Crime Law Soc Change (2017) 67:77–96
DOI 10.1007/s10611-016-9648-0

Cyberfraud and the implications for effective risk-based responses: themes from UK research

Michael Levi[1] · **Alan Doig**[2] · **Rajeev Gundur**[3] · **David Wall**[4] · **Matthew Williams**[5]

Published online: 20 October 2016

Abstract The nature of the risk or threat posed by 'cyberfraud' - fraud with a cyber dimension – is examined empirically based on data reported by the public and business to Action Fraud. These are used to examine the implications for a more effective risk-based response, both by category of fraud and also responding to cyberfraud generally, not just in the UK. A key characteristics of cyberfraud is that it can be globalised, unless there are major national differences in attractiveness of targets or in the organisation of control. This does not mean that all cyberfraud is international, however: not only do some involve face to face interactions at some stage of the crime cycle, but in online auction selling frauds, it appears to be common for the perpetrators and victims to reside in the same country. After reviewing patterns and costs of victimisation and their implications for control, the paper concludes that any law enforcement response must begin by being strategic: which other public and private sector bodies should be involved to do what; what should be the specific roles and responsibilities of the police and where 'problem ownership' should lie; what are we willing to pay for (in money and effort) for greater cybersecurity and how to reduce 'market failure' in its supply; and, how that security is going to be organised for and/or by the huge numbers of businesses and people that are (potentially) affected.

We are grateful to the City of London Corporate for funding this research and to the City of London Police and Steve Strickland for their substantial assistance with the project.

✉ Michael Levi
Levi@Cardiff.ac.uk

[1] School of Social Sciences, Cardiff University, Wales CF10 3WT, UK

[2] Northumbria University, Newcastle upon Tyne, UK

[3] Social Policy and Criminology, University of Liverpool in Singapore, Singapore, Singapore

[4] Centre for Criminal Justice Studies, Leeds University, Leeds, UK

[5] School of Social Sciences, Cardiff University, Cardiff, UK

Introduction

This article looks specifically at the nature of the risk or threat posed by 'cyberfraud', fraud with a cyber dimension. By examining cybercrime for financial gain, it will seek to develop an outline of the implications for a more effective risk-based response, both by category of fraud and also responding to cyberfraud generally. While the dataset upon which this article draws relates to England and Wales, the article is not focussed exclusively on those countries, but upon what the authors suggest are the main risks and threats in any context experiencing an increase in cyberfraud and the steps needed to enhance the effectiveness of risk-based responses. One of the key characteristics of cyberfraud is that it can be globalised, so what is found in one jurisdiction tends to also be found in another, unless there are major national differences in attractiveness of targets or in the organisation of control. This does not mean that all cyberfraud is international, however: not only do some involve face to face interactions at some stage of the crime cycle, but in online auction selling frauds, it appears to be common for the perpetrators and victims to reside in the same country.

Financial and other risks and threats to current and future 'Internet of Things' and 'Big Data' processes in the 'cyber' world are ever present and constantly evolving (see [1]). Regular national and global cyber 'threat assessments' and state-wide Cyber Security Strategies add to the 'awareness-raising' process that puts the probabilities or impacts of certain forms of victimisation on the public agenda with varied degrees of sophistication [2]. Action (pre and post-victimisation) increases demands on law enforcement for resources for investigation and prosecution (while also enhancing the sales of the cybersecurity businesses that have been spawned by the rise of e-commerce and social media).

In this market for understanding threat, risk, and effective responses, it is difficult for most consumers, businesses, government organisations, and commentators to work out a 'rational' response or responses, not least because there is a lack of reliable data on the problem, and little helpful agreed evidence on 'what works' and on who has both the capacity and the motivation to reduce vulnerability [3]. Moreover, given the often transjurisdictional nature of cyberfrauds, there is difficulty in acting against perpetrators, especially because both vulnerabilities and perpetrators are dynamic and responses need regular updating in order to be focused and effective. A key challenge has been the lack of accurate data and measurement of the nature, scale and impact of cyberfraud, largely due to the relatively recent emergence of cybercrime on the criminal justice agenda and its poor capture in existing crime surveys and datasets [4]. Notwithstanding, some areas of business risk have good commercial surveys by vendors and advisers. Nonetheless, it is arguable that there is a significant risk that law enforcement and other resources target the wrong crimes, fail to instil confidence in victims and potential victims in their ability to prevent cybercrime from occurring or are unable to respond effectively because of the nature of the crime and the lack of a suitable evidence base for assessing impact. Indeed, there is often confusion over whether any guardianship component or mix of components of reassurance policing, target hardening, enhancing resilience, or pursuing offenders constitutes 'effective policing' of cyberfrauds [2].

The optimal enforcement response is also influenced by changes to crime control in the UK which was once widely seen as virtually the sole domain and responsibility of law enforcement, but which in the past two decades has moved towards 'plural policing' in partnership with other agencies [5]. This shift has resulted in a new emphasis on partnership and information-sharing; between and across jurisdictions; the framing of responses to crime in terms of prioritising on the basis of harm, disruption, prevention and reduction; the production of explicit and measurable policies, strategies or 'policing plans' which are themselves ostensibly the result of analyses of crime patterns and trends; the application of intelligence-led policing; and the consideration of the priorities of central and local government, other agencies and local communities [6, 7]. Levi & Williams [8] in their study of cooperation within the UK Information Assurance Network evidence that the neo-liberal rationality that has been evoked in other areas of crime control is also evident in the control of cybercrimes. However, they find divisions exist between the High Policing rhetoric of the UK's Cyber Security Strategy and the (relatively) Low Policing cooperation outcomes in "on the ground" cyber-policing.

In the area of fraud, which also includes cybercrime for financial gain, similar imperatives also apply in terms of law enforcement responses to the public, as well as public and private sector institutions, who may approach law enforcement with allegations of criminal conduct or financial loss. An awareness of investigation policies and the reduced availability of resources within the police service, other institutions and regulators, as well as a requirement to follow a broad range of government-initiated policies has seen the police commit ever-fewer resources to high-volume, low value cases. This also applies the more elite forms of fraud such as insider trading and corporate accounting frauds. The shortfall in resources raises questions as to the extent to which the police are able to address the growing threat from cybercrime for financial gain, which has long been a problem for fraud generally [6, 9, 10].

