REPRESENTATION

FRAUD ADVISORY PANEL

HMICFRS INSPECTION ON CYBER DEPENDENT FRAUD

Issued: 08 May 2019

A letter dated 08 May 2019 to Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) on its thematic inspection into the law enforcement response to cyber-dependent fraud.

08 May 2019

HMICFRS
6th Floor, Globe House
89 Eccleston Square
London
SW1V 1PN

VIA EMAIL

Thematic Inspection on Cyber-Dependent Fraud

Thank you for inviting our views on your current inspection into the law enforcement (specifically the police and NCA) response to cyber-dependent fraud. We hope our comments are informative and useful in shaping your work.

We believe that policy-makers and law enforcers have yet to fully comprehend that cybercrime is now committed on an industrial scale. The threat is diverse: from nation states to crime groups to lone individuals, from elite criminals to new and/or inexperienced ones.[1] The scale, complexity and global reach of cybercrime is fuelled by our increasing connectivity and technological advancements including (but not limited to) cryptocurrencies, cloud computing, AI and machine learning, social media, the internet of things, and the rise of e-commerce.[2] Over the next five years these developments are expected to continue to transform the UK crime landscape.[3] Globally, it is predicted that cybercrime could cost as much as US$6tn annually by 2021.[4]

In 2017/18 over one million incidents of computer misuse against households and adults were recorded by the UK Crime Survey for England and Wales. Most of these were cyber-dependent (over half were viruses, others involved hacking).[5] Computer misuse crimes referred to the NFIB by Action Fraud increased by 12% over the same period, driven by an increase in hacking of social media and email.[6] Despite this, one magistrate (with eight years' experience) told us that they had never sat on a computer crime offence or even seen one on the lists for all cases in all the courts in their region!

[1] National Crime Agency (2018). *National Strategic Assessment of Serious and Organised Crime 2018.* https://nationalcrimeagency.gov.uk/who-we-are/publications/173-national-strategic-assessment-of-serious-and-organised-crime-2018/file
[2] *Cisco and Cybersecurity Ventures (6 February 2019). 2019 Cybersecurity Almanac.* https://cybersecurityventures.com/cybersecurity-almanac-2019/
[3] National Crime Agency (2018). *National Strategic Assessment of Serious and Organised Crime 2018.* https://nationalcrimeagency.gov.uk/who-we-are/publications/173-national-strategic-assessment-of-serious-and-organised-crime-2018/file
[4] Cybersecurity Ventures (December 2018). *2019 Official Annual Cybercrime Report*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
[5] Office for National Statistics (24 January 2019). *Crime in England and Wales: year ending September 2018.* https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2018#computer-misuse-offences-show-a-decrease-in-computer-viruses
[6] Ibid.

Chartered Accountants' Hall
Moorgate Place
London EC2R 6EA UK

T +44 (0)20 7920 8721
E info@fraudadvisorypanel.org
www.fraudadvisorypanel.org

Last year the NCA reported a shift in cyber targets away from individuals to businesses.[7] The 2018 cyber security breaches survey found that two in five businesses (43%) and one in five charities (19%) has experienced a cyber security breach or attack in the last 12 months.[8] While fraudulent emails and online/email impersonation were most common, these were followed by cyber-dependent crimes such as viruses/spyware/malware, ransomware, unauthorised use of computers/networks or services by outsiders, and DoS attacks.[9]

Unless law enforcement gets a firm grip on the problem soon, and with the necessary support of Government, we are likely to face similar problems from cyber-dependent crime to those uncovered by your recent thematic inspection of fraud which identified a defeatist culture in which most cases are uninvestigated and victims are left feeling let down.[10]

Overall how effective is the law enforcement response to cyber-dependent crime? Does it have the right structures and people in place to tackle the problem?

It has been reported that until recently only 31% of UK police forces had a dedicated cyber capability.[11] On 31 March 2018 only one in 241 employees in the police workforce had a main function recorded as cybercrime investigation.[12]

In late 2017 we were told that the UK law enforcement response, particularly in relation to crimes involving cryptocurrencies, was behind the curve compared to other jurisdictions. Despite small pockets of expertise there was little opportunity to share knowledge and experience in a co-ordinated way due to a lack of strategic oversight. Inadequate training of frontline staff meant that criminality could be hidden in plain sight.[13] Officers continue to tell us that a lack of resources and skills required to tackle cyber-dependent crime, let alone cyber-enabled crime/fraud, still persist today.

Although this is hardly an adequate foundation upon which to develop an effective response, we understand that things are beginning to change. The National Cyber Crime Unit appears to have a good training programme and are at an advantage of having better resources to grow their experience, expertise and cross-border co-operation. The NCA special programme uses private sector expertise to further assist in their drive against fighting cybercrime. Other forces may benefit from the introduction of similar schemes.

