

AGENDA

CYBERUK 2021 ONLINE will take place on a new dedicated [YouTube](#) channel on 11 and 12 May.

There will be a range of sessions broadcast throughout the day as well as a deeper dive into topics that you can explore from both the NCSC and our sponsors via our on demand library.

BUILDING A RESILIENT AND PROSPEROUS DIGITAL UK FOLLOWING COVID-19

The event will explore how we will recover from the pandemic and build a resilient and prosperous digital UK.

We will also be taking a deeper dive into the following subject areas:

UNDERSTANDING FUTURE TECHNOLOGY	BUILDING RESILIENCE	BUILDING A CYBER ECOSYSTEM
Exploring key technologies which will transform the way we live and work online over the next decade.	Helping organisations to understand the cyber threat and identify tools and approaches that will make them more resilient.	Building and showcasing programmes that will support a strong future cyber ecosystem

DAY 1 - TUESDAY 11 MAY

09:15-10:45	OPENING PLENARY CEO WELCOME: Lindy Cameron, CEO, NCSC KEYNOTE: Jeremy Fleming, Director, GCHQ SENIOR INDUSTRY KEYNOTE: Adam Palser CEO, NCC Group Ollie Whitehouse, CTO, NCC Group FIRESIDE CHAT: Sudhakar Ramakrishna, CEO, SolarWinds Paul Chichester, Director of Operations, NCSC PANEL DISCUSSION: Lindy Cameron, Chief Executive Officer, NCSC, Paul Chichester, Director of Operations, NCSC and Dr Ian Levy, Technical Director, NCSC	
11:00-12:00	SUPPORTING THE DEVELOPMENT OF SECURE CONNECTED PLACES - A CONVERSATION Connected Places, often known as 'Smart Cities', can use data and interconnected systems to benefit the environment, increase efficiency and improve services. Gathering, processing and using this data can, however, create risks to privacy and, potentially, safety. This session, chaired by DCMS, will bring together those involved in the development, deployment and security of Connected Places for a discussion of the varied opportunities and risks presented by such environments. SPEAKERS: Erika Lewis, Director, Cyber Security and Digital Identity, DCMS Professor Greg Clark CBE, Chair, Connected Places Catapult Dean, NCSC Nadira Hussain, Director of Leadership Development and Research, Socitm Graham Colclough, Partner, UrbanDNA	
12:00-13:00	PANEL DISCUSSION: PROFESSIONALISING CYBER SECURITY - BUILDING A FIRM FOUNDATION IN EDUCATION AND SKILLS Ian Levy, Technical Director, NCSC SPEAKERS: Matt Warman MP (Minister for Digital Infrastructure) Andrew Elliot, Cyber Security Policy, DCMS Chris Ensor, Deputy Director Cyber Growth, NCSC Virginia Hodge, Director, Heron Associates Dr Claudia Natanson, Board of Trustees, UK Cyber Security Council	
13:15-13:30	MINISTERIAL ADDRESS The Rt Hon Priti Patel MP, Home Secretary	

* Please note this agenda is subject to change.