Establishing an evidence base

Given the lack of resources available for responding to cybercrime in general and cybercrime for financial gain in particular, we must continuously develop our understanding of the range of risks or threats facing victims – corporate, governmental or individual - and tailor roles and responses accordingly, to the extent that there are sufficient resources to fulfil those roles. To that end, identifying the evidence base on which to predicate law enforcement roles as well as responses of those of other organisations (including the relevance and added-value of cybersecurity businesses) is necessary in order to develop an effective response.

Some data about offenders can be derived from investigating the circumstances and techniques for criminal activity (see this volume), but the evidence is inadequate to test the hypotheses that, for example, cybercriminals are more financially motivated than in the past when they were more likely to be motivated by gaining kudos; or that traditional, analogue criminals – particularly drug traffickers, burglars and robbers – are digitizing their offending habits by turning to the more sophisticated forms of cybercrime in significant numbers, beyond what can be done comparatively easily from 'crime-as-a-service' software kits [11, 12]. There has also been little evidence on the

relationships between types of crime, losses incurred, or the nature and level of cyber involvement; certainly police recorded data have been poor and/or partial in their coverage, leaving little scope for credible refutation of hostile media stories about cybercrime risks and bank/police handling of complaints. Currently criminal statistics as well as business and individual victim surveys show that fraud in the UK is on the rise, while the crime rates for other types of acquisitive crime are falling. However, the evidence base for how 'cyber' has contributed to fraud has been incomplete and weak, both today and historically. Since ICT platforms have become central to the way business and social life is organised, routine activities models lead us to expect that crime follows these changes when the opportunity is easily exploitable.

A much more detailed picture of UK cyberfraud has recently emerged as a consequence of improved law enforcement reporting arrangements (which is patchily present in other countries also). In the UK, following a review of the UK institutional approach to fraud, there is now a centralised reporting process for all actual and attempted fraud allegations, including those involving a cyber dimension. However, the effectiveness of this process is dependent on victims' awareness that they have been defrauded and willingness to spend the time making reports. The review recommended that there should be a National Fraud Reporting Centre as a sole central reporting point for members of the public and both public and private sectors ([13]: 7). This body is located within the City of London Police, which was designated as the national lead law enforcement agency responsible for policing fraud.

Currently renamed 'Action Fraud', the Centre was linked to an intelligence analysis resource: the National Fraud Intelligence Bureau (NFIB), also located with the City of London Police. In 2013, Action Fraud was rolled out nationally. Since 2014 all fraud complaints to the police, unless an immediate response is required for a 'crime in action', have to be recorded through Action Fraud and not locally. Action Fraud collects data for reported frauds by UK individuals and businesses, excluding reports for 'plastic crime' which is collected by CIFAS and FFA UK, to avoid double counting.[1] The former is a member-based fraud prevention service while the latter coordinates information from, and preventative approaches for, some sectors of the financial services industry The NFIB role has been to synthesise and analyse the data from these three sources in order to assess patterns and trends, as well as directing intelligence packages to the most relevant police force, although it has no control over what those individual forces do with its packages, an issue in common with other police intelligence bodies including CIFAS and FFA UK .

For a research project intended to explore the implications of economic cybercrimes for a law enforcement response [11], the authors were given access to Action Fraud data for all fraud and fraud-related offences, including offences recorded under the 2006 Fraud Act and 1990 Misuse of Computers Act, for October to December 2014. This analysis of the *reported* cyber dimension of fraud enabled a detailed picture to be drawn of the types of frauds reported and, with access to the reporting information, the

[1] For 2013–14 CIFAS and FFA UK sent to the NFIB data on 'card not present' fraud, lost or stolen cards and ATM fraud, representing over two-thirds of the total of over 333,000 reported offences and, while most will involve a cyber dimension, the data are not differentiated in the same way as Action Fraud data. This will continue to be the case despite the integration of those commercial sources into the crime statistics (see Levi, this volume).

mode of commission of the alleged crime to assess the issues faced by law enforcement, organisations and the public.[2]

What is cyberfraud and what is the 'cyber' component thereof?

There is a distinction between cybercrime intended solely to harm – such as online harassment, hate speech and child sexual grooming – and cybercrime for financial gain, including cyberfrauds and extortion. There are three main aspects of cybercrime in relation to fraud [14]:

- **Cyber-dependant crimes** which would not exist without the internet;
- **Cyber-enabled crimes** which, if the networked technologies were removed, could still take place but locally and on a more one-to-one basis. Being cyber-enabled allows these crimes to be carried out at scale for less capital and sometimes with fewer criminal staff than would be needed for similar crimes offline; and
- **Cyber-assisted crimes** which use networked digital technologies in the course of criminal activity which would take place anyway.

In focussing particularly on the latter two dimensions of cyberfraud (as the data will show, cyber-dependent crimes are not the main source of cybercrime for financial gain), one of the questions also addressed through the data in seeking to identify where the cyber element occurs, in what forms at any stage, from the planning of a crime through to its execution, to the expenditure and/or laundering of its proceeds.

What is the scale of, and the threat from, cyberfraud in the UK?

This study preceded the extension of the national statistics to cover a broader range of cyber-related frauds in England and Wales (ONS [15]; Levi, this volume). Overall, there were 106,681 reported incidents in the dataset provided to the authors by Action Fraud[3] - of these, 4062 (4 %) involved computer misuse crime, a much smaller proportion than might have been expected, perhaps because people whose systems become infected by malware do not bother calling Action Fraud, if indeed they are aware of it and see it as a prelude to fraud against themselves or others. The two largest components of computer misuse crime involved malware, and hacking of emails and social media.

The analysis of the data suggested that well over half of incidents were significantly cyber-related: 43 % were cyber-enabled, 13 % were cyber-dependent, while a further 29 % of them simply used technology (cyber-assisted); see Table 1.

[2] The analysis of the data was supplemented with interviews with principal agencies for economic crime control, financial services and industrial firms, cybercrime prevention bodies in the public and private sectors, and police officers (retired and current) across the UK.