On 11 April it was announced that every police force in England and Wales now has a dedicated Cyber Crime Unit with the ability to access £7m worth of funding this year to build the units, recruit

---

[7] National Crime Agency (2018). *National Strategic Assessment of Serious and Organised Crime 2018.* https://nationalcrimeagency.gov.uk/who-we-are/publications/173-national-strategic-assessment-of-serious-and-organised-crime-2018/file

[8] Department for Digital, Culture, Media & Sport, Ipsos Mori and University of Portsmouth (25 April 2018). *Cyber Security Breaches Survey 2018.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

[9] Ibid.

[10] Ford, Richard (02 April 2019). *'Defeatist' police fail to investigate fraud cases*. The Times https://www.thetimes.co.uk/article/defeatist-police-fail-to-investigate-fraud-cases-520d9k6b7. Also see the report HMRIFRS (April 2019). *Fraud: Time to Choose. An inspection of the police response to fraud.* https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/fraud-time-to-choose-an-inspection-of-the-police-response-to-fraud.pdf

[11] Action Fraud (11 April 2019). *Dedicated Cyber Crime Units Get Million Pound Cash Injection* (press release). https://www.actionfraud.police.uk/news/dedicated-cyber-crime-units-get-million-pound-cash-injection

[12] Home Office (19 July 2018) *Police Workforce, England and Wales, 31 March 2018*. Data available at https://www.gov.uk/government/statistics/police-workforce-england-and-wales-31-march-2018. Reported in The Police Foundation and Perpetuity Research (December 2018). *More Than Just A Number: Improving the police response to victims of fraud*. http://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/more_than_just_a_number_exec_summary.pdf

[13] Fraud Advisory Panel (26 September 2017). *Cryptocurrencies and Fraud* (executive breakfast briefing).

specialist officers and staff, and invest in technology, equipment and training. It is envisaged that these units will be coordinated and supported by the Regional Organised Crime Units (ROCUs) with the ability to call on extra assistance from the National Cyber Crime Unit when needed. Investment will continue through 19/20 and 20/21.[14]

While this is a step in the right direction it is far too early to assess the impact these units will have on the local and regional police response and the significance of the funding available. With law enforcement systems antiquated and not fit for purpose this may simply be just a drop in the ocean: the initial £7m investment is unlikely to go very far between 43 forces, particularly when viewed against the scale of the problem.

Ultimately, law enforcement cannot, and should not, tackle the problem alone. Cyber-dependent crime is very different to other crime types because of the nature and scale of the adversary, and the tactics, technology, and partnerships (particularly private sector and overseas law enforcement) needed by UK law enforcement to tackle it.[15] This means that a truly collaborative and 'joined up' approach is essential. However from a government perspective, no-one really seems to own the problem, even though many have an interest such as the Department for Digital, Culture, Media and Sport, Cabinet Office, Home Office, GCHQ, and Treasury.[16] This lack of ownership, in our view, is ultimately damaging to the UK economy and undermines trust in law enforcement's ability to prevent, deter, prosecute and remedy.

Does law enforcement provide a high-quality response to victims of cyber-dependent crime? How well does it investigate cyber-dependent crime?

It is fair to say that few cybercrimes receive either a proactive or reactive law enforcement response. Therefore it is unsurprising that research shows many victims (particularly businesses) lack faith in the law enforcement response to cybercrime and decide not to report to the police at all. According to the NCA only 28% of people in one survey said they had confidence in the law enforcement response to cyber-dependent crime.[17] Some businesses will insure against the risk; others won't and will simply view it as a cost of doing business instead. In order to be effective, campaigns to encourage victims to report crime need to be meaningful to the target audience. Crime reports may be helpful to law enforcement to develop a fuller intelligence picture but are not necessarily helpful to victims who want to see justice served. There is a grave danger that victims of such crimes, especially businesses, come to regard police and other law enforcement agencies as at best, ineffectual, and at worst, irrelevant.

In December 2017 Action Fraud launched a new 24/7 helpline to combat cyber-attacks, particularly cyber-dependent ones. Specialist advisors offer advice and support to businesses, charities and other organisations suffering a live attack (ie. one that is ongoing and still affecting systems and the ability to work) and pass reports immediately to the NFIB. Live attacks are sent to the relevant local police force or the NCCU for a response.[18] It was reported that during the pilot (which ran from

