Cyber Crime: What does 2019 hold in store?

Cyber crime continues to make headlines, and it is very seldom good news. Whether the victim is a pensioner scammed of his savings or one of our major banks hit by a huge data breach, the general impression is one of unstoppable criminality, with perpetrators operating under the cloak of the dark net and law enforcement perpetually several steps behind.

Looking forward to 2019, is there any indication that authorities may finally be getting to grips with the constant evolution of technology in the hands of those seeking to exploit it for criminal purposes?

Cyber crime on the increase?

First, is the general perception of a cyber crime epidemic borne out by the facts? This is a far from straight-forward question. The main difficulties are the absence of a universally-accepted definition of what constitutes a cyber crime, the lack of any reliable statistics which differentiate cyber crime, in its many forms, from more traditional offending and, finally, chronic under-reporting by those affected.

In the UK, there has been a recent coalescence around a two-part definition of cyber crime: it is now generally understood to include both *cyber-dependent* and *cyber-enabled* crime. Cyber-dependent offences are those where a computer is the object of the offending behaviour, such as hacking, the deliberate spreading of viruses and denial of service attacks. The new cyber-dependent offence of cryptojacking – the practice of surreptitiously hi-jacking the processing power of someone else's computer to mine cryptocurrency for profit – has surged in popularity as a lower risk and more profitable alternative to ransomware. Cyber-enabled offences, on the other hand, are a much broader category of offending comprising crimes in some way facilitated by use of computers, including many types of fraud, cyber-stalking, malicious communications and the production or dissemination of obscene or indecent material.

The difficulty is that cyber crime is not a term which is recognised by or reflected in traditional methods of gathering and analysing crime data in the UK. As a result, it can be challenging to discern cyber crime trends against the broader statistical landscape.

Let's look first at cyber-dependent offences. The most recent report from the Office for National Statistics (ONS), for the year ending September 2018, defines cyber crime as, essentially, cyber-dependent offences. The ONS definition of cyber crime includes only offences related to unauthorised access to computers, as defined in the Computer Misuse Act 1990, to include such activity as hacking and the deliberate propagation of computer viruses. The latest report indicates a significant decrease in the order of 33% in such pure computer misuse offences. Much of the fall is accounted for by a reduction in the number of

virus-related offending, which fell by 45%, while the number of hacking offences fell by only 13%.

The trend in cyber-enabled offences, on the other hand, is more difficult to track, due to the sheer variety of such offences and the fact that they are not generally distinguished from their non-cyber variants. Crime data does not generally distinguish cyber-fraud, for example, as a sub-category of fraud more generally, or cyber-stalking as a particular type of harassment.

Cyber fraud is thought to be the most prevalent form of cyber crime. It can take many forms, including bank and credit card fraud, internet scams, mandate fraud and countless other examples of dishonest acquisition taking place via electronic means. Indeed, it is estimated that over half of fraud incidents last year were cyber-related in some way (56% or 1.9 million incidents).

The latest ONS figures show little change in the volume of fraud overall, cyber or traditional, during the period of review. However, caution must also be exercised in interpreting this data. Fraud figures are based on fraud reported to Action Fraud and two industry bodies, as well as information from the Crime Survey for England and Wales. Crime Survey data is generally considered to be a more accurate indicator of long-term trends for certain types of offences including fraud, as many instances will be relatively low-level and unlikely to be reported to the authorities. However, Crime Survey data is based on a survey of UK households: offences against businesses are not included. Only those frauds against businesses which have been reported to the authorities are captured within the ONS report. It is generally understood that only a fraction of such offences are ever reported to the authorities, typically those at the most serious end of the scale and where the business perceives that the benefits of doing so outweigh the reputational risk. The result is that, while statistics may be fairly reliable in respect of fraud against individuals, frauds against businesses – a key target for cyber criminals – are likely to be significantly under-recorded.