13:45-14:30	<p>DEVELOPMENTS IN ACTIVE CYBER DEFENCE (ACD)</p> <p>Key developments of ACD tools & services over the last 18 months, particularly in support of the UK Covid-19 response. The services we will be covering are:</p> <ul style="list-style-type: none"> • Suspicious Email Reporting Service (SERS) • The NCSC Takedown Service • Early Warning • Logging Made Easy • Vulnerability Disclosure Toolkit • Exercise in a Box (EiaB) • MyNCSC
14:30-15:30	<p>PANEL DISCUSSION: PROTECTING CONSUMER ACCOUNTS - THE ROLE ORGANISATIONS PLAY</p> <p>Nicola Hudson, Director, Policy & Communications, NCSC</p> <p>We will hear from industry representatives about the steps that are being taken to secure accounts – both behind the scenes to minimise the security burden on consumers and through the provision of empowering security advice communicated directly to consumers. This will be discussed against the backdrop of the evolving online threat to consumers as we explore the real world impact that cyber crime and cyber-enabled fraud is having on victims’.</p> <p>SPEAKERS:</p> <p>Ian McCormack, NCSC Jude McCorry, Scottish Business Resilience Centre Kate Bevan, Editor, Which? Computing Kevin Brown, Managing Director, BT Security George Mudie, CISO, ASOS DCS Andrew Gould, City of London Police</p>
15:45-16:30	<p>RAISING THE BAR ACROSS THE UK: THE ECONOMIC AND SECURITY IMPACT OF THE CYBER ESSENTIALS SCHEME</p> <p>Focussing on Cyber Essentials and the impact it can have – both from a security and economic perspective. A case study of a women’s refuge centre will be used to illustrate the importance of Cyber Essentials in the charity sector, where there may be a low technical understanding but high levels of threat. The growing ecosystem of local cyber security businesses across the UK driven by Cyber Essentials will also be explored.</p> <p>SPEAKERS:</p> <p>Chris Ensor, Deputy Director Cyber Growth, NCSC John Douglas, Director, Information Age Ltd. Sue Burke, CEO, MK-Act Domestic Abuse Services Dr Emma Philpott, CEO, The IASME Consortium Ltd</p>
16:45-17:50	<p>PANEL DISCUSSION: PROTECTING THE NHS FROM RANSOMWARE DURING COVID-19</p> <p>Paul Maddinson, Director, Strategy & Resilience, NCSC</p> <p>We will close the first day of the event with a panel which takes a look back at the increased threat to health from ransomware during Covid-19. The panel will discuss the national collaboration between NCSC, NHSX, and NHS Digital as well as hear a local perspective on protecting the NHS and consider the local impact of national work.</p> <p>SPEAKERS:</p> <p>Neil Bennett, NHS Digital Steven Chilton, University Hospital Birmingham Karen Dooley DD Cyber Security NHSX Ian McCormack, NCSC</p>
END OF DAY 1	

* Please note this agenda is subject to change.

