The Implications of Economic Cybercrime for Policing

RESEARCH REPORT CITY OF LONDON CORPORATION OCTOBER 2015

SUMMARY REPORT
The implications of economic cybercrime for policing – summary report is published by the City of London Corporation. The lead author of this report is Cardiff University.

This report is intended as a basis for discussion only. While every effort has been made to ensure the accuracy and completeness of the material in this report, the lead author, Cardiff University, and the City of London Corporation, give no warranty in that regard and accept no liability for any loss or damage incurred through the use of, or reliance upon, this report or the information contained herein.

October 2015

© City of London Corporation
PO Box 270
Guildhall
London EC2P 2EJ

www.cityoflondon.gov.uk/business/researchpublications
The Implications of Economic Cybercrime for Policing

RESEARCH REPORT CITY OF LONDON CORPORATION OCTOBER 2015

SUMMARY REPORT

www.cityoflondon.gov.uk/economicresearch
Foreword

London, as one of the world’s leading financial centres, had a daily turnover in the foreign exchange market of £2,626 billion in April 2013 – all dependent on a highly interconnected electronic infrastructure and supporting technology. Yet this same technology that underpins and enables these global transactions also opens up businesses and individuals to new risks, in particular relating to cybercrime.

The introduction of sophisticated technology has brought about a step-change in the way economic crime is committed – enabling frauds to be perpetrated at scale, at great speed, and at a distance, with no physical contact necessary between criminal and victim. It can be much harder to identify the individuals initiating crime, and often the location will be outside UK jurisdiction. These factors have resulted in a sharp escalation of such activities in recent years, bringing new challenges for policing and industry in preventing and tackling such crime.

The City of London Police is the National Policing Lead for Economic Crime, and plays a key role in proactively addressing these challenges including developing a national strategy. One major challenge has been coordinating information about criminal activity where this can be geographically widely dispersed. In addition to investigating some of the most serious frauds in the country, the City of London Police hosts the national reporting database – Action Fraud. This current research piece undertakes new analysis of data held by Action Fraud and its partner unit, the National Fraud Intelligence Bureau (NFIB) also hosted by the City of London Police. It finds that between October and December 2014 alone there were 106,681 reported fraud cases, a third of which related to banking and credit industry frauds. The median amount lost to fraudsters across all fraud types ranged from £112 lost through misuse of contracts in the telecom industry, to £38,974 lost from pension fraud. However the annual 250,000 crime reports received present only a limited view of several million crimes that are taking place within the UK annually to the cost of some £30 billion.

Under-reporting presents a challenge both in terms of research and policy responses.

City of London Police initiatives to reduce fraud include training both the private and public sector in specialist skills through their Economic Crime Academy, piloting a focused victim care unit in London – the Economic Crime Victim Care Unit - and working closely with law enforcement across the UK to share information and coordinate action. Most importantly they include the formation of new national police fraud and cyber strategies focused on prevention at a national and local level.

This research report highlights the necessity of working in partnership, both around primary prevention and building in security protection, and working with other agencies to disrupt criminal activities and pursue and prosecute offenders.

Even with these initiatives, there is much more to do. Economic cybercrime is evolving rapidly, at a scale and speed never before seen. This report provides new data and analysis around the scale of this activity and offers a comprehensive view of the challenges facing the policing and law enforcement responses. It appraises the success of different approaches to preventing and addressing crime, and presents practical suggestions with a focus on partnership working, education and awareness-raising, information-sharing across industry, and intelligence-led policing. As such it is a timely piece of valuable research that can help to shape future policies focused on combatting the growing threat of cybercrime.

Mark Boleat
Chairman of Policy & Resources
City of London Corporation

Commissioner Adrian Leppard QPM
City of London Police
Purpose of this report

The use of the internet and technology to commit economic crime has been escalating sharply in recent years, bringing new challenges in preventing and tackling such crime.

This research, commissioned by the City of London Corporation, with the support of the City of London Police, and prepared by Cardiff University, explores the nature of economic cybercrime and its implications for policing, with a particular emphasis on the current ‘Four Ps’ approach of Pursue; Prevent; Protect; and Prepare. As part of this, the impacts of economic cybercrime on individuals, businesses and government entities are considered. The research involved interviews with key stakeholders including UK and international police forces and other police representatives, underpinned by an extensive secondary research review. The research highlights the current challenges for policing economic cybercrime, identifies areas for consideration and presents practical suggestions to help effectively police economic cybercrime in the future.

