</p> <p>David Weston is the Director of enterprise and OS Security at Microsoft. David has been at Microsoft working on penetration testing, threat intelligence, platform mitigation design, and offensive security research since Windows 7. He has previously presented at security conferences such as Black Hat, CanSecWest, and DEF CON.</p>
11.00 – 11.15	<p>The cyber risks with IOT and OT Phil Neray</p>  <p>Phil Neray Director of IoT & Industrial Cybersecurity</p> <p>Phil Neray is Director of IoT & Industrial Cybersecurity at Microsoft. He joined Microsoft after its acquisition of CyberX, an innovator in agentless security and behavioral anomaly detection for industrial and critical infrastructure networks. Prior to CyberX, Phil held executive roles at IBM Security/Q1 Labs, Symantec, Veracode, and Guardium. Phil began his career as an engineer with Hydro-Quebec and as a Schlumberger engineer on oil rigs in South America. He has a BSEE from McGill University and is certified in cloud security (CCSK).</p>



11.15 – 11.35	<p>Threat detection and recovery in the real world Simon Gardiner</p>  <p>Simon Gardiner Technical Cybersecurity Regional Manager</p> <p>20 years at Microsoft specialising in customer Crisis Management / communications. Last 14 years centrally focused on Cybersecurity Incident Response and Tactical Recovery across all industry sectors in Europe and Asia Pacific/ Commonwealths. Advising cyber attacked customers facing critical business down scenarios on how to proceed with investigations and business recovery options, communication strategies, internally and externally, stakeholder support and what to look for in selecting correct partners. Quintessentially explain how challenging their future will likely look like after a major security event and motivated towards providing appropriate risk-based recovery and partner options.</p>
11.35 – 11.40	<p>Break</p>
11.40 – 12.00	<p>EY on how executives think about cyber risks Jonas Halldin</p>  <p>Jonas Halldin Partner, Cybersecurity</p> <p>Jonas is a Partner and Nordic Cybersecurity Market leader at EY Denmark. Jonas has spent almost 20 years in cybersecurity and has held leading positions such as CISO/CSO in various companies and industries. Jonas holds multiple certifications such as CISSP, CISM, CISA, CDPSE & CRISC.</p>
12.00 – 12.15	<p>Economic Espionage and Cyber Crime Dr Nicola Searle</p>  <p>Dr Nicola Searle Digital Economy Fellow and Associate Professor</p> <p>Dr. Nicola Searle is an economist who specializes in innovation in the digital economy. Her current research, funded by the UK government, investigates the economics of Economic Espionage and Cyber Crime. Dr. Searle is a Digital Economy Fellow and Associate Professor at Goldsmiths, University of London and previously worked at the universities of St Andrews and Abertay. She has published two books with Oxford University Press. Prior to her academic career, Dr. Searle worked as a government economic advisor at the UK Intellectual Property Office and as a financial associate at Goldman Sachs. environments to enable consumer-focused, frictionless, end-to-end digital risk management capabilities.</p>



12.15 – 12.35	Disinformation - how to hack a human Ashish Jamain	
	 <p>Ashish Jamain Director of Product</p>	Ashish Jaiman is a hands-on technologist and product innovator currently serving as the Director of Product with the Microsoft Bing Multimedia team, focusing on building tools and services for the creators and influencer community for innovative storytelling using multimedia to engage users and drive growth.
12.35 – 12.40	Final reflections: what is next for cybersecurity? Sian John & Lesley Kipling	
	 <p>Siân John Event Host Director of Security Business Development and Strategic Growth</p>  <p>Lesley Kipling Chief Security Advisor</p>	<p>Siân John MBE is Director of Security Business Development and Strategic Growth at Microsoft. She leads a team focusing on developing opportunities for Microsoft to deliver new security, compliance, and identity offerings to market. Siân is a Fellow of the Chartered Institute of Information Security and was awarded an MBE in the Queen’s 2018 New Year’s Honours List for services to Cybersecurity.</p> <p>Previously lead investigator for Microsoft’s detection and response team (DART), Lesley Kipling has spent more than 17 years responding to our customers’ largest and most impactful cybersecurity incidents. As Chief Cybersecurity Advisor, she now provides customers, partners, and agencies around the globe with deep insights into how and why security incidents happen, how to harden defenses and more importantly, how to automate response and contain attacks with the power of the cloud and machine learning. She holds a Master of Science in Forensic Computing from Cranfield University in the United Kingdom.</p>
12.40– 12.50	Q&A	