#

#

#

18 January 2016

**Cyberspace:
Security and Democracy**

Adrian Leppard

**Why is Cyber Security such an important issue?**

The City of London Police has historically always had an expertise in fraud investigations linked to their close proximity to the financial sector. The Governments Fraud Review in 2006 put this onto a more formal footing with the creating of Action Fraud, the NFIB and dedicated fraud resources targeting the most serious crimes. The City of London Police now run this multi-million pound operation on behalf of the Government. We collate all crimes from every police force in the country and gather intelligence from a range of other private sector sources.

The public interface for this is Action Fraud, which comprises of a call centre and a web reporting tool. We are hoping the new Action Fraud IT system which will come ‘online’ next year will transform the way in which we can engage with the public and industry in particular. We analyse all the reports coming in and allocate packages nationally for further investigation. We also engage with a host of agencies in the UK and abroad and conduct a lot of disruption work to try and stop further fraud offences from occurring.

Part of our national lead role includes running a fraud academy training both the public and private sector in how to investigate fraud, and of course we investigate a lot of fraud ourselves. Our fraud teams carry over 500 of the most serious fraud investigations at any one time amounting to some £5bn of fraud. A couple of our teams are now funded by the private sector. Banking funds a team looking at cheque and credit card fraud and the insurance industry fund a dedicated Insurance Fraud Enforcement Department, investigating amongst other things, some of the most serious ‘cash for crash’ scams. Our newest team is the Intellectual Property Crime Unit focused on addressing some of the fraudulent hard goods and online scams linked to the music and video industry.

The Economic Crime Directorate is a now a £25m operation within the City of London Police, but still only represents a small proportion of the main mission to police the City the London, and protect its citizens and workers from the threat of crime, terrorism and public disorder.

This issue is important because to many, it may appear that traditional crime is falling. However, police are now facing a new challenge in offences involving the internet which are changing the face of crime in the UK. Harassment, child sexual exploitation, terrorism and fraud are all increasingly being committed by suspects with a varying degree of computing expertise.

**The problem of Cybercrime and online fraud**

Cyber fraud and online crime is growing exponentially. 70% of all fraud in the UK is Cyber-enabled, half of which we believe originates from overseas. The extent of the problem remains unseen as under-reporting is a real challenge for policing. The new British Crime Survey results which were only published this month include questions on fraud and Cybercrime for the first time. The figures are significant with some five million frauds and two and half million Cybercrimes being recorded against only seven million of all other crimes. For the first time this shows that Cyber-related offences are the common form of criminality in the UK. The challenge we face as the police is that only 300,000 are actually being formally reported. At the national level therefore, we are not sighted on the scale of the problem we are dealing with.

**Some examples of common online fraud scams used by criminals**

Unfortunately the breadth and variety of online fraud is huge. From online shopping and action sites, to investment fraud and of course cheque and credit card offences linked to identity fraud. Each month the City of London Police closes down around 4,000 entities, including websites, enabling things such as voice-over internet protocol (VOIP) phone numbers, which are fraudulent as they appear to be UK numbers but are actually linked to mule bank accounts created for money laundering purposes. There is evidence to show that criminals are using increasingly complex money laundering methods to disperse money belonging to victims in minutes.

Also, new studies show that 1 in 5 of us have been a victim of bank card fraud within the last year, which highlights a significant surge in this type of crime. It is not clear whether the recent report of ‘Dridex’ malware is related to this; however this just goes to show that the stealing of bank account details from both individuals and businesses is a popular target for criminal gangs.

**What more can be done to support the police in tackling Cybercrime?**

As we know, the vast majority of Cybercrime and online fraud either goes underreported, and what it reported cannot all be investigated due to a lack of police capacity and resourcing. The City of London Police acts as the clearing house for all investigations nationally. Cases are prioritised, based upon a decision-making tool. This takes into consideration the scale, vulnerability of the victim and a number of other contributing factors. The current capacity and resourcing of policing cannot deal with the current scale of Cyber-related fraud, and so I would agree that this is a fair statement but it should read that police fail to follow up *all* Cybercrime. In terms of what more can be done to support the police, industry needs to collaborate fully with law enforcement to tackle Cybercrime. For example, I believe that it is the responsibility of banks and other key players in the financial services industry to disclose the true extent of fraud – the importance highlighted in the recent report of ‘Dridex’ malware which has reportedly stolen £20 million from online bank accounts. Criminals are routinely getting away with it due to banks failing to notify law enforcement organisations. A collaborative approach is the key to success.

