eCrime Reduction Partnership Mapping Study

Michael Levi, PhD, DSc (Econ) & Matthew Williams, PhD
Cardiff University 10/9/2012

Cardiff Centre for Crime, Law and Justice
Cardiff School of Social Sciences
King Edward VII Avenue
Cardiff
CF10 3WT
+44 2920 874376 and +44 2920 874853
Levi@Cardiff.ac.uk and WilliamsM7@cf.ac.uk

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

CONTENTS

PREFACE BY RT HON ALUN MICHAEL MP

How can we deal with the challenge of crime and nuisance behaviour in the fast moving, changeable and border-busting world of the Internet?

That is the challenging question to which no adequate answer has yet been given. This report is a significant step towards defining the answer.

Most crime control measures have some costs as well as benefits, and to get the balance right when dealing with the challenge of minimising the use of the Internet for criminal activity it is necessary first to face up to the challenge of "Internet Governance". Sadly governance is something that grabs most people's attention only when things have gone wrong. The governance of banks interested only a minority of people until the banking collapse forced every country and pretty well every individual citizen in the world to pay a part of the price of a catastrophic failure of governance.

We cannot afford a failure of the governance of the Internet either, yet although the potential exists for a far more mature and effective form of governance than the "real world" has ever achieved, far too little interest is taken in this issue by governments or parliaments or by business. And that is why it is essential to ask whether a partnership model for reducing crime and nuisance on the Internet is the right model to promote.

There are two tests of governance:

- Is a better and fairer society created and nurtured?
- Is the potential of individuals and organisations to do harm controlled to a broadly acceptable level, in a broadly socially acceptable way ?

Other tests, including communication, innovation, profit and health, are secondary to these two major considerations which are basic to social and economic development.

Designing the right model of governance for the Internet is far from easy: The community that uses the Internet is international by nature, its speed of development has been unique in the history of the world, there is a temptation to treat it as "different from everything that went before" - and yet both the opportunities it throws up and the challenges it poses are essentially and inherently human in their nature.

So it's not surprising that two radically different social paradigms have their adherents:

- The Internet's current structure of organisation depends on a company management system whose licence derives from a US Government Department, and a conservative or neoliberal approach – reinforced by First Amendment 'free

speech' rights - idealises the "freedom of the Internet". There has been an instinctive defensiveness within US politics and business saying "if it ain't broke, don't fix it". That used to be the approach to banking too, until we realised that it *was* broke – we just didn't realise it until it was too late.

- The alternative - promoted particularly by China, Brazil and some other countries - is to argue that however light the touch from one "owning government", it is unacceptable and must be replaced by "international ownership" through a UN agency. Whatever the merits of that argument in the abstract, anyone who has observed international bureaucracy at work will harbour deep doubts as to whether any international agency could possibly have the necessary flexibility, speed of action, understanding of diversity and the capacity to deal with complex issues …. and be able to sustain those capabilities consistently over a long period of time.

And that is why at the World Summit on the Information Society in 2005 a third way was adopted - seeking organic development based on "enhanced co-operation" with people and organisations working together through "dynamic coalitions" of the willing. This concept of a multi-stakeholder process was given embodiment in the annual Internet Governance Forum (IGF) event. In turn regional and national IGF partnerships developed and are now arguably more important than the single annual event itself.

The UK IGF was one of the earliest and most ambitious of these regional and national approaches to Internet governance, and from day one we set out the challenge of asking whether this partnership approach could tackle the "nasty stuff" such as crime and exploitation on the Internet.

There was general acceptance that threats to the infrastructure and major crime required action by national governments and their agencies, primarily through international co-operation. But the "Internet community" was clearly becoming a community that included most people in the world in terms of potential engagement and direct or indirect impact.

Fraud and crime and nuisance activity that may not threaten the national or international infrastructure - and therefore lack political potency at national and international level - may nevertheless make use of the speed and universality of the internet to do enormous damage or have massive impact through a multiplicity of small impacts.

So Internet crime reduction and Internet crime prevention, we believed, must be a major area for political and business attention. While the many benefits of the Internet are widely acknowledged, it is essential to the test of whether a 21st-century co-operative model (the multi-stakeholder model of governance) can work to show whether it can cope with crime.

This indeed is central to the challenge of making the best use of the Internet - maximising its use for public, social and economic good and minimising its use for harm – which has been a major preoccupation of the past decade. But while governments engaged with the tricky question of who should "own and manage" the Internet through the two World Summits on the Information Society, there was less attention paid to the issues of governance.

In the debate between the two polarised views mentioned above, the UK played a significant role in trying to develop the alternative option of a co-operative approach. We should be proud that our officials won the argument for an approach which travelled under the ugly title of "multi-stakeholder partnership", behind which lies the beautiful concept of a constant striving for consensus and social harmony, or at least ongoing social accommodation.

That whole approach is now under serious challenge on the international stage and it would be a tragedy if it loses out to the more inflexible and top-down diktats of international bureaucracy, with its tendency to atrophy. It is to the credit of Parliamentarians and business leaders in the UK that issues relating to the Internet and its governance have been given significant parliamentary coverage. An annual debate has been achieved by an All-Party Parliamentary Group (PICTFOR – the Parliamentary Internet and Communications Technology Forum) with the encouragement of its presidents, the Speaker of the House of Commons and the Lords Speaker. Internet related crime is one of the issues on which PICTFOR's work has been complemented by the engagement of Parliamentarians, Industry contributors and others through the policy development organisation EURIM (The Information Society Alliance). Nominet and a number of other industry organisations have demonstrated a commitment to pursuing the public interest.

But that wish to make progress and to define a partnership approach to Internet crime prevention and harm reduction has been frustrated until now by the lack of a proper analysis and framework. Encouragement by ministers in the last government and in the present government gave me a sense that it was worth pursuing the concept, but efforts by a number of industry and expert contributors demonstrated just how frustratingly difficult it would be to map both the activity and the potential alliances that would be effective in this endeavour. We didn't seem to have the ability or capacity to do it.

At that point the consistent and continuing encouragement of Nominet - whose contribution in the public interest right across the gamut of Internet governance issues has been extraordinary - was complemented by financial support from the Nominet Trust.

An expert international seminar hosted by the Oxford Internet Institute provided the launch-pad for a piece of serious academic study, commissioned from Prof Michael Levi and Dr Matthew Williams of Cardiff University.

The work was not easy and starts with an acknowledgement that "high-quality data on eCrimes are hard to find both nationally and internationally". That is true. Those involved in the field can frighten the fainthearted with stories of the immense power available to crooks who go online. The potential for individual acts of damage is overshadowed only by the speed and immense number of hits that can be achieved on the Internet. But this is the stuff of fairytales to frighten the children, rather than factual evidence which empowers people and organisations of goodwill to make the Internet a better and safer place.

This report, by contrast, provides precisely the carefully argued evidence about the potential for action in partnership that we have sought for so long. The recommendations underline the importance of a strategy for the domestic domain and the crucial public-facing value of Get Safe Online. It highlights the sort of work that is needed as part of a shared strategy, and it develops the evidence base to the point that Ministers have been searching for over a number of years.

Until now, Industry has waited for a lead from Government and Government has looked for a lead from Business. Realistically, neither can do it alone and nor can either an agency of government or a partnership or association within the business sector. If ever there were a topic for joint action and mutual support across sectors, this is it. It must be a partnership with appropriate governance - rather like the groundbreaking approach to child abuse online through the Internet Watch Foundation - so that Government takes an appropriate leading part, Business provides the cutting-edge technical and developmental expertise and both welcome the engagement of Parliament and Civil Society to provide legitimacy of scrutiny and to make up the essential four-part structure of governance. Of course there will be tensions in that relationship. It may not be easy to achieve consensus about other eCrime issues as it has been on child abuse - but there needs to be a sensible context in which contentious issues can be examined and resolved.

That is essential if the UK is to deliver on the key recommendation of this report – that "an eCrime reduction partnership approach is the only realistic way forward" with the "firm and consistent support from Ministers" complemented by engagement in partnerships of law enforcement, business (including SMEs), academia, the voluntary sector, local government, civil society groups along with Parliament and the departments and agencies of central government.

For me personally, this report delivers on a long-standing aspiration for us to get to grips with the challenge of how to tackle Internet-related crime. It's helpful that it is published just as the Home Affairs Select Committee embarks on a study of eCrime. Instead of demanding that authorities "do something", this report gives Ministers, Parliamentarians and Industry leaders a chance to unite in positive action which can obtain the backing of wider society. I wish every success to the new co-Chairs of PICTFOR – Stephen Mosley MP and Chi Onwurah MP and their team - in giving Parliamentary leadership to this endeavour.

We have good reason to be very grateful to Nominet, the Nominet Trust and above all to Michael Levi and Matthew Williams for this report.

The best thanks will be to act on it.

Rt Hon Alun Michael MP

House of Commons, London SW1A 0AA - September 2012

EXECUTIVE SUMMARY

Data on eCrime

- High quality data on eCrimes are hard to find, both nationally and internationally. This makes rational policy decisions for both public and private sectors – which anyway are interdependent *in both directions* – even more difficult than they would otherwise be, as nation states grapple falteringly with transnational crimes and with transnational legal processes, priorities and scarce resources.

- The majority of eCrime data collection practices adopt sub-standard methodologies that produce a very partial picture of the problem. Large government surveys, such as the Crime Survey for England and Wales (formerly the British Crime Survey), the Offending, Crime and Justice Survey and Commercial Victimisation Survey only intermittently include questions that relate directly to eCrimes, though the CSEW and the Scottish Crime and Justice Survey have looked regularly at card and identity crimes, and fear of them, and have found that identity thefts arouse more concern than do other crimes. Identity thefts can occur offline, but it seems plausible that when responding, people will be thinking about online data 'theft' from hacking or social engineering. eCrime questions in European surveys, such as the Community Surveys on ICT Usage, have been found to be unreliable. Vendor sources, such as private security surveys, are often based on breach data identified by vendor software, resulting in partial datasets. Official criminal justice related datasets rely on both reported and officially recorded incidents of eCrimes, while even good administrative data in the private sector (e.g. UK Payments, CIFAS Fraud Prevention Service) cannot avoid excluding unidentified eFrauds (for example in the large category of 'bad debt'). In the UK only the Oxford Internet Surveys and the Information Security Breaches Survey (pre-2010) produce eCrimes data that are of gold-standard methodologically: however neither of them survey or estimate direct or indirect economic losses from eCrimes.