[3] There are some inconsistencies in the Action Fraud data relating to the total number of cases; this is due to missing data although totals match up closely wherever possible. It is also worth highlighting that the analysis presented in this report is not comparable to official ONS analysis due to different datasets covering different time periods.

Table 1 Cyber-involvement

	Numbers	% of all	% of cyber-involvement
Cyber-assisted	30,759	28.8 %	34.2 %
Cyber-enabled	45,293	42.5 %	50.4 %
Cyber-dependant	13,859	13.0 %	15.4 %
Not applicable	16,773	15.7 %	
Total	106,681	100.0 %	100.0 %

By volume, the single largest types of reported fraud are banking and credit industry frauds (33 %), a large proportion of which (18 %) are cheque, payment card and online bank account frauds. This is followed by non-investment frauds (28.6 %), which include online shopping and auctions (11.6 %) and also computer software service frauds (7.9 %). The latter, which may be categorised as cyber-dependent crimes, may include, for example, fake antivirus and ransomware fraud. Advance fee frauds (and their different forms) follow (14.1 %). Specific technology-related offences are less prevalent, covering telecom industry fraud (misuse of contracts) at 4.5 %. The remainder of the offences are relatively small in volume.

Table 2 presents data for reported crime by volume by category (including the two largest sub-categories within each).

Analysis of the reporting information suggests that, despite the global figures in Table 2, the cyber dimension is much more nuanced. The data highlights that the internet has not always been the source or medium of the initial contact that led to a fraud. The single most common way that offenders first contacted their victims was by phone or text (35 %). Almost a fifth (18 %) were contacted after visiting a website, 12 % in person, letters and fax (11 %) and 8 % by email. From these data, the overall

Table 2 Typology of reported frauds

Fraud type	Number of frauds	Proportion of total reported frauds
Banking and credit industry fraud	34,913	32.7 %
Cheque, plastic card and online bank accounts (not PSP)	19,127	18 %
Application fraud (excluding mortgages)	10,091	9.5 %
Non-investment fraud	30,490	28.6 %
Online shopping and auctions	12,405	11.6 %
Computer software service fraud	8455	7.9 %
Advance fee payments	15,065	14.1 %
Other advance fee frauds	7498	6.7 %
Lender loan fraud	2078	1.9 %
No identified category	12,404	11.6 %
Categories as % of total	92,872	87 %
Total	106,681	100 %

degree of involvement of network technologies can be estimated, though with some caveats,[4] and are summarised in Table 3.

The data prima facie suggest that frauds using networked technologies are actually relatively low as a proportion of the total of frauds reported. However, it is likely that the data actually underestimate the extent of cyber-involvement throughout the crime, because the data derived from the reporting stage reflect only first contact by the offender. Also, many cyberfrauds are 'micro-frauds', very small impact bulk victimisations that are too small individually to pursue, even if reported ([16]:68). It was also found that whilst many economic crimes involve a cyber-element at a particular point, for example emails or phone calls generated via voice over internet protocol (VOIP) might be used to make initial contact and 'hook' a victim, after which the fraudster will take over and monetise the victim's personal information. Subsequently, it is not always clear for Action Fraud classifiers, or indeed for reporting victims, when the fraud actually began or at what point the cyber component occurs. This relates to a wider challenge of defining fraud. Is it at the point of initial contact, or later on when an attempt to extract money takes place? This is different from the distinction between attempted and realised fraud; some victims are carefully groomed and often will not realise that they have been defrauded until after the event, if at all.

Nevertheless, the data do provide a clear indication of the different levels of cyber-involvement in the different offences although, at this point, they do not reveal the role played by ICT in the offences: this can only be seen when it is cross-tabulated by fraud type. In the early stages of Action Fraud, reported offences that use networked technologies are relatively rare. When the data are ordered according to the level of estimated cyber-involvement, they cut across[5] a number of the Action Fraud data headings: see Table 4. The data – which are reported quite fully to emphasise the variations by crime type of frauds other than cyber-dependent ones – allow us to assess the degree of estimated cyber-involvement for specific types of fraud and help to better understand where ICT is involved. However we caveat that the judgements about cyber-involvement made by victims or report classifiers should be treated with substantial reservation.

Thus, on the one hand, if a targeted response is being considered from the data, then traditional '419' advance fee payment frauds are found to be very low in cyber-involvement (15 %), whereas others, such as dating/romance scams (88 %) and online shopping and auctions (86 %) have the largest cyber component. But the data have limitations. So, within advance fee payments, the first contact method for lottery scams suggests 8 % cyber-involvement; dating scams involve fewer cases but suggest 88 % cyber-involvement; lender loan fraud represents nearly 14 % of all advance fee payments, but only 17 % cyber-involvement on first contact method. Furthermore, it is not

[4] Percentages are indicative rather than absolute, and are adjusted for cyber-involvement (email + visit to a website + web forum + (0.66) of TV, radio or online advert, or flyer) ('in person' and 'other' have been excluded). Classification depends on when the victim feels the fraud began, e.g. at first contact, or the point at which money was being requested. With most frauds today, online usually goes offline to get the money. Blanks are excluded and percentages are based upon total known information. 'Simplified' means main offence and information are joined. As the table illustrates, the Action Fraud headlines format is not very useful in demonstrating cyber-involvement.

[5] Our analysis orders the fraud types in terms of cyber-involvement via first contact. Including all of the types of cybercrime (assisted, enabled, and dependent), it is calculated from the combination of the following values (email + visit to a website + web forum + (0.66) of TV, radio or online advert, or flyer) ('in person' and 'other' have been excluded).

Table 3 Frauds by first contact method by offender

Contact method	Number of frauds	Proportion of total reported frauds
Phone call, text message or similar	31,088	35 %
Visit to a website	15,587	18 %
Other	11,625	13 %
In person	10,932	12 %
Letter or fax	10,159	11 %
Email	6859	8 %
Web forum, chat room or similar	1582	2 %
TV, radio or online advert, or flyer	462	1 %
Newspaper, magazine	179	0 %
Total	88,473	100 %

immediately apparent which offences are cyber-enabled and which are cyber-dependent. Data are insufficient to develop horizontal or vertical analyses of perpetrators, specialisms, networks or interactions, or information sources for exploitation, although repeat victimisation requires such networks.

