Overview

Half of all fraud that takes place in Britain now occurs online, the cost to victims rising to £27 billion a year.

The group Action Fraud received 46,000 reports of cybercrime in 2012, demonstrating the reach of this increasingly sophisticated electronic form of criminal activity. It is not just individuals who are feeling the impacts of such crime, 93% of large corporations and 73% of small firms reported a breach in cyber security in the last year.

Globally cybercrime is now thought to be costing in the region of $300 billion to $1 trillion per year. Whilst the financial stakes of such criminality is high, there are also socio-political consequences. For example it is suggested that there is growing evidence that the revenue garnered by cybercriminals is being used to finance the activities of terror groups, including those of al-Qaeda.

Cyber attacks also pose an increasing risk to national security, which could led to the military being ‘fatally compromised’, and the defence select committee has urged the MOD to make the development of rules of engagement for cyber operations an urgent priority.

Aims and Objectives

This conference aims to explore some of the urgent issues faced by the growing threat of cybercrime, offering current insight into case law, governmental policy, as well as the crucial practical issues of how such crime can be detected, investigated, prosecuted and managed.

Who Should Attend?

This event is a must attend for all those working in the area of cybercrime policing, as well as legal professionals, academics and policymakers.

Feedback

“...excellent conference pitched at exactly the right level. I have learnt a great deal and feel better placed to fulfil my role.”

IPCC

Hot Topics

Expert speakers in the field of cybercrime will deliver presentations in topical subjects including:

- Cross-agency cyber capabilities from force level, the regional response and the National Cyber Crime unit
- Cybercrime legislation in the UK;
- Evidential issues;
- RIP Act authorisations for online surveillance;
- Transnational access to data (both direct access, and co-operation with foreign LEAs and ISPs);
- Practical issues of defending/prosecuting at trial

Expert Speakers

- Jon Boutuher | ACC Hertfordshire Constabulary and Deputy National Lead for Cyber Crime
- Simon McKay | Principal at McKay Law
- David Cook | Associate at Pannone Solicitors
- Nigel Jones | Director at Technology Risk Limited
- Dr Ian Walden | Professor at QMUL
- Jacqueline Zoest | Barrister & Anthony Orchard QC
  | Barrister | Carmelite Chambers

Top Content

Each delegate will receive a complimentary usb flash drive containing all speaker presentations. This enables the delegate to consider the conference materials in their own time.

First Class Venue

This conference will take place in a venue within zone 1 of the London underground for easy access.

There will be 3 refreshment breaks and a hot lunch included on the day which provides an ideal opportunity for networking.
Speaker Profiles

Simon McKay is a Solicitor-Advocate (all proceedings) in England and Wales and a member of the Law Society of Northern Ireland. He frequently exercises his rights of audience in all of the higher Courts and has the privilege of working with and against some of the country’s leading QCs. He is a criminal and human rights lawyer and recognised nationally and internationally for his expertise in covert policing and surveillance law.

His work encompasses:
- defence and appellate work in criminal proceedings (including murder, serious sex offences and Official Secrets Act matters)
- sports and professional disciplinary proceedings
- judicial review
- civil actions, including human rights claims, against the police and other public authorities (particular interest in article 2 cases and witness protection issues)
- media work where it involves a criminal or human rights issue
- whistle blowing claims arising in either the criminal or civil jurisdictions


David Cook is a Solicitor Advocate recognised as an expert in cyber crime and data security. He successfully defended a client in the first prosecution for online file sharing and was instructed in in the second prosecution for online file sharing, again successfully defending the client on the basis of a technical defence. He has advised individuals alleged to be involved in the Anonymous and Lulzsec hacking groups as well as assisted corporate bodies with regard to evidence collation and the preparation of evidence packs for prosecution (private prosecution, referral to the police and referral to Trading Standards teams). David advises businesses on data security and data loss, including with respect to the referral of matters to the Information Commissioner’s Office or representation with respect to breach action. David also represents clients with regard to online reputation management.

David was invited by the Director for Public Prosecutions to assist in the drafting of guidance for prosecutors regarding social media based offences. He frequently provides seminars to local councils and police forces (both at a regional and national level) on the collection of evidence in and prosecution of computer based offences. He has recently assisted in training the North West, South Wales, Yorkshire and Humber police divisions with regard to the national cyber crime capability and gave a seminar to senior police officers at the College of Policing on evidential issues in cyber crime investigations.
David’s expertise is sought out by academics, media commentators and clients alike and he boasts a national client base in relation to advising both individuals and corporate bodies on the prosecution or defence of computer related matters.