- The introduction of security breach notification requirements to some UK public and private sector organisations in May 2011[1] may provide a more robust evidence base on eCrimes breaches. It is however too early to assess the quality of this new data stream that is only recently under the coordination of the Office of Communications (Ofcom) and the Information Commissioner's Office (ICO).

- Based on the best data available, an upward trend is evident for both domestic and business related eCrimes. The Information Security Breaches Survey (2010) indicates a sharp upward trend in all business eCrimes compared to 2008 data. While less extreme, the upward trend in domestic data as recorded by the Oxford Internet Survey (2011) applies to all eCrimes other than obscenity.

- Independent of actual levels of fraud, there is high public anxiety about eCrimes, and such anxieties require 'reassurance policing' that contains both real responses to experienced crimes and a range of public and third party measures to guide sound as well as just profitable risk-reduction practices.

[1] See the Electronic Communications and Wireless Telegraphy Regulations 2011 and the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

UK Information Assurance Community Perceptions of the eCrime Problem

- UK Information Assurance (UKIA) organisational perceptions of the eCrime problem mirror current trends. The majority of organisations perceive malware to be the most significant problem, followed by customer ID theft, hacking and insider unauthorised access. State sponsored eCrime, DoS attacks and corporate and government insider-outsider collusion emerge as lesser concerns.

- Most UKIA organisations perceive the eCrime problem as getting worse. Roughly eighty percent feel that state sponsored eCrime will become more of a problem in the future, along with customer and corporate identity theft.

UKIA Community Perceptions of eCrime Data Sources

- The three most consulted eCrimes data sources are academic, private security national and international surveys. The least consulted (probably because most consultees were outside the financial services sector) are UK Payments, CIFAS and vertical market sources. Police recorded crime data are consulted by just over half of all UKIA organisations. However, Academic, CIFAS and UK Payment sources are the most *valued* sources. Private security national and international are least valued.

UKIA Community Perceptions of eCrime Control

- Organisations perceive most eCrimes as quite difficult to control. Corporate and government insider-outsider collusion are perceived as most difficult to control; while systems hacking, insider unauthorised access and malware attacks are seen as slightly less difficult to control.

- Private sector (finance) and government departments are just under twice as likely as the police to see personal identity theft and malware as more difficult to control.

Perceived Importance of Organisations in Tackling eCrime

- The majority of UKIA organisations are ranked as quite important in the fight against eCrimes. Central government (criminal justice related) departments, private sector (IT and financial) and the police are all ranked as most important. Charities/Not for Profit (NfP)s, local government and other public sector departments are ranked as least important.

- Police and government organisations are around one and a half times more likely to rate central government (criminal justice related) departments as important compared to the finance sector, which rates them the least important out of all responding organisations. Both the finance sector and the police are most likely to

rate private sector (IT) as most important, while charities/NfPs are least likely to rate it as most important.

Expected Responsibility of Organisations in Tackling eCrime

- The majority of UKIA organisations indicate that central government (criminal justice related) departments (such as the Home Office) should have the highest level of responsibility, followed by police, regulatory bodies and central government (non- criminal justice related). The private sector (finance and IT) also feature high in terms of expected responsibility. Charities/NfPs and local government are expected to have the least responsibility.

Perceived Effectiveness of Organisations in Tackling eCrime

- UKIA organisations perceive CERTs and the private sector (finance and IT) as the most effective controllers of eCrime, while charities/NfPs, public sector (other) and local government are perceived as least effective. Police and central government (criminal justice) place fifth and sixth respectively out of a total of seventeen listed organisations.

- Central government (criminal justice related) departments are seen as most effective by the police and least by the finance sector, whereas the police are seen as most effective by academics and least by charities/NfPs. However, the most significant difference in perception emerges with the finance sector: groups and regulatory bodies are most likely to perceive finance as effective while the police rate them as least effective out of the responding organisations.

Perceptions of Frequency of Cooperation with the UKIA Community

- The majority of organisations have some cooperation with the UKIA network. The overall average of cooperation (2.89 on a scale of 1 to 4) indicates that the majority of respondents have 'some cooperation' with other UKIA organisations. This overall mean is a barometer of cooperation, so an upward trend over time would indicate more cooperation amongst the UKIA community. This measure can be used to help evaluate the public/private information sharing 'hub', piloted in 2011 by Government, once rolled-out nationally.

- The finance sector rate themselves as the most cooperative, followed closely by academic/research institutions and the police. Those perceiving themselves as least cooperative include government (including local government), private sector (other), and group/regulatory organisations.

- Police, central government (criminal justice related) and private sector (IT) organisations emerge as the most cooperated with. Conversely, private sector (other), charity/NfP and local government organisations emerge as the least cooperated with.

Perceptions of Cooperation Quality

- The majority of respondents rate their quality of cooperation as just below 'quite good' (a mean of 3.64 on a scale of 1 to 5). This measure, in tandem with the frequency of cooperation measure, can be used to partly evaluate the effectiveness of public/private partnership initiatives stemming from the UK Cyber Security Strategy (Cabinet Office, 2011).

- Academic/research institutions, finance organisations and the police rate themselves as having the highest quality of cooperation. Government (including local government), charities/NfPs and private sector (other) organisations self-identify as having poorer quality cooperation within the UKIA community.

- Police and private security (IT) organisations are identified as delivering the highest quality of cooperation. Local government emerge as having the lowest quality of cooperation by quite some margin.

Wishes for Future Cooperation

- Just under eighty percent of organisations desire increased cooperation with central government (criminal justice related) departments, followed closely by non-criminal justice related departments, government-industry groups and the police. Public sector (other), private sector (other) and charities/NfPs emerge as the least desired. Near two thirds of organisations desire more cooperation with local government.

Desired Aids to eCrimes Reduction

- Just under half of UKIA organisations indicate that in order to further reduce eCrimes they need increased cooperation with the UKIA community, followed by an improved knowledge base/more training (forty percent) and increased cooperation with the international IA community (thirty-six percent). Less than ten percent of respondents want more UK legislation, and fewer than five percent desire more effective non-criminal justice reporting mechanisms. Roughly one third of organisations want more arrests and prosecutions and more effective criminal justice reporting mechanisms.

Barriers to Cooperation with the UKIA Community

- The majority of organisations identify a lack of lead from government as the most significant barrier to national cooperation. Confusion and overlap of responsibilities also feature high, along with a clash of aims and objectives with other UKIA organisations and a lack of reliable and valid eCrime data. Legislation (either too much or too little) and too much centralisation are not perceived as significant barriers to effective cooperation.

- Ineffective international legislation is identified by respondents as the most significant barrier to international cooperation. This is followed closely by a lack of reliable and valid eCrime data, ineffective European legislation and a lack of lead

from international Governments. Too much European legislation and too much centralisation are identified as least of the barriers in relation to international cooperation.

Perceptions of an eCrimes Reduction Partnership

- UKIA organisations are conscious of the need to involve the private sector in an eCrime reduction partnership, coinciding with the key message in the UK Cyber Security Strategy (Cabinet Office, 2011). Many note that partnerships must involve SMEs and engage at board level in the case of larger firms.

- Some UKIA organisations express that both roles and responsibilities within their networks of eCrime control need to be better defined and communicated, including the role of government. Like the UK Cyber Security Strategy, respondents in this study advocate tiered systems that incorporate government, but are not dependent on state-led co-ordination. Clear roles and responsibilities are proposed at the national and regional level for public, private, criminal justice and voluntary eCrime controllers.

- UKIA organisations highlight the importance of joined-up sharing of information, the utility of confidentiality agreements, and symmetry in data sharing—all of which are necessary for effective cooperation, and which through diffusion of benefits will assist in building a better picture of eCrime. The pilot scheme of the public/private information sharing 'hub' in 2011, and the planned national roll-out, will likely make significant advances on these fronts.

- A partnership must be supported by intelligence and analysis from all members, including inter-disciplinary academic contributions (social sciences, as well as computer sciences and informatics).

- Adequate funding targeted at priorities is essential to the success of a partnership. In particular, some respondents urge the need for funding to support not-for-profit and academic involvement. Such funds could also be used to support the inclusion of SMEs.

- Education, awareness raising and engagement with the public emerge as priorities for several UKIA organisations. A partnership must engage with civic bodies and local government.

- The UK Cyber Security Strategy advocates an international approach to cooperation in tackling the eCrime problem. UKIA organisations responding in this study recognised that the international dimension of eCrimes poses challenges for a UK based eCrime reduction partnership. It must address concerns beyond national boundaries and engage with partners in Europe and beyond.

- A partnership should be outcome orientated and should develop action plans whose impacts – on eCrimes and/or on the fear of eCrimes - are measurable.

Further dimensions of the Control of eCrimes

- The control of eCrimes is understood by all to be a complex matter, involving some responsibility on the part of commerce for the 'crime externalities' they create. Even if the number of public police dealing with eCrime were doubled, and if many volunteer expert 'Special Constables' were on hand (as proposed by the UK Cyber Security Strategy) for the day or so they normally work per week, this would have only a very modest impact on the risks that cybercriminals face. Action Fraud and the National Fraud Intelligence Bureau have made a good start, and the introduction of the security breach notifications legislation in the UK under the 2011 amendments to the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and the proposed European Commission Data Protection Directive regulations may signal a move towards more robust collection efforts. However there still remains a need for an active collections policy for eCrimes (including *attempted* eCrimes) against the public as well as against business, without raising unrealistically their expectations about the prospects of criminal justice action following from reports. Recording *mechanisms* of criminal exploitation is not what recorded crime or crime surveys normally do, so that represents a significant challenge.
- There is very little systematic information about what people want and expect from *any* of the preventative or criminal justice sectors (ISPs, police, government generally). Some ISPs work on very slender profit margins and the market is very price-sensitive, so placing eCrime prevention (e.g. Phishing site take-down) obligations on them might have a drastic impact on supply unless burdens were equally shared so that prices to consumers rose fairly. Nor is a 'polluter pays' principle easy to apply, since many fraud and hacking attempts lie outside profitable legitimate service mechanisms. The suspension of .uk domain names by Nominet represents one way forward, with a graduated approach based on the egregiousness and lack of ambiguity of the harm, and the urgency of the prevention[2].