Many other types of cyber-enabled offending are not recorded or reported in a way which allows meaningful trends to be discerned. For example, figures on child sexual abuse and child exploitation – which were separately flagged for the first time this year and therefore cannot be contrasted with earlier years – include computer-related offending such as on-line grooming, the production of sexual images and the use of technology to exploit children. Similarly, malicious communications offences and what is commonly referred to as 'revenge porn' all fall within the stalking and harassment subcategory. While this subcategory saw a very significant increase of 41% compared to the previous year, cyber-enabled offending of this type is not differentiated from non-cyber offending and therefore cannot be separately identified and tracked.

Looking forward, it will be interesting to see whether the apparent downward trend in cyber-dependent crime continues to fall and to explore the reasons behind any such reduction. Could it be that improvements in the cyber security arrangements put in place by individuals

and firms are stemming the tide, or is it simply that that firms which are targeted by such activity are less likely than ever to report it?

Despite the inherent limitations of crime statistics on cyber-enabled offending, it is clear that, against a general backdrop of falling or stabilising crime figures, a very significant percentage of crimes in the UK today are being committed using computers and that this percentage is likely to rise. It is hoped that in future this data will in time be recorded and reported with sufficient granularity to allow a meaningful assessment of cyber crime trends to be made.

Regulation of crypto assets?

The proliferation in the number and use of crypto assets such as Bitcoin and Ethereum continued apace in 2018. Bitcoin, the best known and most popular virtual asset, celebrated its tenth birthday on 31 October last year. Has this milestone represented a coming of age for what has become known as the currency of choice for on-line drugs dealers and extortionists?

While there is of course no inherent link between crypto assets and crime, the quasi-anonymous nature of most crypto assets opens up opportunities for financial transactions to be carried out beyond the purview of the authorities: as such, they have become synonymous with the funding of illicit activities and the laundering of criminal proceeds. Further, the growth of Initial Coin Offerings (ICOs) – a method of raising capital for new business ventures from the public using crypto assets – and the high failure rate of such projects and resultant consumer losses have raised concerns as to the legitimacy of many of these schemes.

2018 saw significant steps being taken by the UK authorities towards the establishment of a regulatory framework for crypto assets as well as an increased focus on enforcement action against rogue operators. Key developments in this space over the last 12 months include:

- The publication in September 2018 of the Treasury Select Committee report on crypto assets, which recommended the introduction of regulation by way of extending the current Regulated Activities Order, under the Financial Services and Markets Act 2000, to bring crypto asset activity within its remit, in a similar way to which peer-to-peer lending was brought within the regulatory perimeter in 2014.
- The publication in October 2018 of the Crypto assets Taskforce report, the culmination of significant collaboration between HM Treasury, the Financial Conduct Authority and the Bank of England. While the report found welcomed the opportunities presented by the underlying distributed ledger technology, it noted that while there is at present limited evidence of crypto assets delivering benefits, there is ample evidence of potential risks to consumers' interests and market integrity as well as the risks associated with their use in illicit activities. The report sets out a clear route to the establishment of a regulatory framework to govern crypto asset related activity in the UK.

- Increased enforcement focus on crypto asset operators, with the FCA confirming that it is currently investigating 18 firms with involvement in the sector, having initially opened enquiries into some 67 firms. The FCA has issued a number of warnings over the course of the year, including a "Dear CEO" letter to warn banks of the financial crime risk associated with the asset class (for more information, please see our related blog post) and added crypto assets to its Scam Smart Warning List.

What are the major developments we can expect to see over the coming 12 months?

First, the government has signalled its intention to go beyond the requirements of the Fifth EU Money Laundering Directive (MLD5) to combat the risk of crypto assets being used in illicit activity. MLD5, which is due to be transposed into UK law by 10 January 2020, will bring both fiat-to-crypto asset currency exchanges – that is, exchanges which allow users to transfer traditional government-backed currency into and out of virtual currencies – and custodian wallet providers within the remit of Anti-Money Laundering and Counter Terrorist Financing (AML/CFT) legislation. During the course of 2019, the government intends to consult upon the possibility of bringing other entities within this remit, including platforms facilitating peer-to-peer exchanges of crypto assets and crypto asset ATMs, with a view to bringing in legislation by the end of the year.