This report provides a summary and overview of the research findings. The main report provides additional detail and depth on the issues explored here, and is available on the City of London Corporation’s research webpage. A Technical Annex which accompanies the main report is also available online.
The Implications of Economic Cybercrime for Policing

Introduction: As crime changes, so must policing

While conventional crimes such as theft, burglary and violence are reducing, there has been a rise in fraud and economic crime. In addition, the internet, with all the advantages for criminals of global reach, speed, new technological developments and capability for sheer scale, has provided a powerful catalyst for change as crime moves from physical to online. This has led to a rise in, and new forms of, economic cybercrime, which involves technology and/or the internet in some way.

Economic cybercrime challenges conventional policing models which are focused on detection and investigation because it represents a paradigm shift in the way such crimes can be committed. This can mean that the police and reporting statistics overlook or miss crimes where the ‘victims’ (including individuals and businesses) are unaware that they have been impacted until a later date, or might simply be reluctant to report a crime because of shame, embarrassment or risk of reputational damage. Examples include individual victims of fraudulent ticket sales, who do not realise the crime has been committed until they try to validate the ticket, sometimes months after purchase, or businesses that are reluctant to report that they have been the victim of fraud, for fear of the impact on their reputation and credibility.

These developments have led to widespread agreement that policing – both in the UK and around the world – faces many challenges in adapting and responding to these evolving patterns of crime, especially economic cybercrimes and the cyber forensic aspects of police investigations.

As economic cybercrime continues to develop and evolve in its various forms, to ensure it can be effectively targeted and reduced, the nature of policing will need to adapt its existing models. For example, to embrace more partnership working, as well as changing tactics in other areas such as a greater emphasis on prevention and disruption over traditional detection and investigation policing.

106,681 reported incidents.
Source: Action Fraud data Q4 2014
What is economic cybercrime?

Economic cybercrime largely involves obtaining, or initiating dialogue to obtain, data, goods and/or money by deception, misrepresentation or straightforward fraud through the use of the internet. Broadly speaking, the main groups that are impacted by economic cybercrime are individuals or ‘the general public’, businesses (which includes companies, banks, and industries), and government entities. This research considers all three groups, with a particular focus on individuals and businesses, including SMEs as well as large organisations.

Today, this type of crime can be understood as having three different forms:

- **Cyber-dependent crimes** – rely on networked information and communications technology (ICT), largely via the internet. Without the internet, the offending would not be possible. These can include computer viruses, distributed denial of service attacks and hacking;

- **Cyber-enabled crimes** - facilitated by these same ICT-connected technologies, but are not dependent upon them, and therefore can exist in some non-cyber form. These can include fraudulent sales through bogus retail websites;

- **Cyber-assisted crimes** - differentiated from cyber-dependent and cyber-enabled crimes, and use networked digital technologies (such as mapping applications) in the course of criminal activity which would take place anyway.

Both the cyber-dependent and cyber-enabled forms of economic cybercrime provide criminals with a globalised reach in a distributed and informational way. If the internet or networked technologies are removed, then these types of crimes still take place, but in a different form. For example, both victim and perpetrator are much more likely to be located in the same country or adjacent countries, when crimes are undertaken offline. The number of victims per criminal attempt is also likely to be lower and the means employed – in person, telephone, advert or letter – can be more amenable to investigation.

The cyber element can occur in different forms at any stage of a crime, from planning through to its execution, to the expenditure and/or laundering of its proceeds.

A third of reports (33%) relate to banking and credit industry frauds.

Source: Action Fraud data Q4 2014
What does economic cybercrime look like?

Economic cybercrime creates challenges for policing and undermines existing models for tackling economic crime, due to a number of key characteristics. These are:

- **Speed**
  Offending incidences of economic cybercrime can occur very quickly – almost instantaneously for the most part – with funds swiftly transferred, and the criminal activity ‘hidden’ or harder to detect than non-cyber economic crime;

- **Any time, any place**
  Economic cybercrime is also an activity that does not respect geographical, territorial or international borders and can be carried out anywhere in the world with an internet connection, crossing multiple jurisdictions;

- **Large scale and volume**
  The volume of crime/damage/funds transfer is much larger for economic cybercrime than for traditional frauds, due to the use of connected technologies;

- **Innovative**
  Rapidly evolving new and different criminal techniques - such as the emergence of ‘cryptocurrencies’ like Bitcoin - provide endless new avenues for money laundering, or the role of organised crime groups. In addition, technological developments and advancements provide new opportunities for criminal misuse.

What does the data tell us about economic cybercrime?

Data breaches and identity frauds have been rising steadily. E-commerce fraud losses increased rapidly in the early 2000s, especially after the rise of botnets, reaching a peak of £181.7m in 2008 before falling until 2011. Losses totalled £217.4m in 2014, when they accounted for 45% of all card fraud and 66% of total remote purchase fraud.