- Free antivirus software supplied by some banks (and the free downloadable products) protect only against some forms of eCrime, and antivirus software (free or paid for) is largely irrelevant to serious corporate and governmental scams. Hard-to-reach 'at risk' groups contribute little to the overall financial cost of eCrimes, but reducing harms to them is an important social objective, alongside the costly eCrimes. eCrimes are a highly varied rather than a singular category of activities, and public policing is important not as a routine response – which is

[2] See, for example, http://www.theregister.co.uk/2011/11/18/dotuk_takedown_refresh/; http://www.chiefofficers.net/888333888/cms/index.php/news/industries/infotech_comms/industry/internet_another_bank_fraud_shows_why_nominet_is_right. (Accessed 14/12/2011). There are difficult issues relating to a possible right to compensation for economic damage to the 'right to property' in the case of suspensions not ordered by a court, which are too complex to deal with here.

unfeasible, even without the current environment of cuts in police resources - but as a mechanism for sending risk signals to selective offender groups and reassuring the public that someone is making an effort to look after them. Reassurance policing within both private and public sectors does require active engagement with a broad range of publics, and this inevitably is a long term iterative process.

RECOMMENDATIONS

1. Questions on eCrime should be included in government national surveys to garner reliable and valid evidence from corporate and domestic domains. These questions should include hard measures such as 'prevalence' as well as softer measures such as 'fears' and 'expectations'. Evidence from the European Commission i2010 High Level Group and Empirica (2007) should be taken into account during the cognitive testing of questions.

2. A cyber security strategy should be developed for the domestic domain, mirroring that of the more business focussed UK Cyber Security and Fighting Fraud Together strategies. The outreach work of public-facing cyber-risk reduction organisations, such as Get Safe Online, should inform and form part of this strategy.

3. As detailed in our review of eCrime costs, estimates and models are either overly simplistic (i.e. based on average losses) or contain mechanics that are opaque and often unverifiable. Further inter-disciplinary academic work is needed to develop transparent and replicable probabilistic financial models of eCrime costs.

4. The UK Information Assurance Community should be subject to an audit of roles and responsibilities to identify gaps and areas of overlap. In particular this audit should isolate the various aspects of 'assurance' and identify how advice and support provided to business and the public is consumed and acted upon.

5. An eCrime Reduction Partnership approach is the only realistic way forward, but needs firm and consistent support from Ministers in order to succeed. Where partnerships are expected to be "industry led" they need to include law enforcement, business (including SMEs), academia, the voluntary sector, local government, civil society groups, parliament and also central government departments and agencies both as points of vulnerability and as victims, not just as policy makers and regulators. The partnership approach should be informed by the requirements outlined in this report. This partnership should establish a dynamic relationship with eCrime public/private information sharing hubs, such as those being created as part of the UK Cyber Security Strategy.

ACKNOWLEDGEMENTS

We are grateful for the assistance and advice provided by a number of individuals – some of whom prefer not be named - and organisations during the conduct of the research: these include foremost the Rt Hon Alun Michael MP – who first stimulated us to look at the possibilities of enhancing public-private eCrime reduction - and who encouraged us to persist. We are also particularly grateful to (in alphabetical order) Richard Horne, Bill Hughes, Stuart Hyde, Daniel Mount, Tony Neate, Philip Virgo, Professor David Wall. Lesley Cowley and Martin Boyle from Nominet, and a seminar organised by the Oxford Internet Institute, gave us the impetus to begin the study. In institutional terms we would like to thank EURIM, Nominet, PCeU, PICTFOR, SOCA, and the UK Internet Governance Forum for their help in the research. We greatly appreciate the time taken by members of the UKIA community in completing the online survey and taking part in interviews. Finally we are grateful to Nominet Trust for funding the research.

INTRODUCTION

This research was commissioned primarily to investigate the potential for the formation of an eCrimes Reduction Partnership within the UK and to assess the current evidence on the cost of e-fraud and on the inter-relationships between public and private sector bodies that have a role in combating eCrimes. This report provides valuable primary data on how UK Information Assurance (UKIA) organisations currently perceive cooperative working and on how they view future attempts to establish public/private partnerships. While the report was commissioned and the research largely completed before the publication of the UK Cyber Security Strategy (Cabinet Office, 2011), the findings are highly relevant to many of the strategy's key deliverables. Although eCrime has enjoyed an ascending role in the National Security Strategy of the UK (HM Government, 2010) and of other countries such as Australia, the Netherlands and the USA – becoming a Tier One threat, above organised crime and fraud generally – it is an extremely broad category ranging from opportunist thefts (or, as we prefer to call them, 'duplications'[3]) of personal data to systematic mass attacks on banks, major corporate Intellectual Property (IP) 'duplication' and state-sponsored or at least state-tolerated cyberwarfare, at the other extreme. However, as with 'organised crime' and other national threats, substantial variations exist in the actual and perceived costs and fear of crime, and there is no simple translation of these strategic judgments into locally felt concerns. These present difficulties for public engagement in interventions, for public scepticisms may have to be overcome or lived with in the course of control strategies. Though we may stray occasionally from this principle, we have chosen to use the term 'eCrimes' rather than the more common singular 'eCrime' or 'cybercrime' to stress the fact that these are different sorts of activities and that they are mainly pre-existing crimes with an online component in how they are attained. Furthermore, we acknowledge the 'schism' that has begun to emerge between the terms and meanings of *e*Crime and *Cyber*crime in policy and academic discourse. We find this problematic and detrimental to a common understanding of the topic, since we risk using the same terms to deal with very different phenomena without always realising this.

Our aim in this review is to critically examine existing data and to throw some light on the current state of public-private and private-public inter-relationships in the struggle against eCrimes outside the 'national security' space. Although there is a continuum in the national security-eCrimes arena, it seems to us that most crimes against business and against individuals fall outside the sensitive highly classified Critical Infrastructure area. To include the latter would also take us too far from the eCrime Partnership concerns that drove this project. For this reason, and because cyberwarfare is already well served by sophisticated

[3] Analytically, the common term 'identity theft' is normally mistaken. In offline theft, when one person takes property, the other loses it. In identity cases, however, the loser is left with their (usually impaired) identity, while the 'thief' and person(s) to whom the data and/or documents are re-sold makes whatever gain their skills and networks are enabled to generate. Therefore 'borrowed', 'duplicated' or 'misappropriated' are more illuminating terms than 'stolen'. We hold out no great hope that usage will change as a result of these comments, but we hope this will make people think more clearly about it.

analysts (Cornish et al., 2009, 2011; Cabinet Office, 2011), we are largely omitting this sphere, though (whether the public see this or not) there is a trickle down of harm from corporate IP espionage (computer-enabled or not) to the economic welfare of citizens. It is also important to focus on the public-facing component of eCrimes because some components arouse a great deal of public anxiety, however hard it may be to disentangle 'natural' concerns from those generated by media stories about 'identity theft' that serve as 'signal crimes' manifesting deeper social anxieties about technological risks outside our control that lead 'aliens' to take over our lives. Such ordinary citizen concerns are at risk of being unintentionally (by default) submerged in the important task of handling the major economic and ideological clashes between nations and corporate entities that have characterized many cyberwarfare discussions and International Conferences. In this sense, our work focuses more on low politics than on high politics, and we seek to reclaim the 'low ground' and 'middle ground' of eCrimes from the High Strategists. The Cyber Security Strategy (Cabinet Office, 2011) of the UK government – like its parallel exercises in Australia and the US – offers comparatively little to those citizen-facing layers of 'the eCrime problem' and arguably mirror strategies should be developed for the domestic domain.

The growth of eCrimes has generated a significant methodological and substantive literature and some very helpful meta-reviews (Anderson et al., 2008; Kanich et al., 2011; Sommer and Brown, 2011). The most recent (as we write) corporate and public sector organisation survey (PwC, 2011a) defines cybercrime as *'an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. It's only a cybercrime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one."*[4] It usefully adds that "it seems many people interpret it in different ways. For example, a sales executive who steals confidential sales and marketing data by copying it onto a USB stick or emails it to himself before joining a competitor might have committed a number of crimes. It could be intellectual property theft or a cybercrime or both."

Measuring the *cost* of eCrimes is a delicate and ultimately partly subjective issue, involving the weighting of emotional as well as objective economic impacts. It should be better recognised, however, that even these objective financial impacts contain elements of disputable interpretation, for example over whether competitor product developments are the result of hacking rather than of insider corruption or of mere coincidence in parallel development. The primary focus of studies to date has been on levels and forms of intrusion, rather than on costs. To the extent that costs are measured at all, the focus is typically costs to business, and though the one-off Office of Fair Trading (2006) scams survey did conduct a gold standard review of consumer fraud, it is hard to separate the online from offline data on fraud attempts and successes, and in eCrime terms, 2005 is a long time ago. Because of the large gaps in our reliable knowledge, therefore, this exercise

[4] The questionnaire used by PricewaterhouseCoopers (PwC) stated: "This excludes routine fraud whereby a computer has been used as a by-product in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one."

aims to lay out some issues for the future rather than presenting an inevitably speculative set of figures for the cost of eCrimes in the UK.