DAY 2 - WEDNESDAY 12 MAY







10:00-10:45	OPENING PLENARY WELCOME AND REVIEW OF DAY 1: Lindy Cameron, CEO, NCSC MINISTERIAL ADDRESS: The Rt Hon Dominic Raab MP, Foreign Secretary and First Secretary of State INDUSTRY KEYNOTE: John Lambert, Distinguished Engineer, Microsoft Threat Intelligence Center	
11:15-12:00	HOW DO YOU SOLVE A PROBLEM LIKE CYBER SECURITY FOR CONSUMER DEVICES? 'SECURE BY DESIGN' Securing the landscape of consumer internet-connected devices is complex. It involves a multifaceted and pragmatic approach that can iterate over time, bringing together governments, standard bodies, industry and the security research community. In this session, the UK government will provide an insight into its Secure by Design programme of work, including an update on the proposed regulatory approach, the new European Standard on IoT security and the role of assurance schemes in implementation and compliance. The consumer association Which? and a representative of both Arm and the IoT Security Foundation will provide an insight into what more could and is being done, beyond legislation, to secure the devices of the future. SPEAKERS: Dr Ian Levy, Technical Director, NCSC Jonathan Angwin, Senior Policy Advisor, DCMS Peter Stephens, Head of 'Secure by Design': Cyber Security for consumer devices, DCMS Stephen Pattison, VP Public Affairs Arm, Chair of the IoT Security Foundation (IOTSF) Andrew Laughlin, Principal Researcher, Which?	
12:15-13:00	OH THAT WAS CLEVER! WHEN EVEN JADED INCIDENT RESPONDERS ARE IMPRESSED Join the NCSC's Tech Director for Incident Management for a tour of some of the interesting technical aspects that have exercised (and perhaps grudgingly impressed) our Incident Management team over the last year. Unsurprisingly, there will be a lot of discussion of UNC2452 this year. SPEAKER: Harry, Technical Director for Incident Management, NCSC	
13:15-14:00	ACCELERATING AND SECURING CYBER INNOVATION AND GROWTH Alumni companies from the NCSC's Cyber Accelerator programme will share their experiences of being a start-up in the UK, talking about the ups and downs and the support they have received to give a deeper understanding of their personal journeys. Chaired by NCSC's Deputy Director for Cyber Skills & Growth, Chris Ensor, they will also be joined on the panel by Andrew Elliot, Deputy Director for Cyber Security Innovation and Skills at DCMS, who will talk about what the UK government is doing to 'build back better' and an NCSC representative who will talk about the new start-up guidance launched in May 2021 and how this ties to the National Security and Investment Bill. SPEAKERS: Chris Ensor, Deputy Director Cyber Growth, NCSC Jamie Akhtar, CEO, CyberSmart Dan Brett - CSO (Chief Strategy Officer) & Founder - CounterCraft Andrew Elliot, Deputy Director Cyber Security, DCMS Bryony, Policy Team, NCSC Vicky Brock, CEO, Vistalworks	
14:00-15:00	PANEL DISCUSSION - IN CONVERSATION WITH... Emily Taylor, Chatham House, facilitates a conversation between: Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology, White House Beth Sizeland, Deputy National Security Advisor Lindy Cameron, CEO, NCSC	
15:30-16:30	RANSOMWARE - THE RISK TO SCHOOLS AND WAYS TO PREVENT IT The NCSC and Department for Education come together to raise awareness of ransomware, following a recent spate of ransomware attacks against the education sector. There will be an overview of ransomware and an exploration of how to back-up school data, and the NCSC Incident Management team will talk about managing a ransomware incident in a school or trust, ending with a high-level panel discussion on cyber resilience in the education sector. SPEAKERS: Rt Hon Nick Gibb MP, Minister of State for School Standards Paul Maddinson, Director, National Resilience and Strategy, NCSC Dan, Incident Management, NCSC Gregory, Engagement Officer NCSC Hannah, NCSC Steve Forbes, Head of Cyber Product, Nominet Jon Gilbert, Chief Information Security Officer, Department for Education Heather Toomey, Cyber Security Lead at the Education Data Hub, Derbyshire County	
16:30-17:35	PANEL DISCUSSION: EMERGING CYBER TRENDS – THE EXPERT VIEW Eleanor Fairford, Deputy Director for Incident Management, NCSC SPEAKERS: Paul Chichester, Director of Operations, NCSC Dr Ian Levy, Technical Director, NCSC Graham Biggar, Director General, NCA Christine Maxwell, Director Cyber Defence and Risk, Ministry of Defence	
17:35-17:40	CLOSING REMARKS Lindy Cameron, CEO, NCSC	

END OF DAY 2

* Please note this agenda is subject to change.





