WILMERHALE

Just a little bit of history repeating: Has the UK reached a familiar juncture in respect of the detection, investigation and prosecution of serious and complex cybercrime?

DECEMBER 14, 2017

In October this year, the City of London Corporation announced plans, backed by H.M. Courts and Tribunals Service, for the construction of a state-of-the-art trial venue complex in central London, specialising in fraud and cybercrime. This has been lauded as a timely tonic for worries about London's continuing role, post-Brexit, as the pre-eminent global legal centre, but does it only go half-way in ensuring that justice is properly served in cases of serious and complex cybercrime? In recognising the need for a specialist, coordinated and technically competent court system to deal with the challenges of hearing cybercrime cases, have we also now reached a familiar juncture in recognising the specialist needs for the successful detection, investigation and prosecution of serious and complex cybercrime?

Cybercrime, (of which there are broadly two types: (i) 'cyber-dependent' crime, that is offences perpetrated against systems and data that cannot be committed without using a computer and which are mostly covered by the Computer Misuse Act 1990; and (ii) 'cyber-enabled' crime, that is mature criminal offences such as fraud, theft and harassment, that are facilitated in cyberspace) is, by many measures, increasing in its frequency, scale and complexity.[1] A cursory read of a daily newspaper bears out former FBI Director Robert Mueller's proposition that, "*there are only two types of company: those that have been hacked and those that will be.*"[2] To which list we should perhaps now also add those companies who remain unaware that they have been hacked.

The demands placed on those responsible in the UK for investigating and prosecuting serious and complex cybercrime (currently the police, the National Cyber Crime Unit ("NCCU") within the National Crime Agency ("NCA") and the Crown Prosecution Service ("CPS")) to effectively identify, recover, analyse and present in court vast volumes of digital evidence that span multiple jurisdictions (such as complex network traffic data) are huge and the required investment in resourcing and specialist technical training comes with a significant lag-time. The reality is that the prospects of the police and/ or the NCCU and CPS currently being able to identify, apprehend, gather sufficient digital evidence and successfully prosecute a suspected cybercriminal located abroad for a cybercrime committed in the UK are remote.

Have we then, now arrived at the same juncture for serious and complex cybercrime that was reached in respect of serious frauds in 1986, with the publishing of the Roskill Report of the Fraud Trials Committee? I.e. that, "*the public no longer believes that the legal system in England and Wales is capable of bringing the perpetrators of serious frauds* [cybercrime] *expeditiously and effectively to book…the present legal system is archaic, cumbersome and unreliable?*" And might one part of the solution be for the creation of a new unified organisation responsible for all the functions of detection, investigation and prosecution of serous cybercrime? Just as it was, albeit not without subsequent criticism, with the creation of the Serious Fraud Office in 1987?

That the UK Home Secretary's recent announcement of the creation of a new National Economic Crime Centre (within the NCA) to coordinate the national response to economic crime made no explicit reference to cybercrime is perhaps an indication that the Government remains fixated on addressing the problems of 1987, rather than 2017.

---

[1] www.gov.uk/government/news/almost-half-of-uk-firms-hit-by-cyber-breach-or-attack-in-the-past-year

[2] archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Authors

Lloyd Firth

COUNSEL

lloyd.firth@wilmerhale.com

+44 (0)20 7872 1014