The collateral emotional damage to individuals from identity frauds and on compromised personal data (irrespective of its use in fraud) is socially and politically important, yet is difficult to place an economic value upon. One conceptual approach is to use the 'willingness to pay' model in which one judges damage by how much people are willing to pay to avoid the risk. Thus one could tot up consumer payments to identity theft insurance services as a measure of anticipated consequences times anticipated probability. However not only does this conceal assumptions – which could be misinformed - about how common and how serious the act would be, but it also ignores relative affordability from disposable income. Irrespective of actual victimisation[5], fear of becoming an eCrime victim is a social cost and, to the extent that it leads to sub-optimal economic behaviour like avoiding e-commerce and online banking, also leads to loss of economic welfare both to consumers and producers/ distributors.

One issue confronting an eCrimes mapping exercise is working out what it is that we want to map. If we want to measure changing techniques, to some extent these are measured in some existing cybercrime surveys by AKJ/KPMG, BitDefender, CyberSource, Garlik, Symantec, 192.com and the longer term surveys like the CSI that are annual but not panel surveys, i.e. we cannot track cybercrime victimisation levels for the same firms over time, and response rates are highly variable or unknown. This is also a problem for the more general economic crime surveys such as that of PwC (2011a, b) which, however carefully conducted and useful in mapping the terrain, may lead us to make false inferences about changing trends in economic crime when in fact, the actual companies and their sectoral mix may be quite different from those responding in previous years[6]. Thus we accept that a quarter *of those companies that experienced an economic crime* reported to the survey that this crime was a cybercrime. However we are not altogether persuaded that cybercrimes have *newly* become the fourth most frequent type of economic crime, and we note that this placement is by *volume* of crimes reported in the previous year: it tells us nothing about the *value* of such crimes. Given the general frequency of cybercrimes (and perhaps their low average impact, though this is not reviewed in the survey), we do not find it surprising that overall, 24 per cent of UK institutional respondents reported more than 10 economic crime incidents in the previous 12 months[7]. Even to individuals, cyber-'attacks' may be expected to be routine.

If, however, we want to measure the *harm* caused by eCrimes in the UK, we need

[5] 'Victimisation' is used in this report in the criminological sense of relating to victims, rather than in the common speech sense of hostility towards others.

[6] The UK dataset was an online survey in which there were 178 respondents 'drawn from listed (37%), private (39%) and public sector (20%) organisations'.

[7] The above survey does, however, offer some fine-grained analysis of the problems of classifying frauds as eCrimes, and notes that its focus on cybercrimes, alongside other factors such as enhanced attention to identifying such offences, may have led respondents to classify as cybercrimes acts they would previously have classified in other ways. It also contains a wealth of other interesting data.

1. to agree the terms in which 'harm' is expressed. This could include feelings, including lost hopes and violation of privacy; Avoidance behaviours, including reluctance to use online facilities, increasing the digital divide; Measurable financial losses, in absolute cost terms or as a proportion of profits, savings; Direct losses alone, or also response costs in enhancing security, pursuing suspects, and compensating others in the case of third party trust?

2. to measure frequency of offences, against individuals and organisations of different types, domestic and foreign but operating in the UK; and

3. to agree the terms in which the *organisation* of offending should be defined. These might include state-sponsored groups, organised hierarchical gangs, looser collaborative networks, individual 'rogue traders', part-time versus full-time offenders (as income sources), etc. This might assist a judgment about the capacity and intentions of threats to the UK, though we might also wish to take into account the possibility of transformations in capacity due to shifts in social networks and criminal entrepreneurship[8].

Currently, there is a concatenation of offences against individuals, businesses of various types, and public bodies, and too little differentiation between data compromise (i.e. risk of identity 'theft') and the use of that data for criminal purposes (whether for false identity documents to be used for illegal immigration, false driving licences, the evasion of congestion charges, deportation orders or arrest warrants, or for activities more commonly termed 'fraud'). Ideally, we might want to know what proportion of data compromises are transformed into actual further criminal attempts, how is this changing, and why? There is also the danger of our control efforts being driven by areas where data are better, such as card-not-present fraud and phishing attempts, neglecting areas where data are poor or are highly speculative (such as IP violations). (Though the defensible counter argument is that we need to act in areas where data are poor but potential harm is high or catastrophic.)

As for offenders, even if we were sensibly to distinguish financial from ideological/ nationalist motivations for the purposes of assessing the threat from different e-criminals, it might still be difficult (and contentious) to divide financial from ideological and play motivations (cf. the decade-long controversy over the intentions – and the appropriate trial venue - of alleged 2002 Pentagon hacker Gary McKinnon). Furthermore, these motivations might change over 'cybercrime careers' (which may not be at all like other full-time criminal careers). Our understanding of desistance from eCrime is poor, and common judgements such as that the nature of cybercrime has changed from relatively innocent play in the 1990s to primarily financial motivation today are plausible but rest on a weak empirical foundation. All of these 'criminal career' evolution issues impact upon cost, incidence and prevalence, but they lie beyond the scope of this study.

[8] See Kleemans and de Poot (2008), van Koppen et al. (2010), and the study of the DarkMarket illicit payment card exchange by Glenny (2011). An very preliminary attempt at exploring the links between cybercrime and organised crime can be found in BAE Systems Detica and the John Grieve Centre for Policing and Community Safety (2012).

The costs of eCrimes may be broken down as follows:

- *eCrime losses (transfer costs):* **Victims face direct losses as a result of eCrimes (e.g. the amounts defrauded). These losses are sometimes considered transfers (from the victim to the fraudster), and in the economic literature, transfers are typically excluded in analyses of the costs of crime.** However we consider such losses to be part of the costs of eCrime, as these are unwanted losses (i.e. the victim has not agreed to the transfer), and as such the transfer represents one from the legal to the illegal economy. One usually uncosted (and difficult to cost) component is indirect or collateral damage, such as feelings of anxiety and other welfare losses, even if no identified use is made of the 'stolen' data[9].
- *Costs of preventing eCrimes before the event (and other anticipatory costs):* Private and public sector entities take certain defensive measures to prevent and/or deter eCrimes, all with costs. These costs range from personal expenditures on shredders (to prevent personal data 'thefts' that may lead to future frauds or other crimes with an electronic component) to corporate membership of (a) service organisations such as UK Payments and Financial Fraud Action UK, one of whose many functions is fraud prevention, and (b) dedicated fraud prevention bodies such as CIFAS Fraud Prevention Service (indeed, the running costs of CIFAS itself) and 'identity fraud monitors' run by credit reference agencies such as Experian and Equifax, or 'fraud insurance', some of which is rolled up by inclusion into premium bank account costs. Costs also result from precautionary behaviour: consumers may avoid using certain services or avoid visiting suspected high-risk websites to avoid being victims of eCrime. It is as well not to overstate this. The estimated total value of Internet card spending (excluding PayPal, wire transfers and other payment mechanisms) on UK-issued cards has risen by almost 150% over the last five years to £53.6 billion in 2010 - an increase of 14% on 2009. Over 26.9 million adults banked online in 2010, and 61% of adults have regular access to an internet bank (Financial Fraud Action UK, 2011). Nevertheless, some customers might avoid online banking services for fear of being defrauded (which would represent a loss to them and to the banks, since the marginal cost of providing online banking is lower than that of its alternatives).
- *Costs of responding to eCrimes after the event:* The costs in response to eCrimes include costs to the criminal justice system (including police, prosecutors, courts, prison service)[10] and of civil remedies in response to eCrimes such as fraud or those IP violations that result from cyber attacks. Larger and more complex eCrimes against firms and government will typically incur expenditures (e.g. through internal and/or out-sourced private sector investigations) even if they are not ultimately reported to the police. In the event, very few sources provided information relating to the costs of

[9] We repeat here that there is an unknown but probably 'high' ratio of compromised to criminally utilised data, e.g. in the aftermath of government or corporate losses of data disks or hacked data. Although these may be well publicised and the publicity may cause widespread anxiety, criminal take up appears to be quite low of, e.g., HMRC's notorious lost child benefit data disks in 2007.

[10] Unless the offenders have *recoverable* surplus assets from which costs can be paid, private sector investigative and legal costs will be deducted from compensation for victims; public sector costs are borne by contributors to council and central government taxes.

eCrime prevention and/or in response to eCrime, nor do many appear to keep data in this form.

Anderson et al. (2012) – to which study the first author contributed – generated a much lower than normal figure for cybercrime, because they refused to speculate about areas where data were poor. In this sense, like Levi et al. (2007) and Levi and Burrows (2008) on fraud generally, their data should be viewed as a minimum established figure. As far as direct costs are concerned, traditional offences such as tax and welfare fraud cost the typical citizen in the low hundreds of pounds a year; transitional frauds cost a few pounds; while the new computer crimes cost in the tens of pence. In some cases, low production and distribution costs to criminals mean that direct social losses are roughly similar to criminal profits. For instance, UK consumers provided roughly $400,000 to the top counterfeit pharmaceutical programs in 2010 and perhaps as much as $1.2M per-month overall. UK-originated criminal revenue is no more than $14m a year, and global revenue, $288m. The five top software counterfeiting organisations have an annual turnover of around $22m worldwide. However, the indirect costs and defence costs are much higher for transitional and new crimes. For the former they may be roughly comparable to what the criminals earn, while for the latter they may be an order of magnitude higher. As a striking example, the botnet behind a third of the spam sent in 2010 earned its owners around US$2.7m, while worldwide expenditures on spam prevention probably exceeded a billion dollars.

In our opinion, the costs of responding to eCrimes should be kept separate from the costs of eCrimes themselves: an unintended consequence of the conventional Home Office practice of rolling them together as 'costs of crime' is that this risks allocating further resources to areas where resources are already high ('because they are more costly') or alternatively, not resourcing those areas where little is currently spent. The costs of eCrime might be disaggregated as losses, resource costs, and externalities. Resource costs may relate to expenditures both in anticipation of and in response to eCrimes (e.g. on fraud prevention systems, on reactive investigative teams), though these distinctions were difficult. Externalities refer to side effects from an activity which have consequences for another activity but are not reflected in market prices. Externalities can be either positive, when an external benefit is generated, or negative, when an external cost is generated. A negative externality of fraud may be the above-noted reduction in the use of online banking services. Another might be where a corporate and/or national reputation for eCrime leads to other firms or countries avoiding doing business with firms in the suspected area, for example outsourcing or other activities that might generate intellectual property theft as well as efrauds. Reputational harm was a serious issue to firms in the PwC (2011 a, b) survey. If we are considering harm to the UK as a vendor of goods, this should not be a serious problem, since the UK is not a major source of viruses or phishing attacks (BitDefender, 2011). However, such national reputational damage is a major problem for some countries. It should also be noted that costs may be estimated by 'bottom-up' and/or 'top-down' methods. *A 'bottom up' approach* seeks to evaluate the costs of fraud from the perspective of the producer or defrauded organisation. An example of the *bottom-up method* might be the use of administrative data on payment card fraud reported to UK Payments (in which

the annual volume/value terms simply represent the sum of all reported frauds). *A 'top down' approach* estimates the economic implications of eCrime from a national perspective.

