



National Cyber
Security Centre
a part of GCHQ

Lead sponsors



CYBERUK ONLINE 2021

#CYBERUK21

#ResilientDigitalUK

WELCOME TO CYBERUK 2021 ONLINE

With just one week to go until CYBERUK 2021 ONLINE, we are delighted to share more information about this year's event and its new, open format. As ever, CYBERUK will showcase world-class content from leading experts at the NCSC and special guests from the cyber and tech industry, national security and government. Join us on our new dedicated [YouTube](#) channel on 11 and 12 May.



SPONSOR ANNOUNCEMENT

We are delighted to have NCC Group and Microsoft as lead sponsors of CYBERUK 2021 ONLINE. You will hear industry insights from their senior leaders.



WHAT CAN I EXPECT FROM THIS YEAR'S NEW EVENT FORMAT?

The YouTube channel is open to all and free to access – there is no need to register and you do not need a YouTube account to attend. We have a full programme each day with an exciting line up of speakers. There are a range of keynotes and panel sessions, as well as some deeper dives into some of this year's key themes. Many of our sessions will be live and broadcast to you from our CYBERUK studio, and some have been pre-recorded to allow for contributions from a wide range of speakers.

The draft agenda is included below - keep up to date with any changes on the [CYBERUK webpage](#). Choose your sessions and tune into the channel at the designated time.

Can't make a decision on what sessions you'd like to watch? Not a problem - all content including additional sessions outside of the main agenda will be available on demand on the CYBERUK 2021 ONLINE YouTube channel during and after the event!

We invite you to join in conversations and ask questions via the event's social media channels and we look forward to engaging with you on 11 and 12 May.

Any questions? Please feel free to get in touch at cyberuk-events@brayleinoevents.com



[National Cyber Security Centre](#)



[@NCSC](#) [@CYBERUKevents](#)

#CYBERUK21 #ResilientDigitalUK



[CYBERUK](#)

If you have received this e-bulletin it means you have agreed to receive further information about CYBERUK. Further instructions on how to attend the event will be available closer to the date.

BUILDING A RESILIENT AND PROSPEROUS DIGITAL UK FOLLOWING COVID-19

Since the NCSC was created in 2016 as part of the government's five-year National Cyber Security Strategy, it has worked towards making the UK the safest place to live and work online. CYBERUK 2021 looks at some of the key challenges faced through the Covid pandemic where the NCSC, in partnership with domestic and international partners, led the way in protecting the NHS and those developing vaccines and medical interventions.

The event will explore how we will recover from the pandemic and build a resilient and prosperous digital UK, considering future technologies which will transform the way we live and work online over the next decade. We will bring together key players from government, national security, industry and academia to deliver world class content, cementing the UK's position as a responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace, and strengthen the UK cyber ecosystem.

At CYBERUK 2021 ONLINE we will be exploring some key themes with our deeper dive sessions. NCSC experts use real-world examples to demonstrate emerging threats and solutions and work with partners to share insights from across government, industry, and academia.

Building Resilience

Helping organisations to understand the cyber threat and identify tools and approaches that will make them more resilient.

Sponsored by:

BAE SYSTEMS

Understanding Future Technology

Exploring key technologies which will transform the way we live and work online over the next decade.

Sponsored by:

 **ukcloud**X

Building a Cyber Ecosystem

Building and showcasing programmes that will support a strong future cyber ecosystem.

Sponsored by:

 **paloalto**
NETWORKS

We are grateful to our additional sponsors who have used their expertise and insight to build a varied and interesting programme of content for CYBERUK 2021 ONLINE. Additional sessions will be available to view on demand from the following sponsors:



CYBERUK is hosted by the National Cyber Security Centre as part of the UK Government's vision to make the UK the safest place to live and work online.

 www.ncsc.gov.uk

 National Cyber Security Centre

 @NCSC @CYBERUKevents

#CYBERUK21
#ResilientDigitalUK

DRAFT AGENDA

DAY 1 - TUESDAY 11 MAY

09:15-10:45	OPENING PLENARY CEO Welcome, Director GCHQ, Senior Industry Keynote: NCC Group, Fireside Chat hosted by NCSC Director of Operations, Panel Discussion.	
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.	
12:00-13:00	PANEL DISCUSSION: PROFESSIONALISING CYBER SECURITY - BUILDING A FIRM FOUNDATION IN EDUCATION AND SKILLS	
13:15-13:30	MINISTERIAL ADDRESS	
13:45-14:30	DEVELOPMENTS IN ACTIVE CYBER DEFENCE (ACD) 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: • 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	PANEL DISCUSSION: PROTECTING CONSUMER ACCOUNTS - THE ROLE ORGANISATIONS PLAY	
15:45-16:30	RAISING THE BAR ACROSS THE UK – THE ECONOMIC AND SECURITY IMPACT OF THE CYBER ESSENTIALS SCHEME 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.	
16:45-17:50	PANEL DISCUSSION: PROTECTING THE NHS FROM RANSOMWARE DURING COVID-19	
END OF DAY 1		

DAY 2 - WEDNESDAY 12 MAY

10:00-10:45	OPENING PLENARY CEO Welcome and Review of Day 1 Ministerial Address Senior Industry Keynote: Microsoft	
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.	
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.	
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.	
14:00-15:00	FIRESIDE CHAT: (TBA)	
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.	
16:30-17:35	PANEL DISCUSSION: EMERGING CYBER TRENDS – THE EXPERT VIEW	
END OF DAY 2		

* Please note this agenda is subject to change.

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.	BAE SYSTEMS
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.	 National Cyber Security Centre a part of GCHQ
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.	 National Cyber Security Centre a part of GCHQ
40 min	CYBER SECURITY FOR SMALL ORGANISATIONS In this session the NCSC provides an overview of our guidance for small organisations. The session details affordable and practical advice to help prevent common cyber attacks and provides tips for preparing a response and planning your recovery to a cyber incident.	 National Cyber Security Centre a part of GCHQ
20 min	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: • 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.	 National Cyber Security Centre a part of GCHQ
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.	 National Cyber Security Centre a part of GCHQ
20 min	BUILDING A CYBER ECOSYSTEM SPONSOR: Palo Alto Networks ADVANCING TRANSFORMATION—INNOVATING TO SECURE A BETTER TOMORROW Automation and integration of security operations are essential to prevent successful cyberattacks and to protect organisations across clouds, networks, and mobile devices in the face of increasingly sophisticated and automated cyber adversaries. In this session, Nir Zuk will describe the ways Palo Alto Networks continues to disrupt our industry through bold innovation that is designed to help digital enterprises securely transform in a complex, changing world—so they can be secure today for a better tomorrow.	
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.	 National Cyber Security Centre a part of GCHQ
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.	 National Cyber Security Centre a part of GCHQ
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.	

ON DEMAND

SESSIONS AVAILABLE ON YOUTUBE FROM 11 MAY		
10 min	INSIDER THREAT: IS YOUR GREATEST CYBER RISK WITHIN YOUR ORGANISATION? 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.	
10 min	THE FUTURE OF PUBLIC PRIVATE PARTNERSHIPS ENABLING CYBER SECURITY 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. Stuart will discuss how public and private sector entities are combining forces in order to deal with such events, building on established successful partnerships.	
10 min	BEATING THE BOTS 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.	
10 min	COLLABORATE FOR RESILIENCE 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.	
10 min	EFFECTIVE MANAGEMENT OF CYBERSECURITY THREATS TO ICS THROUGH ADOPTION OF IEC 62443 PRINCIPLES AND CERTIFIED SECURITY BLUEPRINTS 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.	