

# NPCC National Business Cybercrime Conference 2021

A joint NPCC/SASIG event



**Thursday 4 November 2021**

**9am to 2pm**

**Kia Oval, Surrey County Cricket Club, Kennington,  
London SE11 5SS**

UK law enforcement efforts to combat cybercrime are the 'most joined-up bit of policing' in the country, but police forces cannot do it alone. Cybercrime will be defeated only through collaboration, engagement and partnership with industry and with the community. While there is still a lot more work to be done, huge progress has been made over the past six years.

At this meeting, we will examine the threat and explore the UK's growing and evolving capability to counter cybercrime at the national, regional and local levels. This will be an opportunity for players from all parts of the fight against cybercrime to gather and review progress. The agenda features speakers from the national and regional cybercrime network, as well as industry experts in cybersecurity and cybercrime prevention/detection.

## **Chair – Detective Chief Superintendent Andrew Gould, National Cybercrime Programme Lead, National Police Chiefs' Council**

---

**9am**                      **Registration, coffee and networking**

---

**9.30am**                      **Progress report on the national response to combatting cybercrime**  
**Ian Dyson QPM** Commissioner, City of London Police and National Lead for Cyber Crime, National Police Chiefs' Council  
The pandemic has changed the nature of crime with a significant increase in online criminal activity. This presentation will cover the nature of the changes, developments in policing and how we are addressing these new challenges.

**10am**                      **The human element of cybersecurity in the age of hybrid working**  
**Martin Smith MBE** Chairman, The SASIG  
The world could not have survived the pandemic without the internet. Lockdown has caused wholesale change in the way the world does business, accelerating trends in new technology and human behaviour by decades. Covid-19 has been a game-changer for cybersecurity, finally and firmly establishing it as a critical business enabler. In the age of hybrid working, we must now step up to the new challenges both in technology, the threat landscape, and the supervision of our remote-working employees.

**10.30am**                      **The evolving threat to UK plc**  
Senior representative, NCSC  
Latest update on the cyber threat picture from the perspective of the National Cyber Security Centre, reflecting on what we have seen over the past year and a view of the future cyber threat landscape.

**11am**                      **A case study with a Regional Organised Crime Unit**  
**DS Mike Fishlock** Metropolitan Police  
Operation Vitellius – An Organised Criminal Network using Dark & Clear web to harvest Fullz data.  
Officers engaged online with Fullz vendors on the dark web. Using investigative techniques, Police were able to identify members of an online Organised Criminal Network and evidentially link them to a number of online Fullz harvesting websites. Suspects were arrested, charged and sentenced earlier this year.

---

**11.30am**      **Tea, coffee and networking break**

---

**11.45am**      **Police CyberAlarm – Helping the Police Help You**  
**Detective Chief Inspector Phil Donnelly** National Cybercrime Programme  
**Jon Davies** CTO, Pervade Software  
**Sharon Penfold** Director of Technology, Action for Children  
An overview of the Police CyberAlarm system how it can help organisations of any size increase their understanding of the cyber threat and help policing. The presentation includes the police vision, a technical overview and a testimonial from a current member.

**12.15pm**      **Delivering A National Vision for Secure Business Supply Chain**  
**Mandy Haeburn-Little** Executive Chair, BRIM  
**Nick Bell** Chief Executive, National Cyber Resilience Centre Group  
**Mark Scott** Chief Executive Officer, Cantium Business Solutions  
Delivering a National vision for a secure supply chain in business across England and Wales is no mean feat. This session will explain how that will be done through an initiative being led by policing, private sector and academia

**12.45pm**      **Cyber & Digital Specials & Volunteers (CDSV)**  
**Nick Bell** Chief Executive, National Cyber Resilience Centre Group  
The new Cyber & Digital Specials and Volunteers Programme is working with businesses to utilise the specialist digital skills of their workforce to support policing in protecting businesses and individuals from cybercrime.

**1.15pm**      **Panel session – Working together**  
Facilitated by **Martin Smith MBE** Chairman & Founder, SASIG

- **Commissioner Ian Dyson QPM** Commissioner City of London Police and National Lead for Cyber Crime, National Police Chiefs' Council
- **Stuart Frost BEM** Deputy Director, Head of Enterprise Security & Risk Management, Department for Work & Pensions
- **Philip Marshall** Head of Intelligence Services, Lloyds Banking Group
- **Professor Denis Fischbacher-Smith** Research Chair in Risk and Resilience, University of Glasgow

So much progress has been made over the past few years to build stronger bonds of trust between the law enforcement agencies and public sector organisations/private sector enterprises to assist in the rapid reporting and resolution of cybercrime and other risks. But each side has differing and sometimes conflicting priorities, so how do we ensure that cooperation and communication is kept at an optimum?

---

**2pm**      **End of meeting. Networking luncheon**

---

# About



## The National Police Chiefs' Council (NPCC)

The NPCC brings police forces in the UK together to help policing coordinate operations, reform, improve and provide value for money. Since 1 April 2019, every Police Force in England and Wales now has a dedicated Cyber Crime Unit in place thanks to the multi-million-pound investment from the Government, thus greatly improving the response for victims and support for business.

The National Cybercrime Programme is also responsible for delivering a national training framework for officers and staff dedicated to cybercrime units at force and regional levels. It has since set up the Cybercrime Hub on the Knowledge Hub, providing a valuable resource for officers and staff and funded licenses for the training environment Immersive Labs.

Every force now has a Protect capability responsible for working with local businesses to support them in minimising their vulnerability to attack.



## The Security Awareness Special Interest Group (SASIG)

SASIG is a subscription-free networking forum, membership now represents hundreds of organisations of all sizes from across the world and from all sectors, public and private. Its 5,800+ membership is drawn from CIOs, CISOs and their staff with responsibility for cybersecurity within their organisations. Professionals from other disciplines (risk, HR, legal, supply, etc.) and representatives from government, law enforcement and academia are also being increasingly welcomed at our events. The Chatham House Rule is strictly enforced and universally respected at all meetings, and vendors and the Press are routinely excluded. Thus, the level of debate is extraordinarily revealing and rewarding.

SASIG has a members' website at [www.thesasig.com](http://www.thesasig.com). Please register here for membership.

## With thanks to our supporters...