David joined Pannone, part of Slater and Gordon, in 2011. More information on David can be found on their website - http://www.pannone.com/people/david-cook

**Nigel Jones** is currently a director of Technology Risk Limited, a company specialising in technology risk solutions and training and has recently taken up an adjunct professorial position at University College Dublin. Prior to this he was responsible for the creation of the National High Tech Crime Training Centre at the National Centre for Policing Excellence at Wyboston in the UK and was responsible for the creation of the design and delivery of a core curriculum and modular high tech crime training programme for the UK police service.

Nigel formed the Kent Police Computer Crime Unit in 1993 and is co-author of the ACPO “Computer Based Evidence - Good Practice Guide” and member of the Technical Working Group on the Investigation of Electronic Evidence (TWGIEE) in the USA. Nigel has given presentations at numerous national and international events including the preparation and moderation of a hi-tech crime scenario at the United Nations 10th Crime Congress. In 2002 he was appointed by the UK as a member of the Interpol European Working Party on IT Crime.

In 2003 Nigel was appointed as project manager of a European Commission Agis funded programme to develop a cybercrime training programme for the 28 EU and candidate countries. A network of cybercrime training institutes was created to take this work forward. The project was supported by 19 partner organisations within the EU. Nigel was also project manager for a series of training courses on behalf of the European Police College (CEPOL) to deliver training to senior managers of EU police forces and a further project to deliver training to a group of countries from North Africa, the Middle East and Southern Europe.

Nigel worked in close collaboration for two years with Canterbury Christchurch University in the development of an MSc award in Cybercrime Forensics that is now offered by the University. He was recently invited to Interpol as an expert to provide advice on an international IT forensics investigation. He also chaired the cybercrime panel at the recent Interpol General Assembly. He is currently a member of the Home Office Forensic Regulators digital forensics specialist group which is assisting in identifying requirements for new or improved quality standards, applying to the provision of digital forensics services to the police service and the wider Criminal Justice System. Nigel is currently the training manager for a €2.7m European Commission funded programme to further harmonise cybercrime training across international borders.

**Jacqueline Zoest** is a Barrister specialising in fraud and all types of ‘white collar’ or economic /financial crime. She has a particular interest in e-crime /cybercrime.

She practises from Carmelite Chambers in London and has extensive experience advising clients on and defending and prosecuting criminal cases. Recent assignments include assisting the team representing a ‘LulzSec’ computer hacker charged with multiple computer misuse offences relating to hacking into computer systems of UK and US government and private organisations; and acting as a member of the legal team representing a UK businessman in litigation relating to allegations of a multi-million pound fraud allegedly implicated in the collapse of an Icelandic bank.

Jacqueline is a member of the Serious Fraud Office panel of prosecuting counsel and the Crown Prosecution Service specialist Fraud Advocates panel. She is a contributing author to Westlaw (Sweet & Maxwell) on the subject of Computer Misuse Offences.

Prior to her coming to the Bar in 1995, Jacqueline worked as a Management Consultant advising organisations in the banking /finance, technology and public sectors. Her clients included the Finance Directorate of the European...
Commission and the Australian Government. Her early career was as a computer software developer, designing and programming financial and banking software for organizations in the finance/banking and public sectors.

Jacqueline has a B.Sc. from the University of Cape Town and an LLM in Computer and Communications Law from Queen Mary University of London.

She is a member of the Fraud Advisory Panel; the Bar Association for Commerce, Finance and Industry; the Criminal Bar Association and the Society for Computers and Law

**Anthony Orchard QC** is a Barrister and Queen's Counsel with extensive experience defending and prosecuting serious and organized crime including cybercrime and fraud. He practises from Carmelite Chambers in London and is instructed in cases throughout the UK.

Anthony represented the youngest member of the ‘LulzSec’ computer hacking group who was charged with multiple computer misuse offences relating to hacking into computer systems of government and private organisations (including News Corporation, Sony Pictures, UK Serious and Organised Crime Agency, the CIA and FBI).

Anthony is a specialist in major fraud and confiscation work and has prosecuted on behalf of the Fraud Division of the Crown Prosecution Service, the Serious Fraud Office and the Financial Conduct Authority. Recent cases include a £58 million VAT Diversion fraud and a £27 million ‘boiler room’ fraud.

Anthony regularly advises on and appears in a variety of serious criminal cases, including cases involving high value drug importation, human trafficking or murder. He has appeared in over eighty homicide trials at the Central Criminal Court and elsewhere, many involving allegations of multiple shooting and ‘gangland’ murder. In 2013 he defended Michael Philpott in the “Derby fire” case.

He regularly advises on PII matters, RIPA, Surveillance law, SOCPA contracts, PACE, Abuse of Process and Disclosure issues.

He is a member of the Fraud Advisory Panel, the Fraud Lawyers Association and the Criminal Bar Association (CBA); and is the CBA representative on the Home Office PACE Strategy Board (2004 – current).