Second, following on from the work of the Taskforce, referred to above, significant progress is expected to be made on establishing a regulatory framework for crypto asset-related activities. The first of these is the recently-issued FCA consultation paper which seeks views upon its Guidance on the regulation of crypto assets. The Guidance, expected to be finalised this summer, will provide greater regulatory clarity for firms operating in this space, something which will undoubtedly be welcomed by both firms and their advisers. Meanwhile, the European Securities and Markets Authority (ESMA) issued an advice on 9 January which recommends an EU-wide approach to the issue in order to limit the risks of regulatory arbitrage and to ensure adequate investor protection.

Third, following on from the FCA's work process, HM Treasury will launch its own consultation process which will canvas views upon possible legislative changes to extend the FCA's regulatory remit to encompass further types of crypto asset. This will look at whether there are crypto-based products which exhibit similar features to specified investments but which do not at present fall within the perimeter, and consider whether the perimeter should be extended to include such products.

Fourth, we can expect to see significant movement towards the prohibition or, at least, significant curtailment of the sale to retail customers of derivative products referencing certain types of crypto assets. The Guidance refers to above sets out the FCA's concerns regarding the risks associated with these highly volatile products, which formed the basis of a recent consumer warning issued by the regulator, and confirms that the FCA is to consult on a potential prohibition.

It is clear that 2019 will see significant progress towards the implementation of a regulatory framework within which crypto asset firms will have to operate. This represents a real opportunity for the UK to attract innovators within the sector while closing the regulatory gaps which less scrupulous operators have until now been able to exploit.

Enforcement action against misuse of personal data

The ICO, in its annual report for 2017/2018, confirmed that it had in that year issued the largest number and amount of civil monetary penalties in its history, as well as having launched 19 criminal prosecutions (culminating in 18 convictions) for unlawfully obtaining data under section 55 of the Data Protection Act 1998.

It is a trend which shows little sign of abating since the period covered by that report. Facebook, Uber, Equifax, Heathrow Airport and Yahoo were just some of the big names on the wrong end of hefty ICO fines for breaches in the later part of 2018. The mandatory self-reporting requirement introduced by the GDPR last year is likely to drive the number of breaches coming to the attention of the ICO and, as a result, the number of fines issued, even higher: please see here for a blog post on this topic. Under GDPR, the ICO now has the power to issue significantly higher fines – up to €20 million or 4% of the organisation's turnover, although it remains to be seen to what extent the ICO will seek to make use of its new enforcement powers: it has indicated that it intends to continue to take a proportionate and pragmatic approach, and only to resort to fines in the most serious of cases.

A striking development in 2018 has been the willingness of the ICO to investigate and prosecute criminal data breaches as a hacking offence under the Computer Misuse Act 1990 as an alternative to the more commonly used data misuse offences under the Data Protection Acts. For further information, please see here. The option of taking a case under the 1990 Act allows the ICO to pursue a prosecution which may result in a sentence of imprisonment, an outcome which is not available under the Data Protection Acts. To date, there have been no criminal convictions under the Data Protection Act 2018: it will be interesting to see how the ICO will make use of its new powers in the year ahead and whether it will seek to pursue further cases under the Computer Misuse Act.

Increased law enforcement fire power?

The last couple of years have seen a significant increase in funding for combatting cyber crime, and, importantly, an increased recognition of the need for specialist resources to tackle the particular challenges it poses.

The National Cyber Crime Unit (NCCU) is a specialist unit within the National Crime Agency (NCA) tasked with working with local law enforcement units and the industry to respond to cyber threats. It has pursued a number of high-profile investigations, most recently a crackdown on UK users of a distributed denial of service (DDoS) for hire website. The NCA's annual plan for 2018 – 2019 identifies that the primary threat to the UK continues to stem from Russian-speaking actors although it accepts that cyber crime is becoming increasingly global in nature. While the current political and diplomatic climate precludes

direct liaison with Moscow, the NCCU has recently forged links with the authorities in the Ukraine, Romania and the Baltic states in order to tackle this particular challenge. It is likely that we will see increasing international collaboration, not just with Eastern European states but more generally over the coming months and years.