Additionally, the issue of 'who bears the cost' is often a complex one. It is also one reason why the likelihood of double counting is a major concern in the fraud field. An individual who has been victim of an identity theft may relay this fact in the course of a survey, but so too (though not in a survey of individuals) will any body that provided all, or part of, compensation to that individual for associated losses, as would be normal in the case of credit card frauds unless misconduct by the cardholder can be demonstrated[11]. (Likewise with corporate victims of eCrime, who may be insured.) On the other hand, if we simply take our cost of eCrime data from Financial Fraud Action UK, and/or from insurers, this neglects the 'hassle costs and time' for individuals and businesses of dealing with eCrimes[12], whether disputed or not by counter-parties. This presents a significant challenge to aggregating the costs of eCrime to the UK economy.

Further, determining the true costs of goods and services obtained by fraud can present difficulties. There is little consensus, for example, on whether goods obtained by fraud should be counted at their wholesale price or retail price (with or without VAT). Published data on the opportunity costs of eCrimes – e.g. the trauma of identity theft - to businesses, individuals, and 'the public as taxpayers' are largely anecdotal, yet one might expect some such costs to be substantial, and certainly comparable to other crimes. Moreover, certain types of eCrime – for example impersonations that facilitate terrorism or electoral impersonation/intimidation of postal voting - may produce immense collateral damage, but their estimation will be exceedingly difficult without rafts of assumptions whose validity or even plausibility may be hard to test.[13] This pilot study is not funded to seek to generate such data, but we should not neglect the fact that eCrime may bring such costs to bear on the UK economy.

Finally, though we make no attempt here to translate these into economic costs, public anxieties about eCrimes are a social cost (with some economic consequences). The Scottish Crime and Justice Survey (2011) asked the public how much they worried about a range of

[11] There is no hard information about compensation for those victimised after corporate data protection breaches. However we presume that these are mostly compensated by the company, who may be insured against such losses, passing costs on further down the line. The US mandates such compensation.

[12] In 2010, the US National Victimization survey showed that about 8.6 million households in the United States (up from 5.5% in 2005 to 7% in 2010) had experienced one or more types of identity theft victimization (Langton, 2011). About 23 percent of all victims suffered an out-of-pocket financial loss due to the victimization. Of the victims who experienced a personal loss, the average out-of-pocket financial loss was $1,870, with half losing $200 or less (Langton and Planty, 2011). An ITFRC (2010) study showed that ID theft victims spent about $527 out of pocket for an existing account compromised by an attacker, down from $741 in 2008. They also spent less time repairing the damage from a compromised account -- an average of 68 hours versus 76 hours in 2008 and 300 hours in 2004. However interesting, the data derive from 183 victims who contacted the ITRC in 2009: they in no sense constitute a representative sample of id theft victims, nor – because of the nature of the samples - are these periodic comparisons meaningful.

[13] And if the frauds are substituted by other types of fund-raising (from legal or illegal sources), the terrorist act may not be prevented.

crimes happening to them, and how likely it was that those crimes might happen to them in the next year. Adults were *most worried* about someone using their credit / bank details to obtain money, goods or services (58%) and having their identity stolen (48%): perceptions have remained quite stable in recent years. Furthermore, fraudulent use of credit or bank details (15%), damage to vehicles (11%) and identity theft (10%) were the crimes that adults most commonly thought *were likely to happen to them* in the next 12 months. The SCJS 2010/11 estimated that 4.5% of adults had experienced card fraud in the 12 months prior to interview; and 0.5% of adults had been a victim of identity theft, where someone had pretended to be them or used their personal details fraudulently. Comparing results of the actual risk with the perceived risk, 20 times as many adults thought they were likely to become a victim of identity fraud than were likely to experience this (10% thought this likely to happen compared with the actual risk of 0.5%). The BCS (Chaplin et al., 2011: 81-82) found that 5.2 per cent of plastic card users were victims of plastic card fraud 2010/11, lower than the 6.4 per cent reported in 2009/10. However this was significantly higher than the 1.1 per cent who had been victims of theft in 2010/11. Unlike the Scottish Crime and Justice Survey, the BCS (now renamed more accurately the Crime Survey for England Wales) does not ask respondents about worry about identity and card fraud, but it is implausible that this will be radically different from the Scottish data.

METHODOLOGY

Rapid Evidence Assessment

As part of the research design we conducted a Rapid Evidence Assessment (REA) of existing eCrime data sources that related to the UK. Standard meta-synthesis procedures were utilised in the search and selection of relevant research studies. As part of a REA Study Quality Standards (SQS) are established to set a bar on the quality of studies which are included. For this review we adopted the following standards: i) research samples that were representative of the population under study; ii) research populations that were national or trans-national; iii) adequate government, organisational or academic sponsorship; and iv) appropriate relevance to eCrime, e-security and related subject matter. Studies that fall below these standards are excluded from the review, but some are mentioned for information.

An REA draws on published sources of information, systematically and critically appraising identified studies against specified criteria, all in a relatively compressed timescale. As part of an REA, a set of criteria against which to evaluate sources (to separate the 'wheat from the chaff') is established, conventionally called a Quality Assessment Tool (QAT); indeed this is a central task of all systematic analyses/ REAs/meta-analyses (sources are evaluated with particular regard for the quality of the data contained therein). The use of such criteria is intended to prevent the inclusion of research results which may be derived from questionable methods and/or which may ultimately lead to presenting data which conceals the fact that sources have been comparing apples and oranges.

Very early on in the present research, however, it became clear that subjecting the literature on eCrime to a conventional QAT 'screening' would not be feasible, because of the nature of the task being undertaken and the characteristics of the available literature. The difficulties faced are summarised below.

The research was most interested in *eCrime statistics*, while REAs typically examine evaluations of policy interventions—and therefore criteria of what makes a good study differ.[14]

The present study looked to publicly available information on eCrime in the UK (from sources throughout the public and private sectors and the academic journals). The studies reviewed broadly fell into three categories:

1. reports derived from networks of organisations (often sharing a common membership of an umbrella body) aggregating key administrative data to monitor trends and patterns;

2. surveys that aimed to generate a more general portrait of eCrime or particular forms of cyber/fraudulent conduct, although almost all with far more modest investment and

[14] In other words, while most previous REAs grade research used in their meta-analyses on the evaluation methodology employed (where randomised experimental approaches using some variant of the Maryland scale are largely seen as the gold standard), the present research was concerned with statistical data quality (data quality refers to "fitness for purpose").

attention to methodological issues than in any general crime surveys since the 1970s; and

3. those that scientifically sample eCrimes within agencies or departments and then extrapolate from them.

In addition, there are some more broad-based attempts to estimate opportunity costs and other features of the cost of eCrimes (Detica and Cabinet Office, 2011). But very few of these studies are derived from academic or professional analytical sources (whereas Rapid Evidence Assessments of policy evaluations typically review studies conducted by research professionals). Academic sources will broadly follow accepted article/report formats—which include section(s) on methods. But in the case of many eCrime (and non-eCrime fraud) studies, details of the methodology used are typically lacking. In particular, it is inescapable that while many eCrime studies relating to the private sector may appear to constitute 'research', the fundamental reason the work is conducted is to raise awareness of a threat often overlooked by the business or individual Internet user community, and/or to market the ability of the research sponsor to offer consultancy and/or related support services to tackle the problem. The net result is that much is based on loose methods (at best), or represents sound social science but with limited value for aggregation in any meta-analysis.

Added to this, given that the pool of relevant sources was not a deep one, a major concern was that 'setting the bar too high' would have left the study with little to review and discuss. While applying a formal Quality Assessment Tool (QAT) was not practical, the research did screen the available data, and placed a particular premium on including data that was reasonably current and that applied to the UK only. This is particularly difficult for crimes which – unlike most offline crimes – may be targeted at the world at large: even in telemarketing cases using 'sucker lists', the people listed may reside in different countries.

The first key dimension was the data collection methodology typically employed in each field. The range of information sources is outlined above, but it was seen to be particularly important to separate data derived from administrative record-keeping from that obtained by sample survey methods:

- Data from *administrative record-keeping* include, for example, data on (or summarising) reports of confirmed/suspected fraud discovered/investigated by companies in the financial services sector. These data are often aggregated and provided by membership organisations (e.g. CIFAS/UK Payments) to allow for the aggregate analysis and presentation of fraud trends.

- Data from *sample surveys*, on the other hand, will have been captured through the questioning (e.g. through self-response or interviews) of a sample of the overall population of interest (where a sample frame serves as a proxy for the population of interest). Sample surveys fall into a further two categories: probability sample and non-probability sample surveys. Probability sample surveys employ some probabilistic method to select at random entities from the sample frame for participation in the

survey.[15] Non-probability sample surveys employ methods other than probabilistic selection (most commonly thresholds) to determine which entities provide information.[16] Unless otherwise noted, the term "survey" in this report refers to a probability sample survey.

A second key dimension was to consider the purpose for which the data had been assembled and the implications thereof.[17] Different users may seek quite different goals in assembling fraud data. Data may be collected:

- To inform general *policy-making*, perhaps by indicating the volume and cost of eCrime to the UK in general terms;
- To generate *strategic intelligence*[18] on eCrime—indicating broad trends or typologies of eCrime, which can assist law enforcement organisations and/or the organizations which have been hacked and/or defrauded to design a suitable overall response;
- To generate *tactical—or operational—intelligence*[19] products which may then be used to identify and apprehend specific individuals and/or groups of eCriminals;
- To provide an alternative and more inclusive (i.e. of victims who do not report) picture of the eCrime problem compared with the official police crime data.