**What are some of the challenges of tackling Cybercrime at the local level?**

I think the real issue here is how law enforcement activities reach into jurisdictions where there are no formal powers. Cybercrime does not follow constabulary lines, and the scale of the problem is an issue for police. There are efforts being made on a national level to combat online fraud and Cybercrime. For example we work with the National Cyber Crime Unit (NCCU) and the police Regional Organised Crime Units and of course in London the Metropolitan Police Cyber Crime Unit. The NCCU is leading the UK’s upstream response to Cybercrime working with other law enforcement organisations nationally to target those organised crime groups who in turn are targeting the UK.

The NCCU, the City of London Police and other organisations such as the UK Computer Emergency Response Team (CERT)/Cyber-security Information Sharing Partnership (CiSP) are by supporting partners with specialist capabilities and coordinating the national response to rapidly changing Threats.

**How does Templar work with the police on the issue of tackling economic crime?**

The fact is collaboration with industry is the only route to protect society; police cannot tackle Cybercrime without the help of industry. Law enforcement, large organisations, small and medium-sized businesses, banks, academia, telecommunication and internet service providers need to make up a virtual task force. I applaud Templar’s efforts in leading a number of industry forums.

There needs to be recognition amongst all key stakeholders that Cybercrime is everyone’s responsibility. It is the responsibility of the police to stimulate industry to protect personal data and to provide advice and support. However, industry needs to start to own the responsibility; it is the only approach that is going to succeed in this type of crime. There is a lot that needs to be achieved which falls outside of law enforcement’s remit, one of which being to improve standards. Schemes such as Cyber Essentials are trying to achieve this – Cyber Essentials introduces basic controls all organisations should implement to mitigate the risk from common Cyber Threats. This includes controls such as installing a firewall, introducing malware protection (e.g. anti-virus) and patch management (e.g. Windows Update). All of this will build standards and improve industry’s Cyber maturity as a whole.

My Force, which leads on economic crime, is working with the banking sector, the National Crime Agency and the Home Office to develop a joint taskforce looking at how crime can be prevented and illicit payments stopped. We already share information on money laundering cases with the banks in order to prevent crime and to identify potential criminal networks, and are keen to do more with our partners in Europe as well.

**How the new General Data Protection Regulation (GDPR) will be help police in fighting Cybercrime**

The European Union’s GDPR plan to introduce mandatory reporting to the regulator, where organisations have suffered a serious breach, will most certainly help policing by encouraging organisations to introduce more effective information security processes. How the provision will be interpreted is still up for discussion – how do you make this practicable? There needs to be a clear definition of what the difference is between an ‘incident’ and ‘serious breach’. Also, the proposed timescale currently states that a serious breach must be reported within 72 hours. Launching an investigation takes time, and it can be hours or even days before the CERT has discovered what the nature and extent of the breach is. The challenge for industry is how you operationalise reporting, but mandatory reporting will help support policing efforts.

**How Cybercrime will be policed in the next five years**

In the next five years, I would hope to see improved skills and capabilities of officers at the local level, in order to deal with Cyber-related crimes and investigations. The Service as a whole suffers from the same capacity and skills shortage as industry, but initiatives have been introduced to try and bridge the skills gap including a limited number of new resources in regional hubs and of course new training for all staff. We also need to be innovative, for example, the police are using the support of Special Constabulary officers who work in the IT industry to provide niche expertise and skills. A number of ‘Cyber Specials’ with specialist computer skills are trained in intelligence and forensic work, and are used in search and arrest teams in order to tackle Cybercrime.

As I reach the end of my policing career, I leave a Service which is well versed in the prevention of the more visible crimes, but which needs to continue to evolve to meet the threat posed by Cybercrime, especially online fraud. Prevention is a key strategy within the police and there is a requirement to train local officers about what people can do as a minimum to protect themselves, including anti-malware techniques and up to date patching of applications and systems. We have recently launched a new strategy for the police service, ‘Fraud Protect’ which includes national, regional and local responses with ‘prevention’ as the key driver and focused on providing a better service to victims.

Whilst prevention is a priority, the reality is the police are not going to be able to wholly eradicate the problem. So, the next step is to protect more people. The primary objective for the police is to engage with victims and help them deal with their loss – whether that be financial or psychological – and to investigate the crime where practicable. I would hope to see a shift in how police approach Cybercrime to be primarily victim-focused. Statistics do not need to show how we have arrested more people, as this misses the point. Instead, we should measure success in policing by how many people we have helped protect.

Whether we are looking to take on more investigations or helping to protect local communities, there is only so much that can be achieved within the limited resources available and the competing priorities police forces are seeking to deal with. Ultimately this new crime needs new resources from government. Notwithstanding the need for policing to make further savings within public sector budgets, I hope the most recent British Crime Survey results will cause the government to consider ring fencing new funds to deal with the enormous scale of criminality being experienced by individuals and businesses in the UK.

© Adrian Leppard, 2016

Gresham College

Barnard’s Inn Hall

Holborn

London

EC1N 2HH

www.gresham.ac.uk