From the Action Fraud data, however, it is also possible to identify which types of fraud are most lucrative for the fraudster, especially where the most money is lost by the victim. Although it is worth noting that to generate criminal *profits* data we would have to know about operational costs to offenders and how many victims over what period they had defrauded, which might span several jurisdictions. In many cases, even with criminal network analysis software, it is unlikely that this information can be deduced from victimisation data alone, unlinked to identified (but not necessarily caught or convicted) offenders. It is, however, possible to calculate the median financial losses by the main categories of fraud: medians generate less distortion of the data than the figures alone or means, though there is still potential for inaccuracies. These victim cost data are presented in Table 5.

The data in the Table reveal that the most money was lost by corporate rather than by individual victims through pension fraud, business trading fraud, financial investments, and bankruptcy and insolvency fraud. On the other hand, more reported cases have individual than business victims. There is no clear relationship between the volume of cases and the value of financial losses, nor between those involving individuals and organisations. Nor is there a clear relationship between either of these and the level of cyber-involvement in a fraud.

The data provide some useful graded indications of the self-assessed impact of fraud upon the victim,[6] enhance our understanding of the victims' perspectives and thus helps

[6] The City of London police graded self-assessed harm into the following categories: a) 'Concerned about the fraud but it has not impacted on health or financial well-being'; b) 'Minor - only a small impact on either health or financial well-being'; c) 'Significant - impacting on health or financial well-being'; d) 'Severe - have received medical treatment as a result of this crime and/or at risk of bankruptcy'. There is an 'other' category, which is where the impact is either unknown or not deemed relevant to reporting the case.

Table 4 Level of cyber-involvement in cyber-enabled and cyber-assisted frauds (Offender First Contact Method)

Action Fraud category/sub-categories	Total	Cyber-involvement	% of Cyber-involvement
Dating scam	835	737	88 %
Online shopping and auctions	11,350	9754	86 %
Counterfeit cashiers' cheques	559	428	77 %
Rental fraud	773	572	74 %
Ticket fraud	910	655	72 %
Mandate fraud	966	520	54 %
Mortgage related fraud	144	69	48 %
Fraudulent applications for grants from charities	9	4	44 %
Business trading fraud	124	38	31 %
Other regulatory fraud	72	22	31 %
Prime bank guarantees	12	3	30 %
Other consumer non-investment fraud	4703	1358	29 %
Fraud by failing to disclose information	160	46	29 %
Pension fraud by pensioner (or their estates)	7	2	29 %
Charity fraud	238	63	27 %
Insurance broker fraud	39	10	26 %
Pyramid or Ponzi schemes	164	38	24 %
Other fraud	11,553	2250	19 %
Cheque, plastic card and online bank accounts (not PSP)	13,437	2449	18 %
Consumer phone fraud	352	61	18 %
Fraudulent applications for grants from government funded organisations	41	7	17 %
Other financial investment	1017	170	17 %
Bankruptcy and insolvency	18	3	17 %
HM Revenue and Customs (HMRC) fraud	6	1	17 %
Lender loan fraud	1929	319	17 %
Other advance fee frauds	6794	1017	15 %
Inheritance fraud	743	109	15 %
'419' advance fee fraud	550	80	15 %
Door to door sales and bogus tradesmen	1242	170	14 %
Banking and credit industry fraud – information	3637	495	14 %
Share sales or boiler room fraud	387	44	11 %
Dishonestly retaining a wrongful credit	32	3	11 %
Corporate procurement fraud	33	3	9 %
Pension fraud committed on pensions	24	2	8 %
Insurance related fraud	253	20	8 %
Lottery scams	1238	97	8 %
False accounting	133	9	7 %
Fraud recovery	368	26	7 %

Table 4 (continued)

Action Fraud category/sub-categories	Total	Cyber-involvement	% of Cyber-involvement
Time shares and holiday club fraud	219	15	7 %
Application fraud (excluding mortgages)	6350	428	7 %
Retail fraud	1660	109	7 %
Fraud by abuse of position	500	29	6 %
Pension liberation fraud	230	12	5 %
Telecom industry fraud (misuse of contracts)	3194	119	4 %
Corporate employee fraud	451	12	3 %
Computer software service fraud	7813	167	2 %
Department of Work and Pensions (DWP) fraud	9	0	0 %
Passport application fraud	1	0	0 %

Table 5 Median amounts given to fraudster by victim

Fraud type	Estimated loss to fraudsters per victim[a]
Pension fraud	£38,974
Business trading fraud	£28,609
Financial investments	£21,534
Bankruptcy and insolvency	£20,000
Fraudulent applications for grants from government-funded organisations	£11,500
Fraud by abuse of position of trust	£8100
Corporate fraud	£3869
Department of Work and Pensions(DWP)Fraud	£3298
False accounting	£2000
Other regulatory fraud	£2000
Banking and credit industry fraud	£1721
Insurance fraud	£1084
Advance fee payments	£784
Computer misuse crime	£536
Fraud by failing to disclose information	£440
None of the above	£420
All charity fraud	£390
HM revenue & customs fraud (HMRC)	£281
Non-investment fraud	£274
Telecom industry fraud (misuse of contracts)	£112

[a] The table illustrates the amounts lost to fraudsters per victim. It is estimated by using the *median* rather than the *average* because the averages are skewed by large standard deviations, and often estimations of loss. The Advance fee frauds, for example, are numerous and yield relatively small amounts to fraudsters. The data field is skewed because of some large entries, so, to correct for these, the median has been used to demonstrate the difference

to prioritise action (in combination with judgments of how feasible a case will be to take forward to criminal justice). This analysis is presented in Table 6. It shows that the types of fraud with the most impact on the 'victims' are: 'pyramid or Ponzi offences', followed by 'dishonestly retaining a wrongful credit', 'fraud by abuse of position of trust' and 'pension frauds'. By comparison, offline retail fraud has the lowest impact on victims (perhaps because it is likely to be reimbursed via payment card firms). Again the degree of cyber-involvement associated with each type of offence, is highly variable, although cyberfrauds against individuals registers as the most significant in terms of harm.