**Online banking frauds**

Losses to the banking sector from online banking fraud rose in 2009 at £59.7m, and peaked to a new high in 2013/14, at £60.4m. Criminals also appear to be targeting businesses more, reflected in a higher average loss per online fraud case during 2014.

**Security breaches**

In a 2015 report by PwC, 90% of large organisations reported that they had suffered a security breach, up from 81% in 2014. Small organisations recorded a similar picture, with 74% reporting a security breach, up from 60% in the previous year. Of these, 11% of respondents changed the nature of their business as a result of their worst breach. For companies employing over 500 people, the ‘starting point’ for breach costs – which includes elements such as business disruption, lost sales, recovery of assets, and fines and compensation, commenced at £1.46m on average, up from £600,000 the previous year. For small businesses, their lower end for security breach costs increased to £75,200, up from £65,000 in 2014.
Online scams

A YouGov survey (April 2013) found that in their lifetimes, approximately 500,000 UK adults had fallen victim to a dating scam; around 900,000 had been conned by a boiler room scam; 700,000 by a charity scam; 900,000 by a ‘need funds for an emergency’ scam; 700,000 by an inheritance scam and 800,000 by a lottery scam. It is also noteworthy that this data only captures incidences where the individual is aware, at the time of the survey, that they have been the victim of economic cybercrime.

A rise in reported fraud and the role of ‘cyber’

Data supplied by Action Fraud – the UK’s national fraud and internet crime reporting centre for frauds experienced by UK individuals and businesses – from the period of October to December 2014 (Q4), shows a considerable rise overall in reported fraud in the UK. Of 106,681 reported incidents, cyber-enablers were identified in a fifth of cases. They ranged from online sales (19%), email (17%), hacking (11%) and social network media (9%).

An assessment of three months’ reports to Action Fraud suggests that of cyber-related frauds reported, just over a third (34%) are cyber-assisted, half (50%) are cyber-enabled and just under a sixth (15%) are cyber-dependent.

Understanding the true scale of economic cybercrime

Reported fraud offences that use networked technologies actually appear to be relatively low as a proportion of total fraud. However, it is likely that the data underestimates the extent of cyber-involvement throughout the crime because reporting reflects only first contact by the offender. Many economic crimes involve a cyber-element at a later point – for example a phone call generated via voice over internet protocol (VOIP) might be used to make initial contact and ‘hook’ a victim, after which a fraudster will take over. Subsequently, it is not always clear to know when the fraud actually began. This relates to a wider challenge of defining fraud – is it with the initial contact or later on when an attempt to extract money takes place? Some victims are carefully groomed and often will not realise that they have been defrauded until well after the event.

A lack of reliable data

A further key barrier to better understanding – and consequently, tackling economic cybercrimes – is the lack of accurate reliable data and measurement of its nature, frequency, scale and impact on businesses, the national infrastructure and the general public². These data issues include:

- Inconsistencies in the information held between various stakeholders;
- Lack of data sharing protocols;
- Confidentiality and anonymity of respondents;
- Failure to adopt gold standard data collection practices, linked to under-reporting; and
- Knowledge and perception of victimisation.
This combines with a failure to report - or an active decision not to report - identified crimes in the first place in some instances, and therefore there is significant under-reporting of economic cybercrimes.

Many of the data problems are due to the relatively recent emergence of cybercrime and its poor capture in crime surveys and datasets. The majority of non-government British and international studies lack rigour in this area. While large-scale government surveys - such as the Crime Survey for England and Wales (formerly the British Crime Survey), the Offending, Crime and Justice Survey, and the Commercial Victimisation Survey - adopt ‘gold standard’ methodologies, they have only recently begun to systematically include questions on cybercrime. This means that it is not possible to examine trends rigorously at this point in time using this data.

Private security surveys are often based on breach data identified by vendor software, so they show only part of the picture. Official criminal justice-related datasets rely on both reported and officially recorded incidents of cybercrime, which is often insufficient as this relies on a) the crime being reported by the victims and b) accurate recording of the nature of cybercrime. In the case of the former, there is often reluctance among business to report security breaches, due to the anticipated negative financial and reputational impacts if the damage is known about or picked up by the media. Individual victims similarly may report online fraud to their bank, but not the police. In the case of the latter, as mentioned, recording of cybercrime tends to be poorly reflected in traditional data capture methods.

Given the problems outlined, it is apparent that the cybercrime data pool is currently unsatisfactory, both in terms of quality and quantity. The largest databases produced by vendors are likely to be partial and biased, while the best quality data from national surveys adopting random probability sampling techniques, can suffer from poor conceptualisation and a lack of historical questions on the topic. This represents a key challenge to developing an effective policing response.