ON DEMAND

SESSIONS AVAILABLE ON YOUTUBE FROM 11 MAY

20 min	BUILDING RESILIENCE SPONSOR: BAE Systems RESILIENCE THROUGH COLLABORATION Dr Mary Haigh, BAE Systems CISO, will explore how collaboration is essential in ensuring resilience is embedded within an organisation. Mary will reflect on the challenges and opportunities during the pandemic and lessons learnt. Mary will also talk about the importance of working with others and how diversity delivers better results as well as the importance of working as a team and how BAE have been piloting some of the NCSC's own ACD capabilities.	
40 min	REFRESHING THE 10 STEPS TO CYBER SECURITY The '10 Steps To Cyber Security' was originally written in 2012 by CESG, but a lot has changed since then. Changes in the external environment, the threats that organisations face and how we use new technologies mean that now is a good time to update the Steps. The revision aligns the 10 Steps with newer NCSC guidance including Cloud Security Principles, managing Ransomware Attacks and our Board Tool Kit.	
40 min	UNDERSTANDING CYBER CRISES Despite increasing interest for cyber security issues in the academic community, cyber crises and the requirements for effective strategic cyber crisis management are still largely under-researched. Drawing on crisis management research and new empirics, this brief will suggest one way of conceptualising cyber crises theoretically and explore how this might help us to better understand common strategic challenges of cyber crises and how to manage them. SPEAKERS: Sarah Backman, PhD Candidate in International Relations, Stockholm University Dr Deborah Petterson, Deputy Director, Private Sector CNI, NCSC	
20 min	UNDERSTANDING FUTURE TECHNOLOGY SPONSOR: UKCloudX HOW CAN ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) BE USED TO IMPROVE CYBER SECURITY? AI and ML are maturing at different rates across a range of technology disciplines. But, as they mature, they offer both opportunities and potential threats in maintaining and improving cyber security. This panel will explore: <ul style="list-style-type: none"> • Real-world use and near-term advances of ML • The evolution of technologies and tools • The complexities of ground truth information • The skills needed for the cyber security workforce of the future 	
40 min	SECURING THE FUTURE: EMERGING TECHNOLOGY AND FUTURES LITERACY We've often historically thought about emerging tech through a purely technological perspective, but really we need to consider how society/people will interact and use it, as well as the markets/economics perspective. Anticipation is an emerging discipline in cyber security that is concerned with how we imagine and tell stories about cyber security futures and Futures Literacy is the skill set that we need to do it effectively. SPEAKERS: Anna, Strategic Research Lead, NCSC Reid Derby, Innovation Lead for Cyber Central Ben Koppelman, Research & Innovation Lead, CyberSmart Professor Genevieve Liveley, Professor of Classics, RISCs Fellow, Turing Fellow, University of Bristol Simeon Quarrie, Founder & CEO, VIVIDA.io	
40 min	PREPARING THE UK FOR A SECURE FUTURE IN QUANTUM TECHNOLOGY An overview of what is happening within the UK with quantum technology and specifically quantum computing, including exploring what quantum computing means for cryptography as well as how the NCSC is supporting the industry through work being done with Trusted Research & Secure Innovation Guidance. SPEAKERS: Dr Ian Levy, Technical Director, NCSC Bryony, Policy Team, NCSC Harpreet, University Engagement Lead, NCSC Joanna, Head of Cryptography Research, NCSC Michael, Technical Director, NCSC	

* Please note this agenda is subject to change.

ON DEMAND

20 min	BUILDING A CYBER ECOSYSTEM SPONSOR: Palo Alto Networks	
40 min	INDUSTRY DISCUSS THEIR EXPERIENCES AND BENEFITS OF BEING PART OF THE NCSC'S CYBERFIRST PROGRAMME An overview on the CyberFirst programme and how it can help support your graduate recruitment, gender diversity and interaction with the local community. Listen to case studies from those involved and hear first hand from our panel of industry members. SPEAKERS: Chris Ensor, Deputy Director Cyber Growth, NCSC Keith Lippert, Vice President and Deputy Chief Information Security Officer, Allstate Laura Price, Employer Brand Specialist, BT Security Julian Meyrick, Managing Partner, Security Strategy Risk & Compliance, IBM UK Ltd Emily Turner, Head of Education & Engagement - Chief Resilience & Security Office, Lloyds Banking Group Emily Beeney, Vice President, Morgan Stanley Luke Fairless, Technology Director – Security & Capability, Tesco	
40 min	HOW TO MAKE A DIFFERENCE LOCALLY An insight into the evolving cyber security education ecosystems, who is involved, how they work, future plans and how you can get involved. Hear how industry, cyber clusters and academia are all working together to create vibrant and exciting regional cyber security education ecosystems. SPEAKERS: Chris Ensor, Deputy Director Cyber Growth, NCSC Phil Jackman, CyberNorth Richard Yorke, Managing Director, CyNam (Cyber Cheltenham) Ciara Mitchell, Cluster Manager for ScotlandIS Cyber, ScotlandIS Clare Johnson, Partnerships and Outreach Manager (Digital and STEM), University of South Wales	
10 min	DIVERSITY AND ITS IMPORTANCE IN THE CYBER MISSION Despite multiple initiatives to address the cyber security skills gap, this remains a major challenge for organisations; widened further by cost-cutting measures during COVID-19. In this session NCC Group explore the range of skills needed to enhance cyber security and how these can be a business enabler. NCC Group also share practical actions to build your resilience quickly and effectively, focusing on recruitment, training and diversity.	
10 min	CYBER SECURITY AS THE FOUNDATION FOR THE UK'S DIGITAL TRANSFORMATION 2020 brought new challenges to an already complex and rapidly evolving security landscape. In this session Chris Perkins, Public Sector Lead at Microsoft UK, will discuss the trends, challenges and opportunities that face us as we return to a hybrid workplace. Chris will be joined by Pete Cooper, Deputy Director of Cyber Defence at the Government Security Group, to explore how UK Government is supporting organisations in improving their security posture.	