In reviewing the different sources, the present study sought to separate these (and other) different purposes. Clearly the timeliness of information available is critical here: data derived from a survey affecting particular types of victim may assist general policy making and possibly serve to provide strategic intelligence, but it cannot be expected to provide any operational utility in 'nailing' a particular offender.

[15] A census can be thought of as a probability sample survey in which all units within the sample frame are selected to participate with a probability of one (i.e. all units within the sample frame are asked to participate).

[16] Non-probability sample surveys also include surveys such as web-surveys which record findings of whoever responds – a particularly common method in eCrime surveys, though this is mitigated in some commercial surveys by sending out to a range of pre-selected bodies. A consequent weakness of such non-threshold or even threshold approaches (i.e. of all non-probability samples) is that it is difficult to generalise from non-probability samples to the larger population of interest.

[17] A crucial dimension of 'data quality' refers to 'fitness for use' or 'fitness for purpose', an inherently fuzzy concept (Office of National Statistics, 2005a, hereinafter ONS, 2005). This immediately begs the critical question of *what is the purpose of capturing statistics on eCrimes?*

[18] Strategic intelligence has been defined as "an assessment of targeted crime patterns, crime trends, criminal organisations, and/or unlawful property transactions for purposes of planning, decision-making and resource allocation" (Criminal Intelligence Training Coordination Strategy Working Group, 2004).

[19] Tactical, or operational, intelligence has been defined as "evaluated information on which immediate enforcement action can be based; intelligence activity focussed specifically on developing an active case" (see CITCSWG, 2004 in note above).

Primary Research

As well as providing a review of existing eCrimes data sources, we conducted primary data collection selecting the UKIA community as our population of interest. As the primary aim of this mapping study was to assess the possibility of an eCrimes Reduction Partnership it was important to survey the views of those most likely to form such a partnership. However, given the impracticalities of doing so, we were unable to canvas the views of representatives of Civil Society and Parliament, both of which should have a role in a reduction partnership initiative to enable good governance and accountability. We adopted two forms of primary data collection: i) an online survey which collected quantitative and qualitative data and, ii) a series of qualitative in-depth interviews with key members of the UKIA community.

The UKIA community sample for the survey was drawn from the Information Assurance Collaboration Group[20] *UK Information Assurance Community Map v2* (2010)[21]. All listed organisations were contacted where possible amounting to a target population of 200 UKIA organisations. Based on this number we achieved a 52 percent response rate (104 organisations) with good coverage within all sectors (public, private, criminal justice, voluntary, regulatory bodies and groups)[22].

[20] The Information Assurance Collaboration Group (IACG) works with Her Majesty's Government, and particularly with Cabinet Office and the Communications-Electronics Security Group (CESG) within the Government Communications Headquarters (GCHQ) , in order to deliver collaboration between industry and the business of government and so extend and simplify the deployment of pragmatic, appropriate and cost effective Information Assurance across the UK public sector.

[21] The boundaries of the UKIA community are not easily defined. A tightly bounded definition while including most public organisations with a UKIA remit is likely to exclude many academic, voluntary, private organisations and Civil Society. Therefore a loose definition was chosen that included any organisation with a perceived role in eCrime control.

[22] Usual response rates in social science research range between 20-40 percent.

REVIEW OF eCRIMES DATA SOURCES

A key problem to better understanding and controlling eCrimes is the lack of reliable data on their prevalence and impact on businesses, the national infrastructure and the general public. Several papers provide insightful reasons why existing data are flawed (see for example Anderson *et. al.* 2008, 2012; Casper 2007; and Sommer and Brown 2008). The data issues identified include i) Information asymmetries; ii) Lack of data sharing protocols; iii) Confidentiality and anonymity of respondents; iv) Failure to adopt gold standard data collection practices; and v) Knowledge and perception of victimisation.

We will begin by considering the surveys on the prevalence and incidence of attacks and then consider the smaller amount of studies on the cost of eCrimes. The most voluminous sources of data on eCrimes are vendor databases of malicious code activity (e.g. Symantec's Threat Assessment Report[23]). However, these data understandably focus on breaches such as botnet activity and subsequent spam levels that are technologically measurable by vendor specific software, (i.e. in the process of data generation, persons are not asked if they experienced a breach). This approach, while valuable in identifying overall trends, does not represent all the populations of interest (e.g. public sector organisations, business community and domestic users). Essentially they cannot provide the detail required on prevalence of breaches within each sector or region (where the unit of analysis is an organisation or individual), the perceived or actual impact of breaches, and the reaction of business or individuals to attack. Numbers of attacks identified by anti-virus vendors may once have been meaningful, but the growth of server-side polymorphism has led to constant transformations which mean they are no longer a sensible count of malware. Furthermore, the origin of such statistics raises important questions of perceived impartiality. For this reason alone these data must be excluded from any scientific investigation into the prevalence and impact of eCrimes.

It is possible that the introduction of the security breach notifications legislation in the UK under the 2011 amendments to the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and the proposed European Commission Data Protection Directive regulations may signal a move towards more robust collection efforts and better security breach data. However these initiatives are in their infancy, precluding an evaluation of data robustness and coverage. Furthermore, early reports on the proposed changes to the European Commission Data Protection Directive regulations indicate that organisations will find it difficult to meet the stringent security breach reporting requirements[24].

[23] Symantec gathers malicious code intelligence from more than 133 million client, server, and gateway systems that have deployed its antivirus products. Additionally, Symantec's distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks that provide valuable insight into attacker methods.

[24] See LogRhythm (2012): http://logrhythm.com/Company/PressReleases/87ofUKBusinessUnabletoIdentifyDataBreach.aspx

Table 1. eCrimes Data Sources: National Surveys

Survey	*Sampling strategy*	*Scope*	*Sponsorship*	*Cycle*
Information Security Breaches Survey	Random probability[1]	UK national - businesses	Government/BIS/ PwC & Infosecurity Europe[1]	Biennial (since 98)
National Hi-Tech Crime Unit Survey	Non-random	UK national - businesses	Government/ Police	Annual (02-05)
British Chambers of Commerce Survey[2]	Non-random	UK national - businesses	BCC	2001, 2004 & 2008
Audit Commission Survey	Non-random	UK national (mainly public sector)	Government	Triennial (81-04)
British Crime Survey/Crime Survey for England and Wales[4]	Random probability	UK national - domestic	Government/HO	Annual (Since 01) Biennial (82-00)
Offending Crime and Justice Survey	Random probability	UK national - domestic (perpetrators)	Government/HO	Annual (03-06)
Commercial Victimisation Survey[5]	Random probability	UK national - businesses	Government/HO	1994 & 2002
Community Surveys on ICT Usage[6]	Various[3]	European member states (domestic and business)	Eurostat	Annual (since 03)
International Crime Victimisation Survey/European Crime and Safety Survey[7]	Random probability	International - domestic	European Commission	Quadrennial (89-04/5)
The Oxford Internet Survey[8]	Random Probability	UK national - domestic	Economic and Social Research Council	Biennial (since 03)

[1] In 2010 a self-selecting sample was employed and for the first time the survey was not sponsored by the Government.
[2] Using IT: Small Firms and Technology (2001); Setting Businesses Free from Crime (2004); The Invisible Crime: A Business Crime Survey (2008)
[3] Sampling methodology varies by member states. For the majority some type of random sampling is employed.
[4] The BCS/CSEW includes a module on identity fraud (since 05/06). A technology crimes module was included in 03/04 but has not since been repeated.
[5] Questions regarding electronic crime were included in 2002. Consultation is on-going regarding a third wave of the survey.
[6] The i2010 High Level Group concedes in their Benchmarking Framework: "For businesses, the indicators on the percentage of enterprises having encountered security problems and the percentage of enterprises that have updated security devices have proved not to be reliable. Only the indicator on enterprises taking ICT security precautions proved to be feasible."
[7] Domestic respondents were only asked about electronic fraud.
[8] Domestic respondents were only asked about virus infection, fraud, and obscenity.

Table 1 provides details of existing and defunct surveys of eCrime victimisation (excluding vendor statistics) relevant to the UK[25]. (For a more exhaustive list of sources including vendor statistics, see Casper 2007). Each of these surveys identifies the organisation or individual as the unit of analysis. That is to say an employee (usually the person with responsibility for IT security) is asked about security issues and attacks in relation to their organisation, or a member of the general population is asked similar questions in relation to the home. These surveys capture instances of 'known' victimisation where the respondent directly experiences an eCrime attack or has been made aware of the attack by software (e.g. virus checker) or by another person (such as a payment card firm who telephones the victim about a transaction suspected by the firm). In contrast to vendor data, these surveys not only identify prevalence of 'known' breaches, but also capture data on impact and response. Impact questions vary by survey, but often include length of system downtime, financial losses, potential reputational damage and anxiety in relation to possible future attack (in relation to surveys of the general public). Response questions include reporting and system upgrade behaviour, among other topics.

The table also includes details of the sampling strategies adopted for each survey. Random sampling strategies yield the most representative data, while non-random approaches produce partial and often biased results. The majority of the surveys on business eCrimes adopt the latter type of sampling, also known as the self-selecting method, due to the prohibitively high cost of the alternative random probability approach. The resulting data pool on business eCrimes is biased towards knowledgeable victims from sectors where IT security is well embedded (i.e. there is an IT security manager to answer the survey questions). Those respondents who are reluctant to respond, due to a lack of knowledge or interest or fear of reputational damage from notification of a breach, are absent from the dataset, leaving a skewed picture of the eCrimes problem. Unlike in some American states, where Security Breach Notification is required by law, creating a near census of breaches (See Anderson *et. al.* 2008), the UK picture from the perspective of surveys adopting non-random samples is partial and biased at best.