It is however, worth noting that the forthcoming 2016 Crime Survey for England and Wales is, for the first time, due to include data collection on cybercrime. Early estimates suggest this will lead to an increase of approximately three million additional crimes reported.

Detailed exploration of surveys of cybercrime victimisation relevant to the UK (excluding vendor statistics) is provided in the Technical Annex accompanying this report (available online).
Policing economic cybercrime: the challenges

As highlighted, accurate reporting represents one of the key policing challenges, making it difficult to establish the full extent and nature of the economic cybercrime problem. This is because surveys do not adequately capture the cyber aspect of economic crime. The evidence base for how ‘cyber’ has contributed to economic crimes is therefore incomplete and weak, both today and over time. Other than cyber security vendor data, we depend on victims, or others, identifying and communicating their experience of an economic crime and also their idea about how it was done.

Cost and complexity

Other policing challenges include the cost and complexity of investigations. The geographical freedom of economic cybercrime requires cross-jurisdictional working, which is challenging in terms of the practicalities and logistics and also in the wider context of police funding cuts.

Coordinating an effective response to an international threat is particularly challenging when the nature of the threat is not fully known or understood, and develops rapidly. There are also deficiencies in database systems, competing policing priorities and concentration on local issues, as well as the need for adequate technical skills, knowledge, equipment and training. Finally, understanding the different types of ‘harm’ that economic cybercrime can cause – beyond purely physical and financial – such as mental and psychological damage, is also an important aspect to consider.

Against this backdrop, there are some key questions to be answered:

- Who within and outside policing should be involved and in what capacity?
- What should be the specific roles and responsibilities of the police, and which areas should lie outside their remit?
- What resources – in money and effort – will be considered worthwhile for greater cyber security?
- How is that security going to be organised for and/or by the huge numbers of businesses and people that are (potentially) affected?

29% of reports relate to non-investment frauds (includes online shopping and auctions (12%) and also computer software service frauds).

Source: Action Fraud data Q4 2014
Policing economic cybercrime: the current approach

The nature and scale of the challenge posed by economic cybercrime for policing is extensive and will take time and resource to address. There are however, leading and good practice examples of efforts to effectively police economic cybercrime. One example explored in this research, is the work of the City of London Police, which has adopted a significant role as the National Policing Lead for Economic Crime.

The City Police’s approach to policing economic crime to date has ranged from developing a national strategy for the policing of economic crime, through working in partnership with key bodies including the National Crime Agency (NCA), Home Office, Crown Prosecution Service and others. As part of this, the City Police has assessed local policing capabilities, to ensure that at both a national and local level, policing tactics are consistent and applied with maximum effectiveness.

The City of London Police has also expanded on the range of its activities, covering for example:

- Increasing the annual reach of the Economic Crime Academy to 1,000 delegates in 2014/15 to help police forces develop specialist skills;
- A number of victim support initiatives such as piloting a specialist victim care unit for London (Economic Crime Victim Care Unit).

In the wider policing context however, beyond these initiatives and those put into place by other forces, there is much work to do, particularly in the context of the Government’s existing ‘Four Ps’ strategy.

A fifth of reported cases involved ‘cyber enablers’: online sales (19%), email (17%), hacking (11%), social network media (9%).

Source: Action Fraud dt

---

The Implications of Economic Cybercrime for Policing
The ‘Four Ps’: Pursue, Prevent, Protect and Prepare

Both in principle and in practice, there is uncertainty about what is expected from the police and what is reasonable to expect from them in tackling economic cybercrime. The response to this conceptual problem may determine the extent to which there is a gap between the emerging fraud strategy and its delivery.

Existing Government strategy, and particularly the CONTEST counter-terrorism strategy, has four components (the ‘Four Ps Model’) and involves a multiplicity of national and transnational organisations intervening both before (‘Protect’ and ‘Prevent’) and after (‘Pursue’ and ‘Prepare’) criminal activity.

- **Pursue** – following up organised criminals by prosecution and disruption;
- **Prevent** – stopping people from becoming criminals (rather than about crime prevention);
- **Protect** – primary prevention for business and the public against serious and organised crime; and
- **Prepare** – post-event resilience for attacks and reducing the impact of crime, as well as future prevention.

Given this framework, it is useful to understand the role that the police currently play in the Four Ps Model and the shortcomings of the approach in the efforts to combat economic cybercrime.

The police role in ‘Protect’

The police currently play a relatively minor role in the ‘Protect’ function against economic cybercrime. Given the range of potential victims in the general population and in business, they have no way of identifying and reaching them before they become actual victims.

Government in general does play a role, and the private sector seeks to make profits from advertising better cyber security.