The international cyber crime offensive will be further boosted by the establishment of a new joint taskforce comprising military and security services experts from the Ministry of Defence and GCHQ. The initiative, announced in September last year, signals a significant commitment to combatting the threat from Russia as well as on a domestic level. At a cost of £250m, it is set to quadruple the number of skilled UK personnel on the cyber crime offensive.

On a domestic level, specific training is to be provided to the City of London police to respond to the particular challenges of crypto asset-related fraud (a development covered in more detail here). The principle is that officers specialising in economic crime should be better equipped to deal with the particular complexities posed by this type of fraud.

Finally, the National Cyber Security Centre (NCSC), which recently celebrated its second anniversary, has become a valued part of the UK's defence against cyber crime. It is not an enforcement authority but rather a centralised resource for law enforcement, government agencies, corporates and international partners with the aim of understanding cyber security risks and promoting best practice.

Conclusion

The threats posed by cyber crime continue to increase in both number and complexity. Presenting constantly evolving opportunities for low risk and high reward criminal activity, cyber-related offending will continue to represent an increasing proportion of overall criminality.

Significant steps are now being taken to combat this threat: legislative and regulatory changes are underway, whilst increased public funding and the marshalling of specialist resources aim to increase public awareness and improve enforcement capability. The most interesting questions to consider during 2019 will include:

- Whether the number of cyber-dependent criminal offences continues to fall according to quarterly ONS crime statistics: will, for example, the rise in cryptojacking drive a reversal of this trend?
- Whether any meaningful trend in respect of cyber-enabled offending can be derived from these statistics, and in particular whether these statistics will support the popular and media perception of significant increases in such offending against generally falling or static crime statistics;
- Whether, by the end of the year, we will see a new regulatory framework in which firms offering crypto asset-related products and services will have to operate and any significant enforcement action being taken by the FCA against rogue operators. It will be particularly interesting to see whether 2019 will be the year that enforcement action is finally taken in the UK in respect of alleged Initial Coin Offering fraud;

- How the Information Commissioner's Office will make use of its enhanced enforcement powers under GDPR and the Data Protection Act 2018; and
- What if any measurable success will be achieved by the network of local and national agencies now specialising in cyber security and enforcement work in addressing the emerging threats emanating both globally and locally.

Even if significant progress were made on all these fronts over the course of 2019, cyber crime is here to stay. Aims for the year ahead should include the implementation of appropriate measures to accurately capture cyber-related trends, the creation of a regulatory framework in which the risks posed by crypto asset activities can be effectively managed, use by Information Commissioner's Office of its new powers in respect of both civil and criminal data breaches, and the establishment of an adequately-resourced and well-coordinated network of local and national agencies with the requisite specialist knowledge and experience to represent a credible line of defence.

Jill Lorimer
Partner
Criminal Litigation
T +44 (0)20 7814 1295
E jlorimer@kingsleynapley.co.uk

Jill specialises in advising individuals facing investigation and prosecution by the Financial Conduct Authority (FCA) and the Serious Fraud Office (SFO). She has developed a particular expertise in advising individuals and corporates facing investigation or prosecution for cyber-related offences, including computer-enabled fraud, malicious communications, data protection breaches and other forms of computer misuse. Jill has written and spoken widely on this topic and has a particular interest in the regulatory and criminal aspects of crypto assets and Initial Coin Offerings (ICOs).

Kingsley Napley LLP is authorised and regulated by the Solicitors Regulation Authority, registration number 500046. The firm is located at Knights Quarter | 14 St John's Lane | London EC1M 4AJ.

www.kingsleynapley.co.uk