Notwithstanding the limitations from identification and reporting, the data do point to where the biggest threat from cyberfraud lies (and thus one of the grounds for deciding if this should be one of the main foci of any cyber-related law enforcement response). On the other hand, those categories reflecting the biggest losses – such as pension, business trading and financial investment frauds - are areas where cyber-enablement or cyber-dependency was not an obvious significant factor. Those offences with significant cyber-involvement seem to vary in both number of cases, average loss and likelihood of realistic levels of recovery (where such data is available), as shown in Table 7. The data also show that some of the financial loss of frauds is unlikely to be recovered for the victims (though the number of cases where recovery is known is a small percentage of the total, and the true position is likely to be much worse).

Table 8, conversely, shows that those areas where the greater (mean or median) amounts are likely to be recovered are in the business or public sectors (such as DWP, HMRC, business trading fraud or false accounting) where cyber-involvement is low (the highest level of cyber-involved first contact method was less than 16 %).

Overall the data provide an evidential basis for understanding which frauds have the greater and lesser levels of cyber-involvement, to illuminate some considerations – and challenges – for developing any effective risk-based responses by law enforcement.

Table 6 Fraud impact levels by self-assessed severity

Fraud type	% of severe	Harm factor[7]	% Cyber-involvement
Pyramid or Ponzi Schemes	74 %	2.87	24 %
Dishonestly retaining a wrongful credit	73 %	2.73	11 %
Other financial investment	70 %	2.77	17 %
Fraud by abuse of position of trust	70 %	2.76	6 %
Rental fraud	68 %	2.70	74 %
Pension fraud committed on pensions	67 %	2.80	8 %
Lender loan fraud	66 %	2.68	17 %
Dating/romance scam	64 %	2.65	88 %
Other regulatory fraud	62 %	2.67	31 %
Bankruptcy and insolvency	60 %	2.80	17 %

Table 7 Estimated median amounts lost to, and recovered from, the fraudster by highest levels of cyber-involvement[a]

Fraud type (sub-categories)	% of Cyber-involvement	Estimated median loss per victim (£)	Estimated median recovery per victim
Dating/romance scam	88 %	£2595 (n = 528)	£1700 (n = 27)
Online shopping and auctions	86 %	£210 (n = 9329)	£160 (n = 483)
Counterfeiting cashiers' cheques	77 %	Not known	£305 (n = 36)
Rental fraud	74 %	£980 (n = 603)	£700 (n = 28)
Ticket fraud	72 %	£450 (n = 897)	£528 (n = 32)
Computer virus/malware/ spyware	71 %	£100 (n = 191)	£132 (n = 48)
Denial of service attack	55 %	£605 (n = 6)	£6 (n = 1)
Mandate fraud	54 %	£9820 (n = 682)	£3845 (n = 32)

[a] The number of cases may differ because: a) the recoveries may be from a different time period to the losses; b) there are fewer recoveries than losses because i) there are simply fewer recoveries ii) recoveries from any given set of losses may arise in subsequent time periods iii) there may be inaccuracies in the reporting process (e.g. the losses may be overestimated, or the person who lost the money may not know that it was recovered, say by someone else, such as a bank)

The implications for an effective risk-based response: what do the data tell us?

The data provide only a 'snapshot' insight into cyberfraud, showing that ICT plays a substantial but far from exclusive role in criminal fraud. Before commenting further, we would note two negative or unresolved issues that inform the imperfect nature of the picture the data presents.

First, the data are not completely accurate. The cyber component of reported fraud is ill-represented as a standalone data field. Hard to capture (even for the victim) is when the fraud involves different types of networked technology, such as VOIP through the phone system, enabling offenders to engage cheaply and less identifiably than with traditional technologies with victims online. While cyber-enabled or cyber-dependent economic crime appears to be just over a quarter (27 %) of Action Fraud reports, other

Table 8 Average amounts (median and mean) recovered from fraudsters

	Amount recovered		
Fraud type	Median	Mean	N
Financial investments	£7107	£39,958	150
Banking and credit industry fraud	£1621	£47,542	966
Corporate fraud	£988	£35,863	47
Pension fraud	£24,244	£30,904	10
HM Revenue & Customs Fraud (HMRC)	£40,141	£40,141	2
Fraud by abuse of position of trust	£1629	£20,882	30

indications suggest that cyber-assisted crime is around 60 %. Furthermore, it is mistaken to see crimes in a binary way as either online or offline because many start online, until a victim is hooked; then the fraud may go offline. Other crimes stay online all of the time – at least prior to cashing out the proceeds - for example, many dating/romance scams and some other advance fee frauds, and most computer misuse crimes.

The second issue is the lack of information on perpetrator profiles and their organisation or interaction, information sources and approaches. Victims seldom know to what extent 'organised crime' is involved or whether those involved are highly computer literate or rely on crimeware-as-a-service where cybercriminals access online specialists to supply to them the means, such as malicious software, supporting infrastructure, stolen personal and financial data. The data especially do not allow easy identification of how far the same groups or individuals operate different frauds, how far they specialise, whether (or how) they share approaches, software or lists of potential victims (repeat victimisation is a noteworthy feature of cyberfraud), how they network, organise or cooperate.

Despite respondents' beliefs at the time of reporting that 97 % of 'their' offenders were in the UK, we also know that the geographic location of the perpetrators, or the locations for different aspects of the crime, including servers, is very difficult to identify – with all the attendant difficulties of investigation and prosecution where there is an overseas dimension. In other words, the crime scenes, as well as the likelihood of access to documents, witnesses and equipment, are less clear than the data make them appear to be.

On the other hand, the Action Fraud data do reveal a complex and nuanced picture of cyberfraud with significant but specific types of cyber-dependant, cyber-enabled and cyber-assisted crimes, information on losses and number of incidents, differentiated patterns of cyber-involvement and the impact on victims. We can argue that cyber-enabled fraud reflects much greater financial losses than cyber-dependant crimes, whose losses are more likely to be incurred through payment for business disruption and recovery. In particular we would note in terms of responses:

- There is a high level of cyber involvement in reported cases of fraud, but there is no established pattern of what crimes are cyber-involved, or who carries them out;
- Cyber-involvement is an elastic term, given its role among a number of other media in initiating and perpetrating frauds;
- Financial losses can be substantial by case, by crime, but there are variations – not all cyberfraud results in significant losses and not all frauds involve ICT (except perhaps in the trivial sense that financial transfers usually are electronic, whatever form they take);
- Even in those industries with well-established prevention and protection approaches, such as financial services, the level of reported cyberfraud and cybercrime remains high, though much is prevented;
- The level of loss recovery from cyberfrauds is relatively low (as it also is from other crimes: see [17]).