The issue is both a marketing and service delivery one. Governments have previously run campaigns in favour of specific safety requirements (whether the use of seat belts or the dangers of smoking for example) to ensure a general basic level of awareness. Such an approach may be essential to allow the police, as trusted guardians, to offer additional guidance on protective measures against economic cybercrime for business and individuals.

Compulsory built-in antivirus with automatic updates into all ICT devices might be one way forward – but this would raise issues of whose security offerings are to be taken up, and by what criteria, as well as the fact that there are sometimes technical limitations to having built-in security. Understandably, banks have avoided engaging with this issue beyond providing free antivirus, due to its complexity. Despite such free offerings to their customers, a notable (though unpublished) proportion of individuals and businesses do not take it up (presumably not all because they already have other antivirus software installed). It could be argued that encrypted online banking and communications should be a compulsory precondition of internet banking.
The police role in ‘Prepare’

The police are, and need to remain, partners with other organisations involved in both the Protect and Prepare roles. As with Police and Community Together (PACT), travel safety and other school or community-based initiatives, the broader family of policing can both inform the agenda about threats and risks, and also provide figures of authority to deliver the message to individuals and SMEs (larger organisations are already networked or have in-house expertise in this area). Proposed ‘Cyber Security Protect Officers’ will have specific roles in interventions, primarily in schools and colleges, to dissuade or divert individuals at risk of engaging in cyber-related criminal conduct, but this should include economic cybercrime as well as anti-bullying, grooming and terrorism.

The key relationship will be the police’s own networks with those agencies who are already engaged with specific sections of the community – whether Age UK, Citizens Advice or the Confederation of Small Businesses – or organisations like the Fraud Advisory Panel or North East Fraud Forum (NEFF). Such public/private partnerships are crucial as an approach. In 2015 the NEFF co-sponsored the North East Regional Cyber Crime Conference as a platform to bring north east businesses together to raise awareness of the current cyber threats and to explore means of preventing a cyber-attack within their organisations and to promote the North East Regional CiSP (Cyber-security Information Sharing Platform).

While this does not require significant staff input it will require limited amounts of funding and a clear central source of information, material and, crucially, accessible sources of both online and offline support and guidance to address specific issues.

Victimisation

Repeat victimisation has become very important as a focus of police and Prepare/Protect interventions. If those individuals and businesses more likely to be repeat victims can be identified and encouraged to improve their security and resilience, with support as required, they can be saved from harm and Pursue costs reduced (including policing and, if it gets that far, criminal justice and penal costs). Whitty (2013) for example notes that a quarter of dating scam victims had been previous victims of fraud.

Although this may not translate to other forms of cyber-enabled fraud, it seems likely that there will be a concentration of victims in some demographic and business sectors, which the police may be well placed to identify via the Action Fraud reporting tool and thus use as the basis for part of the emerging strategy. It should also be noted that the need for repeat victimisation help is not restricted to economic cybercrime: the telephone is a common method of communication for mass marketing and investment frauds.

Some progress has been made at a general level in some categories of fraud, such as mass marketing frauds, but more effort needs to be made. While segmentation work has been
undertaken for organised crime (including fraud) victimisation and enablers, there needs to be a concerted push to identify individuals and businesses particularly ‘at risk’ and to help them. This can be done for groups in advance of their becoming victims (or not) - as has recently been done to discourage frauds against those liberating their occupational pensions - and/or after they first report a fraud.

Peer influence

In addition to the use of websites and formal organisations, awareness measures may need to be supplemented from outreach by trusted (and trustworthy) persons. Peer influence and community level bodies seem particularly well placed to perform this function and it is better that such bodies proactively seek out or arrange face-to-face sessions with representative organisations – Women’s Institutes, senior citizen groups, etc. – rather than rely on vulnerable or poorly-informed individuals to use the internet for information. Organisations such as Age UK, Citizens Advice, and even a vetted group of ‘cyber-savvy’ volunteers would be appropriate service deliverers, depending on the demographic. This, however, would require a shift in skills from those used when dealing with victims of theft, burglary and violence, since the demographic of volunteers may itself need training in fraud victimisation and cyber-skills.

In short, people find advice more credible when they get it from their peers and people they can relate to. Also, they are more likely to follow security advice when it is very simple and requires little effort to implement; better still when it is conducted on their behalf by third parties like their internet service providers and social media service providers.