While surveys that adopt random probability approaches to surveying eCrimes produce the most representative data, conceptual issues with question wording and with knowledge assumption can undermine the reliability and validity of data produced. Such problems led the European Commission i2010 High Level Group to conclude many of the questions in the Community Surveys on ICT Usage relating to business eCrimes attacks were unreliable. They also reported similar problems in relation to their domestic surveys (i2010 High Level Group, 2006). A European Commission sponsored review into eCrimes questions in the annual Information Society Surveys found questions relating to businesses were likely to be unreliable because: i) SMEs lacked the expertise with technical terms; ii) the outsourcing of security to specialists resulted in the lack of technical details; and iii) the general reluctance

[25] Both recent PwC UK surveys (*Cybercrime, Protecting Against the Growing Threat: Global Economic Crime Survey* 2011 and *Combating Cybercrime to Protect UK Organisations: Global Economic Crime Survey* 2011) are not included in the table due to the global selection of the sample. However, the latter survey does include a relevant analysis of the eCrimes problem in the UK in the larger corporate and public sectors, even though the sample is relatively small and non-random.

of businesses to admit a problem in their own IT systems. In relation to domestic respondents the review concluded eCrimes questions were possibly unreliable due to: i) a lack of expertise with the technical terms such as virus, firewall etc.; ii) the inability to trace back any incident to a certain cause (virus / adware / spyware / fraud); and iii) the ambiguous or vague question wording (Empirica, 2007).

Large-scale random probability national surveys, such as the Crime Survey for England and Wales (formerly the British Crime Survey) [26], the Offending Crime and Justice Survey, and the Commercial Victimisation Survey, have sometimes included questions on eCrimes victimisation and perpetration in their questionnaires. However, surprisingly few respondents reported eCrime experiences, and in the light of other data on anxiety about identity theft and the prevalence of security breaches, this led us to wonder about response validity. Furthermore, questions on e-victimisation are sparse, often only focusing on a very limited range of completed e-fraud[27]. We recommend that eCrimes questions (hard measures such as 'prevalence' as well as soft measures such as 'fears') are reintroduced into these national surveys and that the evidence from the European Commission i2010 High Level Group and Empirica (2007) are taken into account during cognitive testing.

Given the problems outlined, it is apparent that the eCrimes data pool is currently unfulfilled, 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, suffer from poor conceptualisation and a paucity of detailed questions on the topic. The remainder of this data review will focus on the most 'satisfying' datasets available at this moment in time: the Information Security Breaches Survey and the Oxford Internet Survey. The ISBS's history of random probability sampling and adherence to standardised and well conceptualised[28] questions make it the most robust and least biased business eCrimes database in the UK. Similarly, the Oxford Internet Surveys have consistently adopted a random sampling technique and have included a good range of eCrimes questions that the general public understand.

The ISBS is the only national survey of eCrimes breaches that has adopted a gold standard approach to sample selection. This has allowed for appropriate weighting to be employed ensuring each business sector is equally represented. The consistency of the survey approach also means comparisons over time are reliable meaning it has provided the most authoritative picture of eCrime trends over time in the UK up to 2008. The 2010 ISBS adopted a self-selecting sample framework that reduced the representativeness of the findings and therefore precluded a robust basis for comparison to previous ISBS surveys.

[26] The CSEW is not based on a simple random sample and instead uses a stratified and partially clustered sample design.
[27] The BCS included a technology crimes module in 03/04 but it has not since been repeated. The only consistent question in this survey on eCrime relates to identity fraud (since 05/06).
[28] The PwC research team ensured that questions asked in the first survey (1998) became standard for all subsequent surveys. This ensured that (to the extent that they were the same individuals) respondents became familiar with the terms expressed, resulting in plausibly sounder answers over time.

The data for the ISBS 2010 presented in Graph 1 is derived from the responses from small to medium sized firms as they represented the largest group of respondents. It is important to note reports of eCrimes breaches from large firms were far in excess of those reported by SMEs, making the sharp increase in eCrimes attacks in Graph 1 a conservative estimate. What is clear is that the trend in eCrimes attacks has reversed from a general decline since 2004 to a sharp increase from 2010. This is contrary to trends in the US where a general decline in eCrimes breaches has been recorded since 2000 by the CSI Computer Crime & Security Survey. However, it must be stressed that methodological differences between surveys make direct comparisons problematic.

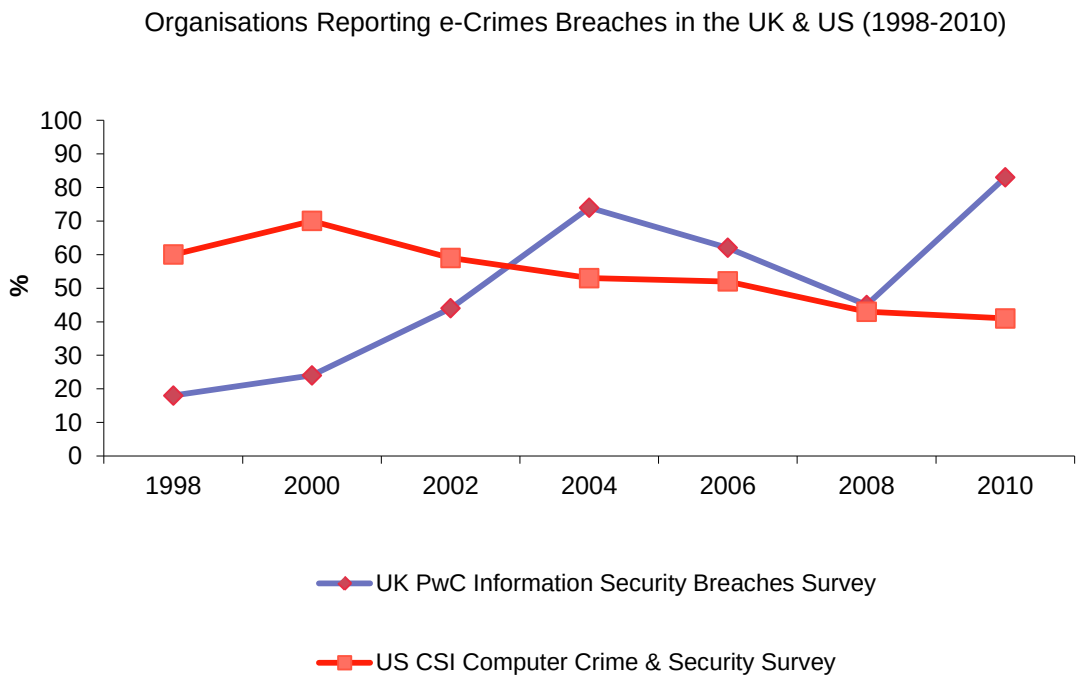


Figure 1

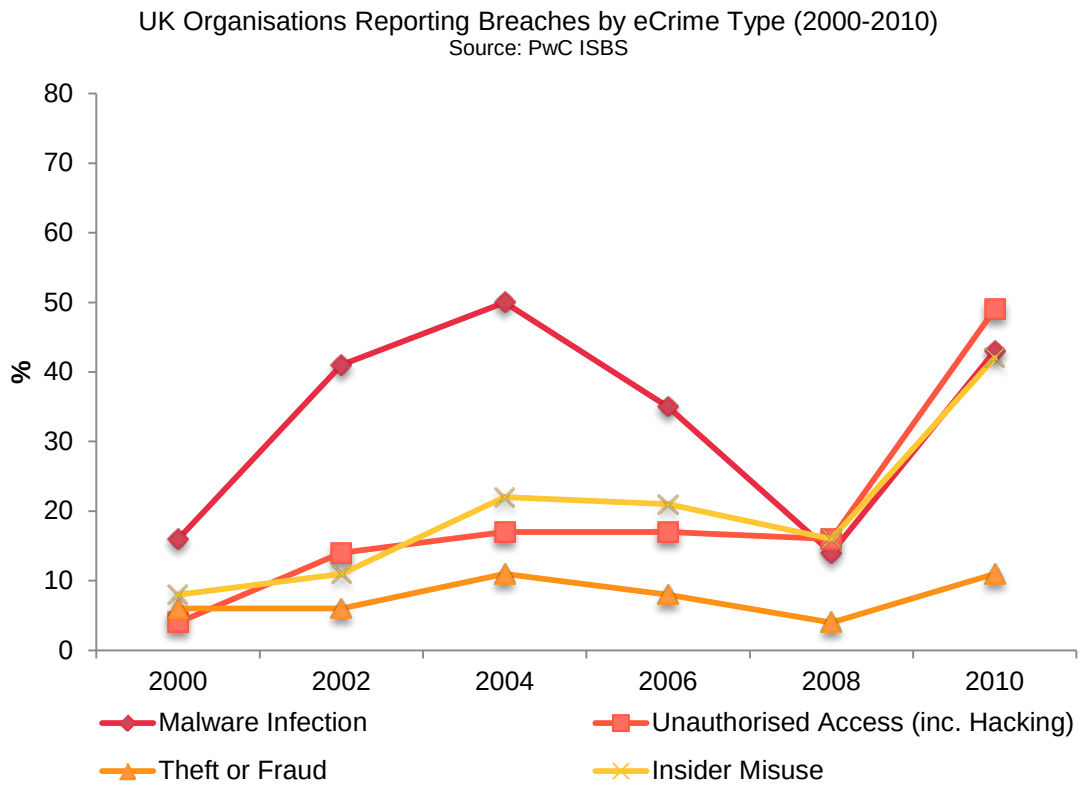


Figure 2

Graph 2 shows ISBS recorded breaches over time disaggregated by eCrime type. Malware attacks show the most marked decrease in breaches between 2004-2008, followed by theft & fraud and insider misuse. The reported prevalence of unauthorised access (including hacking) remained relatively stable in the same period. Reports in 2010 indicate a sharp increase in prevalence for malware infection, insider misuse and unauthorised access, and a slightly modest increase in reports of theft and fraud. Reports of insider misuse and unauthorised access peak at new all time highs (42 and 49 percent respectively), while malware attacks return to near their peak prevalence in 2004. To confirm (or modify) this UK upward trend *validly*, it is imperative that the ISBS adopts its previous gold standard survey strategy during the next data collection phase.