The key point from the data is that the main perception or fear of cybercrime relates to denial of access, disruption and loss of data and identifiers (see [12]) but, in practice, few of these result in actual immediate and direct financial loss to victims. There is a

substantial level of high-volume, often low-value, cyberfraud with varying degrees of harm, in which the cyber component varies by crime. This heterogeneity can and should influence law enforcement responses, but not in a simple way either for prevention or for offender pursuit.

The implications for an effective response: what are the main issues for any law enforcement response?

From the victim perspective, the data do address some significant policy- and law enforcement-related issues within the volume-value-category-cyber matrix: the majority of cyberfrauds are high-volume, low value with low levels of recovery, usually targeted at individuals. Thus we need to be concerned not merely whether or not a differentiated response is required at national and local levels, but also whether such a response requires a reactive investigative response and/or a technical-led investigative capability; whether the emphasis should be on awareness and education and how should any response balance volume, loss, harm, perpetrator or deterrence as the main drivers of any response. Such a response should also take into account the empirically tested effectiveness of individual and national level reduction mechanisms [2].

Second, and not unique to cyberfrauds, any response has to take account of a landscape that changes dramatically as networked technologies transform the way that fraud could be organised, as cybercrime has become more professional, harder to identify and/or recognise, and provides anonymity for offenders, at least under normal conditions, without significant forensic investigation efforts that are highly limited in absolute availability and cost. An emerging and dynamic cybercrime threat landscape that challenges policing is the human-centred interactive ecosystem of the Social Web where the threats posed by cybercrime frequently elude more traditional approaches to policing.[7] Activity conducted via the Social Web represents a new frontier for national and international security and crime fighting, yet such interactive spaces remain largely unregulated. Given the scale, international reach and open nature of the Social Web, the police struggle to meet an expectation of protection from the public, due not just to resources and skills but to a perceived lack of actionable intelligence on emerging cyber threats. As technologies become cheaper and more widely available, the increase in global internet penetration, new users, activities and products will be incorporated into what is now a global online community, growing the pool of both potential victims and criminal actors. Easier access means a greater proportion of users than previously may be unfamiliar with technologies, making them 'easy targets' both as intermediaries for (e.g. botnets, money mules) and as victims of fraud.

Third, the Action Fraud reports and other data from CIFAS and FFAUK suggest that cyberfrauds have been rising, though the lack of comparable data for previous years makes this a matter of very plausible interpretation rather than demonstrable fact (see Levi, this volume). Given the rise in the number of Internet-enabled devices and the proportion of the population who are connected, it would be a surprise if this were not

[7] Examples of the Social Web include online interactive mainstream media, interactive blogs, and the suite of technologies often referred to as social media.

so. Given a large number of people around the world with the motivation to defraud and so many situational opportunities outside their domestic jurisdictions that the internet now provides, it may be impressive (but not reassuring) that the reported cyberfraud rate is not higher. Strategic planners need to consider what it would take to produce a much higher (or lower) cyberfraud rate.

The data also indicate that there are significant variations in the impact of cyberfraud by crime category and even within the latter, there are non-trivial variations in the level of cyber involvement in the crime, in the types of victims (whether businesses or individuals), the interplay between cyber involvement and other communication modes for the commission of the crime, and the losses associated with the crime. Such variations have implications for effective risk-based responses.

The implications for an effective response: what should be the main considerations for policy?

First, as it is the sovereign responsibility of the state to protect its citizens, including its critical national infrastructure, financial services, key commercial intellectual property and government secrets, against cybercriminals, including other national governments, it is a reasonable demand to require government to provide the necessary state response, requiring the engagement of the intelligence agencies, strong and effective intra- and inter-country collaborative, information-sharing and support networks. Certainly it would be expected that any national government develops a strategy that seeks to address cybercrime and to identify those government and other agencies to whom specific roles and responsibilities, as well as resources, could be devolved.

Second, given the trends and approaches to both policing and to fraud, as noted above, there is likely to be a clear limit to the reliance on an open-ended law enforcement response, and to a reliance solely on law enforcement to respond, given the median amounts involved, the investigative and evidential accessibility, the low likely recovery of the proceeds of cyberfraud, and the problematic nature of both crime scene and geographic location of perpetrators. Clearly policing cyberfraud involves a multiplicity of national and transnational actors intervening both before and after the criminal activity: but it is not clear how far law enforcement, given its competing agendas and resources, can investigate cyberfraud that has – or may have - international dimensions which are not readily penetrable on a routine basis.

Third, there may be a symbolic need for law enforcement to show particular criminal networks and individuals that involvement in crime has its costs, even if – as has been shown in the rapid revival of alternative drug and identity data cryptomarkets following take downs such as DarkMarket, Silk Road and Onymous (see Décary-Hétu and Giommoni, and Dupont, this volume) – the impact on crime and precursor availability is modest. Target audiences may include not just the immediate offenders but others at home and abroad, and also potential perpetrators, victims and potential victims who may need reassurance and/or a continuing message of intent. Similarly, the technical knowledge from investigations and inter-country cooperation would be essential inputs into organisations in both public and private sectors to ensure their in-house capacity is informed with credible awareness and alert campaigns. If part of the police reaction is to be intelligence -led and proactive, how is this to be achieved? What kinds of fresh

and existing sources can be deployed to get a better and quicker picture of offending and offender networking than exist at the present?