Finally, in addition to reducing repeat victimisation (and saving future policing and associated costs), the dimension of care for victims has begun to receive more attention. The Mayor’s Office for Policing and Crime (MOPAC) recently established a Victim Care Unit; though important, this relatively expensive resource can be applied only to a small percentage of victims. Being a victim of fraud is sometimes accompanied by guilt and self-blame; counselling and help for both mental health and practical needs is an important and under-developed area, whether the individual or business person is a first time or repeat victim. Limited research has been conducted into the impact of different forms of face-to-face, cyber-enabled or mixed mode economic crimes, but there is no reason to suppose that fraud victims are any more resilient than the victims of other crimes. The fact that the individual might have been tricked into parting with their money voluntarily does not make them less needful of help, and the social benefits of reduced fraud are significant. Some will consider fraud victims to be less deserving of help, but this does not mean that they should not be equipped with the knowledge and skills to reduce repeat victimisation. Who is available to help with these tasks and how they will be paid (if needed) and by whom, remains a difficult issue.
The Implications of Economic Cybercrime for Policing

The police role in ‘Prevent’

‘Prevent’ is the mechanism used to attempt to ‘divert’ potential criminals from committing crimes. Some potential offenders can be identified from their role in chat rooms, social media and other forms of internet presence, but the level of threat they pose may vary considerably. If the evidence suggests that they may be reaching a serious threshold, then some disruption may be attempted. Some police interviewed as part of this research highlighted the risk of longer term isolation from the labour market that might result from bringing minor offenders into the criminal justice system. Though HR and employee vetting functions may benefit from recent developments such as the Cifas Staff Fraud Database, the prediction of future harm from past conduct remains in an early stage of science.

Though there is some security information available in schools, colleges and universities, this is patchy, and issues around the morality of cyberconduct or fraud, as well as the legal requirements for data protection under the Computer Misuse Act 1990 and Data Protection Act 1998, receive little or no attention, either in general or in relation to ICT and other courses. However, resources available for a significant police or non-police role in reducing the risk of future cyber criminality are very modest, and since many of the threats come from overseas, those potential criminals or victims are not readily influenced by UK interests or by education here. This is an area of preventative intervention that needs to be worked on internationally if progress is to be made.

The police role in ‘Pursue’

Prepare, Protect and Prevent offer the police fairly minor roles and, in light of resource constraints and expertise, these roles are possibly more suitable for other institutions who can integrate these responsibilities into wider, complementary functions. Policing has, in any case, gradually shifted towards intelligence-led efforts to reach out and enhance sources of information. Nevertheless, with fraud, the police are mostly dependent on what gets reported to them by victims or third parties with guardianship roles. Unless connected with already actively monitored organised crime groups or suspected terrorists, insider threats are reactively policed by law enforcement following reports by the private or public sector. Although recorded and victim-survey measured property crimes have been falling, there are a host of other crime and non-crime demands on falling police resources, and newer or redefined issues requiring attention. These include counter-terrorism, child sexual exploitation online, modern slavery, online bullying, offline sexual grooming, and racial harassment. Against this background context, it is necessary to explore where to engage in terms of Prevent, Protect and Pursue and how to integrate it into current policing plans and priorities.

While law enforcement bodies have developed a number of relevant strategies, these strategies and their implementation by type of cybercrime and victim, need to be reconsidered in the light of the data now available. For example, the ‘cyber’ involvement can vary in the course of a crime: many cyber-enabled crimes begin online
to hook victims, but offenders may take victims offline (sometimes assisted by technology) in order to extort money; even if the victim pays in cryptocurrency, there may be a pay-out that is made offline (i.e. not connected to ICT) at a later stage, when the criminals want to realise their gains. Thus Preparation strategies need to be flexible in order to increase resilience, and Pursue strategies need to find intervention points over the spectrum of economic cybercrime, from organising the crimes to money laundering, whether their aim is prosecution, asset freezing and recovery, and/or crime disruption.

The effectiveness of promoting an emphasis within the Pursue framework on disrupting cyber-enabled crimes, which can be done either via surveillance/informants/covert human intelligence sources or by rapid reactions to crimes in progress which reduce criminals’ ‘take’ from one victim or a run of victims, is not clear. However, disruption does offer an extensive set of tools which are used in a number of other areas, from child sexual exploitation to organised crime groups. They are also used by major industry players such as Microsoft and the Federation against Copyright Theft, and by transnational police agencies such as Europol’s European Cybercrime Centre.

As early as 2011, the NFIB suspended a number of websites, telephone numbers and email accounts as well as redirecting those who accessed the suspended websites to an alert page. Disruption also allows law enforcement to take a more proactive approach in engaging with potential offenders and their networks. It can provide relevant intelligence and the basis for information-sharing that, as we have already noted, is a significant part of the development of Protect and Prepare.

Telephone (35%), websites (18%) and in person (12%) are the most common methods used by economic criminals.