[14] Action Fraud (11 April 2019). *Dedicated Cyber Crime Units Get Million Pound Cash Injection* (press release). https://www.actionfraud.police.uk/news/dedicated-cyber-crime-units-get-million-pound-cash-injection
[15] Fraud Advisory Panel (05 June 2018). *The Thin Blue Line: Who is really policing cyber space?* (executive breakfast briefing).
[16] Ibid.
[17] National Crime Agency (2018). *National Strategic Assessment of Serious and Organised Crime 2018.* https://nationalcrimeagency.gov.uk/who-we-are/publications/173-national-strategic-assessment-of-serious-and-organised-crime-2018/file
[18] Action Fraud. *What to do if you are suffering a live cyber attack: a guide for businesses, organisations and charities*. https://data.actionfraud.police.uk/cms/wp-content/uploads/2018/01/Action-Fraud-cyber-attack-leaflet-4pp-A5.pdf

October 2016) 377 reports were received and disseminated to the NCCU or local forces.[19] However, we are unaware of any subsequent statistics on the use of the service and its effectiveness, outcomes or customer satisfaction. The evidence to date does not convince us that these 'calls for service' receive a satisfactory response.

How well does law enforcement help people and organisations protect themselves? How effectively does law enforcement develop and disseminate relevant guidance?

Cybercrime is often misunderstood and feared simply because the technical language and terminology used sounds so complex to the average person. While the nuances between cyber-enabled and cyber-dependent crime might be important to specialist law enforcement; most frontline officers, business people, and the general public are unlikely to differentiate between the two. Most victims are also unlikely to make a connection between two different but related cyber-attacks (one of which might be cyber-dependent). Caution is needed to avoid unintentionally marginalising these groups through the words we use when we talk about cybercrime, particularly if it comes to pass that cyber-dependent crimes are prioritised and cyber-enabled are not.

Police also need to be more open with individuals and organisations about the threats and tell them how to self-protect. The National Cyber Security Centre (NCSC) is doing good work here, particularly in relation to businesses and other organisations. So too is the City of London Police's Cyber Griffin initiative that helps businesses and individuals in the Square Mile protect themselves by providing practical and non-technical advice.[20] Government, tech companies and banks could also do more for society at large. We have long-advocated the need for a nationwide public service campaign to deliver a consistent (and repetitive) prevention message.[21] This call remains unheeded. More than two years on from the *Which?* 'super-complaint' on authorised push payment fraud we are still waiting for the introduction of new measures to protect consumers.[22] Why is it still possible to buy a computer without state of the art security and protection built in?[23] These are, in our opinion, symptomatic of a deeply rooted inertia in adequately tackling the threat.

Law enforcement must also get much better at horizon-scanning to anticipate the next threat or variation of it so that people and organisations can ready themselves in preparation. For example, CEO fraud is a growing threat to businesses. Over time it has morphed from paper to digital and will eventually use AI, becoming even more sophisticated and convincing. As early as 2007 we began warning of the risks arising from the increased use of virtual worlds, social media networks and virtual currencies[24] and followed up with an expert roundtable on virtual currencies in 2014 (which included law enforcement representation).

---

[19] SC Magazine (6 December 2017). *Action Fraud Launches 24/7 Helpline to Combat Cyber Attacks.* https://www.scmagazineuk.com/action-fraud-launches-24-7-helpline-combat-cyber-attacks/article/1473681

[20] https://www.colp.uk/cybergriffin/ We have benefited from these sessions ourselves and have also received very positive feedback from other people working within the City.

[21] Fraud Advisory Panel (2016). *Fraud Review: Ten Years On*. https://www.fraudadvisorypanel.org/wp-content/uploads/2016/06/The-Fraud-Review-Ten-Years-On-WEB.pdf

[22] This Is Money (14 February 2019). *System that makes a name as important as your bank account number when making a payment delayed until next year.* https://www.thisismoney.co.uk/money/beatthescammers/article-6704155/Confirmation-Payee-help-prevent-bank-account-fraud-delayed.html

[23] One objective under HM Government's *National Cyber Security Strategy 2016 – 2021* is that the majority of products and services coming into use become 'secure by default' by 2021. See paragraph 5.2.3. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[24] Fraud Advisory Panel (01 May 2007). *Government Should Extend Legislation into Virtual World, Says Fraud* Watchdog. (press release). Also Fraud Advisory Panel (10 November 2009). *Cybercrime – Social Networks and Virtual Worlds.* (press release).

Law enforcement could benefit from more readily using networks already established by third parties who can tailor core messages and cascade them to their own audiences. The City of London Police Multi-agency Campaigns Group is one good example of this. It brings together public, private and third sectors to collaborate and support (mostly social media) campaigns and share best practice and lessons learnt.

Finally, while we are aware of the UK Cybersecurity Strategy, we remain unconvinced on current evidence that we have properly recognised the sheer scale of the threat to individuals, businesses and the UK that these crimes pose.

We would be pleased to expand upon any of the points raised above.

Kindest regards

David Clarke
Chairman