Fourth, we are persuaded from the Action Fraud data that relatively little of the reported cyberfraud lends itself to a traditional reactive law enforcement response, though it may be susceptible to specifically targeted significant awareness and prevention campaigns ('Protect' and 'Prepare' in the jargon of the Home Office) that aim to encourage new and bolster existing individual level security behaviours, some of which have been shown to be effective in reducing cybercriminal victimisation [2]. Even once messages are disseminated, on radio, television, the press, and via friends and families, however, there are always some that do not follow the advice or who wrongly interpret the message and engage in economically damaging avoidance behaviours, and consideration may have to be given to automated security with opt-out rather than opt-in requirements (for example, for on-line banking), especially if insecurity can cause problems for others, like botnets.

Here we suggest also that further research, like that of Williams [2] on the effectiveness of individual level security behaviours, and behavioural studies on mechanisms of security adoption, be done on national longitudinal datasets where they exist. Such research would help identify what needs to be done to enable and nudge such people to take action to protect themselves and make better informed judgments, whilst allowing them to continue to enjoy the benefits of the internet. Certainly the imperfect information on the nature, motivation and geographic location of the perpetrator, as well as the limited likelihood of any law enforcement intervention would require a 'nudge' to financial and other services to be more proactive in requiring the use of mandated software, if only to encourage more security awareness and less self-determination among businesses and the public, particularly for those who do not have a common understanding of what to do to protect themselves, and why.

There is scope for a more dynamic, structured and response-focused approach to guidance, warnings and awareness-raising, including the identification of and support for organisations and media sources that have an established engagement with individuals who may thus be more predisposed to listen. Similarly, there is a role for law enforcement or other approved bodies to set up educational 'mock operations' to warn users who respond to fraudulent offers of different kinds (created by the authorities) that they could have become victims of fraud, via on-screen 'pop ups' (such tactics could also be used on criminal marketplaces as warnings to those seeking illicit products or co-offenders on the web.) This may have particular resonance for repeat victims.

An effective response: what should be the overarching themes?

Overall, we are not in a position to offer a fully-evidenced effective risk-based strategy to address risk and threats where there is no clear answer from the data, but we would argue that the Anglo-Welsh case study provides a basis for continuing dialogue on these important social and economic issues, which touch an ever-increasing proportion of the population in the UK and elsewhere.

If we are asked to consider that would be a general optimal law enforcement response in the light of these data, and bearing in mind the problems that law

enforcement, organisations, and governments will continue to face in cost to pay-off questions vis-à-vis cybercrimes, we would argue that this must range from the internet server and services providers actively developing means to promote secure use and reduce the risk of threat of economic loss, to using transnational criminal justice to render the most damaging cybercrimes unprofitable, and to engaging users and customers in a proactive awareness of prevention and protection. Further, any role in cyberfraud reduction shows the need for clarity in tasking and in the messaging from strategic, operational and symbolic police actions. Assessing the cost, impact or added-value of investigations or prosecutions, disruption and asset recovery on domestic and foreign offenders remains in its infancy (see Dupont and see Décary-Hétu & Giommoni, this issue; see also [18, 19]): but it needs very careful consideration for each case, particularly in terms of cross-border intelligence and cooperation arrangements. In addition, and in line with contemporary approaches to partnership/'plural' policing and engagement with stakeholders and communities of interest, attention needs to be given to the roles and responsibilities of the network of relevant agencies and industries (the UK Information Assurance community, including Cyber-security Information Sharing Partnership initiatives -https://www.cert.gov.uk/cisp/) and to a realistic assessment of what they may be better placed to provide, or able to offer in the way of complementary support [8]. This is a dynamic process, and the negotiation of agreements and resourcing are a necessary but not sufficient condition of actual cooperation.

There is an important self-interest not only in organisations taking their own initiatives to address cybercrime but also in coordination and cooperation between organisations, where the law enforcement role will be primarily one of disruption and occasional deterrence, as well as providing guidance and information on emerging risks and threats, issues particularly true of small to medium enterprises (SMEs). Larger organisations often have dedicated ICT departments and are better informed of the risks and threats. They are also likely to be able to afford the appropriate resourcing responses. For them, the issue is less of awareness and education, or even having access to law enforcement resources to investigate and prosecute fraud, than access to specialist guidance on threat and risk profiles and types to design and deploy responses, leaving law enforcement to identify and take action against the identifiable groups who initiate the more significant or recurring cyber-attacks against them. For SMEs, dedicated awareness and educative responses are required [8]. A combination of experience to increase perceptions of risks and having mitigations/solutions in place would likely help overcome the resource, expertise and scepticism barrier for the majority. It is important here to consider the need for 'knock-on' effects, such as through the supply chain, which can generate systemic weaknesses if not addressed. It may also be important to supplement such responses with specialist guidance and advice on a planned basis.

Of much more concern is addressing the same challenges at the level of the individual victims where, as the Action Fraud data suggests, the majority of cyberfrauds by number, though not by value, take place. Any strategy for policing cyberfraud needs to have a significant educative component that is intelligible (a) to victims and intended victims and (b) to those in a position to monitor behaviour and provide relevant advice. Such an approach also has to recognise and reflect the specific characteristics of the crime itself. People have to have a common understanding of what

to do to protect themselves, and why, know what to do and to actually carry out these measures and review them over time. Cyber-fraud prevention is not a one-time effort, and both online and offline social engineering seeks to move potential victims away from the protections they might know about in the abstract to their informed use in practice.

There is scope for a more dynamic, structured and response-focused approach to guidance, warnings and awareness-raising, and the police can play a collaborative role in arrangements to provide that advice before and after individuals become victims. For public reassurance and for deterrence/incapacitation, some police action is needed and more up-skilling for existing officers – or employing specialist civilian staff - is necessary. Some 5000 police have been given a modest amount of training via the College of Policing, and this is a beginning. Our suggested next steps for this include the need for better, early education of risk management and a focus on helping vulnerable citizens to appreciate and manage the risks of both online and offline fraud, and this may be better done via peers and the third sector than by the police and websites alone, however user-friendly.

Conclusion

The routinisation and pervasiveness of internet use has made certain types of internet-based crimes for economic gain possible (cyber-dependant economic crimes), and has facilitated immensely the scale of others (cyber-enabled and cyber-assisted economic crimes) by reducing the cost and effort of reaching out to potential victims. Cyberspace content is constantly evolving, for an extensive range of functions, services and products, while also providing platforms for aggregation and innovation, in the perpetration of cyberfraud. Cyberspace has multiple criminal actors living in many jurisdictions whose typologies and methods of organisation and operation do not lend themselves easily to existing definitions and understanding, e.g. in terms of 'hotspots' analysis.