Source: Action Fraud data Q4 2014
Areas for future consideration

While some progress has been made, there remains areas of challenge in the Four Ps Model, which raise a number of potential issues and questions in the context of policing economic cybercrime:

- **Revisit and refine the Four Ps Model**
  The Pursue component remains under severe pressure and has not yet received significant allocations from police resources. The other components of the ‘Four Ps’ Model also need revisiting and refining in terms of a targeted (and widely advertised) response. This research highlights the importance of reinforcing and comprehensive messages that emphasise police choices and solutions through: identifying ‘signal’ concerns; visible control – public reassurance by seeing visible proof that their problems are important to the police and are being addressed in specific ways; a targeted, intelligence-led approach focusing resources on a hierarchy of threats drawn from Action Fraud/NFIB data; joint action from the police and other partner agencies across at least three of the four Ps, and evidence of dedicated resources where practicable.

- **Greater education and awareness**
  There are challenges around victim awareness and understanding of economic cybercrime, whether amongst individuals or businesses, and the subsequent under-reporting or indeed non-reporting by victims. Arguably, a high proportion of reported crimes might not have been committed if preventative action had been taken. As part of addressing this, there is scope for a more dynamic, structured and response-focused approach to guidance, warnings and awareness-raising, to complement the valuable alerts that the NFIB and the NCA currently distribute.

  Businesses need to be incentivised to report and be reassured that doing so will not undermine their competitiveness, and that action will be taken on the back of reporting. This is increasingly being recognised through private sector partnerships and improved relationships with police forces.

- **Dealing with the negative impacts**
  How should the negative impacts of cybercrime be managed in policing? There is a need to consider the recovery of financial losses but also the emotional impacts of being a victim of economic cybercrime for individuals. The latter are harder to predict and measure, but remediation via reassurance mechanisms – including protective registration against identity theft - is possible.

- **Monitoring and protection for victims**
  Should there be a greater degree of compulsion on private and public sector bodies who lose personal and financial data through security breaches, to provide free of charge monitoring and protection to those individuals affected? This might encourage organisations to protect their data better. Even if it does not lead to greater care by organisations, one might argue that it is a right of victims that contributes to restorative justice as well as to reduced re-victimisation risks.
How much are we prepared to spend?

What are we prepared to resource for the policing of cyber frauds, especially as these types of fraud increase as a proportion? Evidential rules and judicial attitudes may need to change before the private sector can play a bigger role. Policing has to balance resources with other crime and social problems. This is of enormous difficulty for the police, the NCA, the security services, and the general public and businesses of all sizes.

Evidence-based judgements

There is a need to manage the risks by making evidence-based judgements about trends in offending and impacts on different sectors of the population, directly and via business and government.

Action Fraud as a centralised reporting structure is a key step forward in collecting intelligence and data to inform policing.

Despite some limitations, the available data, particularly that from Action Fraud, can provide a foundation for more evidence-based policy with which to refresh and refine existing strategies and approaches.

How might the police respond to these challenges?

It is important that cyber-dependent and cyber-enabled economic crime are established on the policing agenda and in ways that allow a meaningful and realistic response, where the role of the police is less about being the sole player in the law enforcement landscape. This needs to be more about identifying specific roles and responsibilities in that landscape, alongside equally realistic assessments of the roles of other agencies and the promotion of partnership and other arrangements.

This will require a careful analysis of resources, police priorities and engagement with other agencies to complement police roles. A more coherent, joined-up approach should be taken, addressing those economic crimes that by volume, value, harm and/or severity of threat, and identification of the organisation and location of perpetrators, appear to pose the biggest risk, while acknowledging that the rest might be left unpursued. This approach would undoubtedly be unpopular across a range of people, including politicians, the media, and sections of the public. However, demonstrating that the police could do more with the same, with the aim of achieving greater resource provision, might help address this.
Additionally, there are a series of other measures that could improve the policing effectiveness of economic cybercrime:

- **Review Home Office guidance**
  A review should be undertaken of the 2004 Home Office guidance on fraud acceptance criteria for fraud generally, and economic cybercrime in particular, now that Action Fraud and industry data paints a much clearer picture of current risks and threats; the NFIB’s case screening rules go some way towards this goal.

- **Help Protect and Prepare individuals and SMES**
  For individuals and SMEs, the dominant thrust of policy and action should be in the Prevent, Protect and Prepare sphere, with the police developing coherent strategies, coordinating identification of key risks and threats from data, preparing communications materials, developing response packages for individual forces in relation to the most common and harmful economic cybercrimes, identifying relevant partnerships and associations with their respective constituencies, and promoting better arrangements for cybercrime victims (for both care and reducing repeat victimisation).