* Please note this agenda is subject to change.

ON DEMAND

SESSIONS AVAILABLE ON YOUTUBE FROM 11 MAY

10 min	<p>"CLOUD, UNLESS" - HOW A CYBERATTACK CHANGED HACKNEY COUNCIL'S RELATIONSHIP WITH TECHNOLOGY OVER NIGHT</p> <p>In October 2020 Hackney Council suffered a serious cyberattack. Hear how they responded to the incident, working at extreme pace, and adopting a "cloud, unless" policy to restore services for Hackney's residents and businesses as quickly as possible.</p> <p>Matthew Cain, Head of Digital, Data and Customer Services at the Council explains their aspirations for security, resilience and user centricity, to prevent a similar attack in future and build back better.</p>	aws
10 min	<p>INSIDER THREAT: IS YOUR GREATEST CYBER RISK WITHIN YOUR ORGANISATION?</p> <p>CDS Defence & Security has worked with the UK MOD since 2015, delivering Insider Threat capability into their wider SAFEGUARDING programme. In this presentation, CDS DS will take you through the techniques and processes that made the UK compliant with the wider FVEYs community, the evolution of the threat and why a holistic approach to cyber security is essential in the modern threat landscape.</p>	cds Defence & Security
10 min	<p>THE FUTURE OF PUBLIC PRIVATE PARTNERSHIPS ENABLING CYBER SECURITY</p> <p>Stuart McKenzie, Senior Vice President at FireEye Mandiant hosts a session reflecting current attacker trends in an increasingly hostile cyber threat landscape, the rapid rise of ransomware as an attacker's tool of choice and some of the most significant and high profile incidents in recent times.</p> <p>Stuart will discuss how public and private sector entities are combining forces in order to deal with such events, building on established successful partnerships.</p>	FIREEYE™ MANDIANT
10 min	<p>BEATING THE BOTS</p> <p>Cyber threat actors are increasingly automating their attacks on global organisations and entities. Businesses are becoming more aware of the impact of bots on their brand and revenue, but are struggling to prepare and respond to these types of attack. FTI Cybersecurity experts share some of the counter-bot strategies they have developed for clients, highlighting the need for a comprehensive approach to this threat encompassing people, processes and technology.</p>	FTI CONSULTING CYBERSECURITY
10 min	<p>COLLABORATE FOR RESILIENCE</p> <p>Could an enhanced collaborative approach improve the effectiveness of your SOC? In this on-demand video, Luke Ager (Chief Technology Officer – Cyber Security) and Abi Peach (Business Lead, Cyber SOC Services) discuss how the building blocks for a collaborative, hybrid SOC can decrease your cyber risk and improve understanding of your unique threat environment faster and more efficiently than a purely in-house or outsourced approach.</p>	QINETIQ
10 min	<p>EFFECTIVE MANAGEMENT OF CYBERSECURITY THREATS TO ICS THROUGH ADOPTION OF IEC 62443 PRINCIPLES AND CERTIFIED SECURITY BLUEPRINTS</p> <p>Addressing the profound impact that the Network and Information Systems (NIS) Regulations has had to the operations and culture of Operators of Essential Services, we focus on a proven approach to adopting secure principles and standards for establishing secure delivery policies and procedures inclusive of oversight and governance of the supply chain.</p>	SIEMENS