Cyberspace is developing its own criminal marketplaces and financial arrangements, some of which require specialist awareness and access to address. The perpetration of cyberfraud outstrips current preventative and other measures for control protection and has increased the difficulties of identifying, investigating and prosecuting offenders as much as it has increased vulnerabilities among businesses, governments and to individuals (including the general public). There is widespread agreement that policing in the UK and also around the world has fallen behind the curve of evolving patterns of crime, especially cyberfrauds and the cyber-forensic aspects of police investigations. The latter is expensive and time-consuming, even disregarding the enormous forensic resources for child sexual exploitation online.

Given the very differentiated and nuanced nature of cyberfraud, however, it is clear that any response, including that of law enforcement, must be a collective and strategic approach with the intention of: Increasing the effort the offender must make to carry out the crime; increasing the risks the offender must face in completing the crime, including cashing out the proceeds; reducing the rewards or benefits the offender expects to obtain from the crime; removing excuses that offenders may use to rationalise or justify their actions; reducing incentives, opportunities and access to expertise that may tempt

or incite offenders into criminal acts; increasing the awareness of potential victims of the need for prevention and understanding of risk; increasing the roles and responsibilities of internet providers, and organisations who provide services through the internet, in building in security and building in buy-in from users, customers, etc.; and balancing guidance, reassurance and deterrence in a way that appears to recognise and respond, cost-effectively, to the evidence base of the risk and the threat, an evolving process.

Cyberfraud harms the interests of almost all licit business, government and individuals, though not equally. The need for a law enforcement response is unquestionable in principle but is hedged by a plethora of issues and limitations in practice, and is not feasible for a large proportion of frauds. In this context, we would argue that any law enforcement response must begin by being strategic: which other bodies should be involved to do what; what should be the specific roles and responsibilities of the police and where 'problem ownership' should lie in terms of cybercrime and cyberfraud; what we (and sub-sets of 'we') are prepared to pay for (in money and effort) for greater cybersecurity; and, how that security is going to be organised for and/or by the huge numbers of businesses and people that are actually and potentially affected, that will broaden further with the risks posed by the Internet of Things. We argue that the UK case study provides some grounded data on which to take these issues forward, although we would also caution that many initiatives are emerging rather than comprehensive and well-established in a developing dynamic commercial environment. Whatever measures are adopted, it is unlikely that they will be simple harm reduction processes (like wearing seat belts) but will need to evolve with both private and public sector governance.

References

1. Williams, M. L., & Burnap, P. (2016). Cyberhate on social media in the aftermath of Woolwich: a case study in computational criminology and big data. *British Journal of Criminology, 56*(2), 211–238.
2. Williams, M. L. (2016). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology, 56*(1), 21–48.
3. Williams, M. L., & Levi, M. (2015). Perceptions of the eCrime controllers: modelling the influence of cooperation and data source factors. *Security Journal, 28*(3), 252–271.
4. Levi, M. and Williams, M. L. (2012). eCrime reduction partnership mapping study: final report. Cardiff University. Available at: http://www.cardiff.ac.uk/socsi/resources/Levi%20Williams%20eCrime%20Reduction%20Partnership%20Mapping%20Study.pdf.
5. Crawford, A., Lister, S., Blackburn, S., & Burnett, J. (2005). *Plural policing: the mixed economy of visible patrols in England and Wales*. Bristol: Policy Press.
6. Levi, M., & Maguire, M. (2012). Something old, something new; something not entirely blue: Uneven and shifting modes of crime control. In T. Newburn & J. Peay (Eds.), *Policing: politics, culture and control*. Oxford: Hart Publishing.
7. Maguire, M., & John, T. (2006). Intelligence-led policing, Managerialism and community engagement: competing priorities and the role of the National Intelligence Model in the UK. *Policing and Society, 16*, 1.
8. Levi, M., & Williams, M. L. (2013). Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space. *Information Management & Computer Security, 21*(5), 420–443.
9. Doig, A., & Levi, M. (2013). A case of arrested development? Delivering the UK National Fraud Strategy within competing policing policy priorities. *Public Money and Management., 33*(2), 145–152.
10. Gannon, R., & Doig, A. (2010). Ducking the answer: fraud strategies and police resources. *Policing and Society, 20*(1), 39–60.

11. Levi, M., Doig, A., Wall, D., Gundur, R., & Williams, M. (2015a). *The implications of economic cybercrime for policing. Report*. London: City of London Corporation.
12. Levi, M., Doig, A., Wall, D., Gundur, R., & Williams, M. (2015b). *The implications of economic cybercrime for policing. Technical Annexe*. London: City of London Corporation.
13. Attorney General (2006). Fraud review. London: Office of the Attorney General, http://webarchive.nationalarchives.gov.uk/20120816224015/http://www.lslo.gov.uk/pdf/FraudReview.pdf.
14. Wall, D.S. (2005). The internet as a conduit for criminals. In A. Pattavina (ed), Information technology and the criminal justice system (pp. 77–98). Thousand Oaks: Sage (revised 2015) Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=740626.
15. ONS (2016). Overview of fraud statistics: year ending Mar 2016. London: Office of National Statistics.
16. Wall, D. (2010). Micro-frauds: virtual robberies, stings and scams in the information age'. In T. Holt & B. Schell (Eds.), *Corporate hacking and technology driven crime: social dynamics and implications* (pp. 68–85). Hershey, PA: IGI Global.
17. Home Affairs Committee (2016) Proceeds of crime: Fifth Report of Session 2016–17. London: House of Commons
18. Metcalf, L. and Spring, J. (2015). Blacklist ecosystem analysis: Spanning Jan 2012 to Jun 2014, http://www.sigsac.org/ccs/CCS2015/, pp.13–22.
19. Spring, J. (2014). Modeling malicious domain name take-down dynamics: why eCrime pays. https://resources.sei.cmu.edu/asset_files/ConferencePaper/2014_021_001_88269.pdf.