- **More information-sharing with large organisations**
  For large organisations, there is a need for promotion and participation in information-sharing and police/government/industry guidance on emerging threats and trends around which the organisations can develop their responses, while establishing across English and Welsh police forces, sufficient resource and expertise to provide some assurance.

- **The aims are to increase appropriate business and customer confidence in the security of the internet and offer some credible downside risks to cyber-criminals, including freezing and confiscation of the proceeds of cybercrime, in countries of operation and offender residence.**

- **A change of police tactics**
  The traditional police approach of investigate and report should give way to a focus on prevention and disruption of websites as policing tactics.

- **More presence and partnership working**
  There is a need to develop a hierarchy of law enforcement responses focused on reassuring businesses and the public of the presence of law enforcement in this space, as well as investigating and prosecuting the perpetrators where feasible and likely to have the greatest deterrence impact. More partnership working is also required; police forces in the UK, and internationally, cannot work in a silo. Police forces also need to work more closely with industry and the private sector.

- **Improve proactive and reactive responses**
  Improve levels of proactive as well as reactive responses to the same levels and focus that policing has taken in other areas - such as organised crime and corruption.

  Additionally, the police response should involve intelligence-led policing – access to big data and information-sharing across organisations and sectors, as well as a change to police recruitment practices and role requirements, and a drive for greater innovation and creativity.
Conclusions: police and public responsibilities

While economic cybercrime is not an insurmountable challenge to policing, it is necessary to think critically about what can be achieved with existing resources; a sentiment recently expressed by the head of the National Police Chiefs Council. Even if a ‘reasonable’ amount of extra resources were available, this would not solve a large proportion of the investigations into cyber-enabled economic crime, nor would greater investigative success alone substantially reduce the levels of such crime. When combined with the fast-paced nature of economic cybercrime, and the ability of cybercriminals to innovate and commit crimes at rapid speeds, at high volume, and to great scale, it is clear that policing economic cybercrime is a key challenge for now and the future.

The public needs to accept some responsibility for its susceptibility to internet and telephone-enabled offers from strangers, acquaintances and even from people thought to be friends. But the public deserves and needs to be helped to make better decisions, and the police can play a collaborative role in arrangements to provide that advice before and after becoming a victim. A start might be made by asking – for every economic cybercrime – what it would have taken to have stopped it from happening or to have reduced its scale, and then to see who – victim awareness, software or internet service providers, third parties or police/other enforcement agencies – might have intervened to affect those harms, and why they did not either attempt to or succeed.

Ask, ‘is it too good to be true?’

For public reassurance and for deterrence/incapacitation of criminals, some police action is needed and more up-skilling from existing officers is necessary. This could include disruption of suspected frauds-in-action via banks, families, and money service bureaux - though the potential victims themselves might resist if they do not accept that they are in the process of being defrauded. For the rest, we need to prepare for a long struggle against local and transnational criminals using the internet and the telephone to extort us, to deceive us into thinking we are dealing with genuine organisations, or who persuade us that their offers are not ‘too good to be true’. Indeed, for us to ask ourselves that question would itself represent progress.

It is important to realise that all countries, not just the UK, are grappling with these difficulties. The substantial problems of economic cybercrime, which have been far from eliminated by policing and prevention efforts, arise across the world. We are in the early stages of a long struggle to reduce cyber risks and economic crimes generally, and we would do better to think of this practically and feasibly in terms of better risk management rather than risk elimination.
The Implications of Economic Cybercrime for Policing

Better early education

The suggested next steps include the need for better early education of risk management (relevant for not just economic crime but also child exploitation and bullying online). We also need to focus on helping vulnerable citizens to appreciate and manage the risks of both online and offline fraud, and this may be done better via peers and the third sector than by the police and websites alone, however user-friendly. For both individuals and businesses, we need a focus on security that is built into products and online interfaces, that is not obstructive, and is explained clearly to people.

Median amounts of money lost to fraudsters ranged from £112 to £38,974 per victim.

Source: Action Fraud data Q4 2014
Endnotes

1 See: http://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Pages/default.aspx

2 Several papers provide insightful reasons why existing data are flawed (see for example: Anderson et al., 2013; Anderson, Böhme, Clayton, & Moore, 2008; Casper, 2007).


4 As highlighted by preliminary research into the association between autism and cybercrime, and international law enforcement, following a rise in cybercrimes involving individuals with autism. See: http://www.emeraldinsight.com/doi/10.1108/AIA-05-2015-0003

The Implications of Economic Cybercrime for Policing

RESEARCH REPORT CITY OF LONDON CORPORATION OCTOBER 2015

SUMMARY REPORT

www.cityoflondon.gov.uk/economicresearch

CITY OF LONDON

CARDIFF UNIVERSITY

POLICE