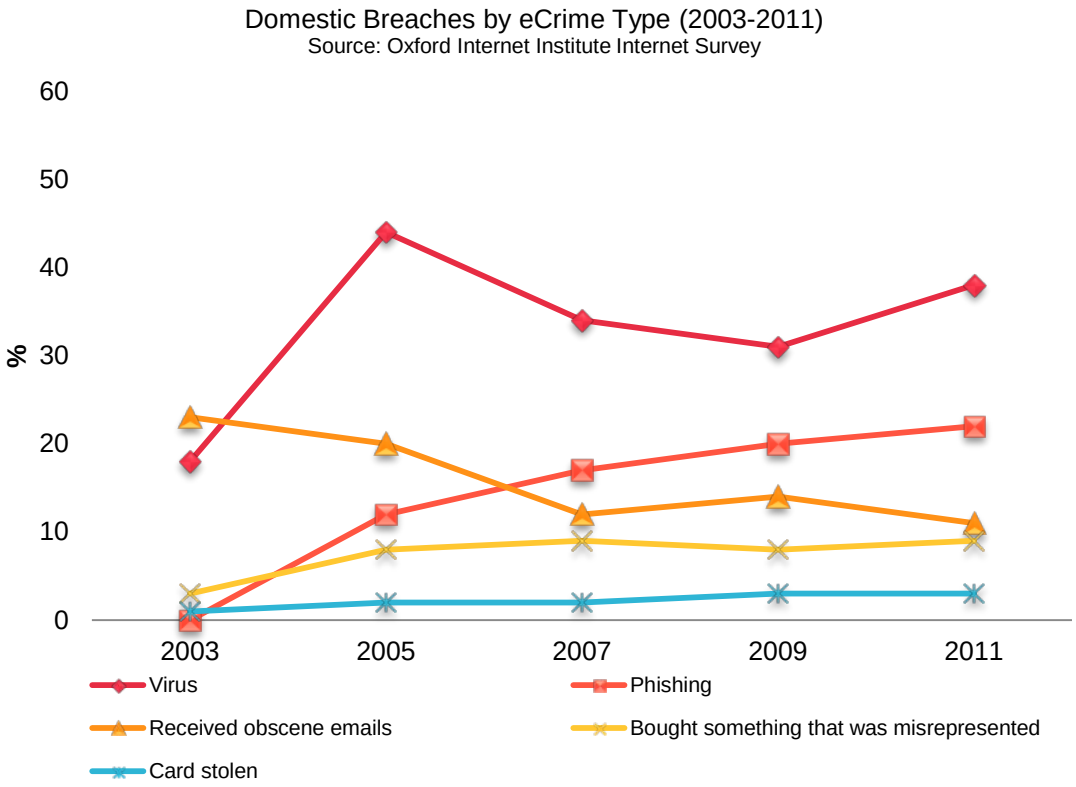


Figure 3

Graph 3 details trends over time in domestic eCrimes breaches collected by the Oxford Internet Survey. Given the public's limited understanding of many eCrime types, this survey adopted more colloquial terms to ensure robust data collection. Unfortunately this precludes a forensic comparison with business eCrimes trends. However, the pattern of those members of the public experiencing virus attacks is similar to the patterns of business malware attacks. A decline is evident from 2005 to 2009, with a definite upward trend in 2011 (an increase of 7 percent compared to 2009). Similarly, there is an upward trend in recorded domestic phishing attempts, indicating, as with business recorded eCrimes, that eFraud is on the increase (although domestic online credit card theft remains stable at 3 percent). These domestic eCrimes data add weight to the position that in general eCrime trends are on the rise in the UK.

THE COST OF ECRIMES TO THE UK

There is a tendency towards inflating costs in under-researched areas, where both falsification and verification are difficult. Anderson et al. (2012) distinguish between traditional crimes that are now 'cyber' because they are conducted online (such as tax and welfare fraud); transitional crimes whose modus operandi has changed substantially as a result of the move online (such as credit card fraud); new crimes that owe their existence to the Internet; and 'platform crimes' such as the provision of botnets which facilitate other crimes rather than being used to extract money from victims directly. (See also Wall, 2007, for a helpful typology.) In few areas can we be more precise than an order of magnitude. However looking at non-state sponsored cybercrime as a whole, traditional offences such as tax and welfare fraud plausibly cost the typical citizen in the low hundreds of pounds a year; transitional frauds cost a few pounds; while the new computer crimes cost in the tens of pence. However, the indirect costs and defence costs are much higher for transitional and new crimes. For the former they may be roughly comparable to what the criminals earn, while for the latter they may be an order of magnitude more. As a striking example, the botnet behind a third of the spam sent in 2010 earned its owners around US$2.7m, while worldwide expenditures on spam prevention probably exceeded a billion dollars. In sections that follow, we set out some relevant data without duplicating the work of Anderson et al. (2012), to which one of us contributed.

Bank losses from eCrime

The majority of studies are sectoral. One good example of a sectoral study using administrative data is the annual report from Financial Fraud Action UK via UK Payments (formerly, APACS), which collates reports made to it by member banks, which comprise most retail banks. Not everyone accepts that the banks properly record as fraud all eFrauds reported to them as such. There are two issues here: one (much broader than its application to eCrime) is that there is a discretionary judgment about whether to classify losses as 'fraud' or as 'bad debt', which judgment varies between financial institutions in ways that even their senior management may be unaware of; the second is the 'phantom withdrawals' issue, in which the banks resist claims by Ross Anderson and the Cambridge Computer Laboratory that malfunctioning – intentional and otherwise – in the ATM technology lead them to misattribute as customer negligence losses to customers that do not result from customers' negligence but rather result from design flaws (and insider corruption). But no-one has seriously tried to estimate the scale of such alleged mis-attribution, or what difference it would make to the £29.3 million the banks state they lost from ATM fraud in 2011. Such misattributed losses are unlikely to be very large: the argument is over who pays for the fraud. It might make a difference if one were comparing *consumer* eFraud losses versus *bank* eFraud losses. In the scale of eCrime, however, it is unlikely that such disputed transactions are significant, however bitter may be the feelings of individuals denied compensation and however well-publicised these events are in the consumer press and television.

Total fraud losses on UK cards fell by seven per cent between 2010 and 2011 to £341 million. This is the lowest annual total since 2000. Card fraud losses against total turnover – at 0.06% – are at a record low and are half of the ratio in 2008, reflecting significant prevention measures rather than any known reduction in criminal motivation.

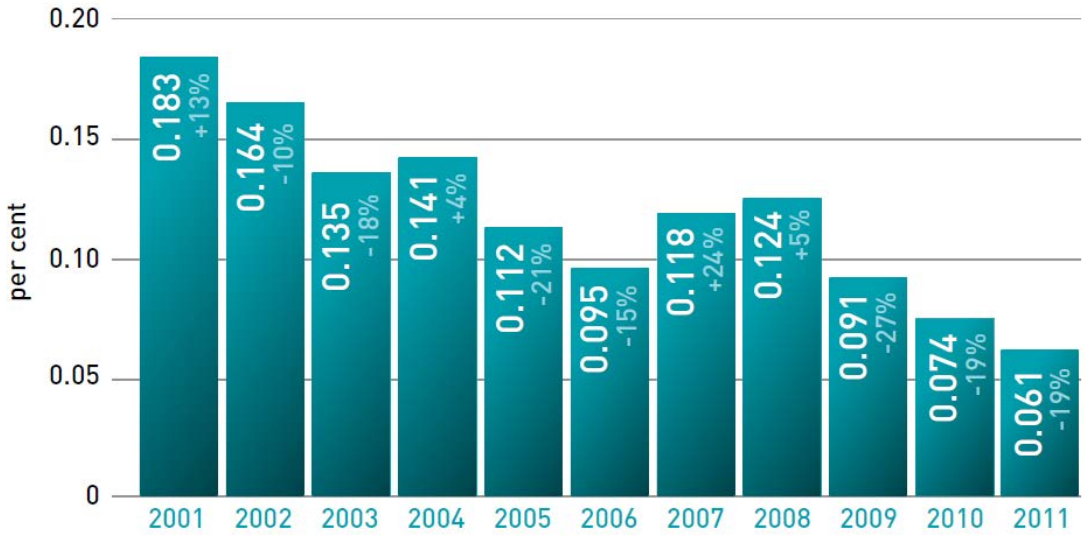


Figure 4 - Fraud to Turnover Ratio on UK-issued Cards 2001-2011

More generally, UK Payments calculate in aggregated form the losses to customers, reimbursed by banks, of e-commerce frauds; and they separately report the losses arising to customers from Internet Banking. The data are estimated largely because it is not easy to deduce ecommerce from the categories used to record card transactions, many of which predated the rise of ecommerce. The data exclude PayPal, wire transfers and other payment mechanisms. An estimated £139.6 million of card fraud took place over the internet in 2011, up from £135.1 million in 2010, but still significantly lower than losses 2006-2009. Internet fraud now accounts for 63% of card-not-present losses. The estimated total value of Internet card spending rose by almost 150% 2005-2010 to £53.6 billion in 2010, and the eFraud losses therefore have risen at a slower pace than the ecommerce transactions. This ratio arguably is a more valid measure of changes in harm than are the absolute fraud losses, though the (unmeasured) anxieties provoked by concerns that fraud is rising are themselves additional to these figures. It is intriguing to consider what those anxieties would be if no data were published but if the public instead relied solely on anecdotes or 'guesstimated' figures in the media and in social online and offline discussions. (It is also moot how many of the 'anxious public' have ever read or absorbed these data, though they are well reported in the broadsheet and some popular press.)

The vast majority of this type of fraud involves the use of card details that have been fraudulently obtained through methods such as skimming, data hacking, retail employee data 'theft'/unlawful copying of data files, or through unsolicited emails or telephone calls. The card details are then used to undertake fraudulent card-not-present transactions. The Financial Fraud Action UK (2012) data are set out below:

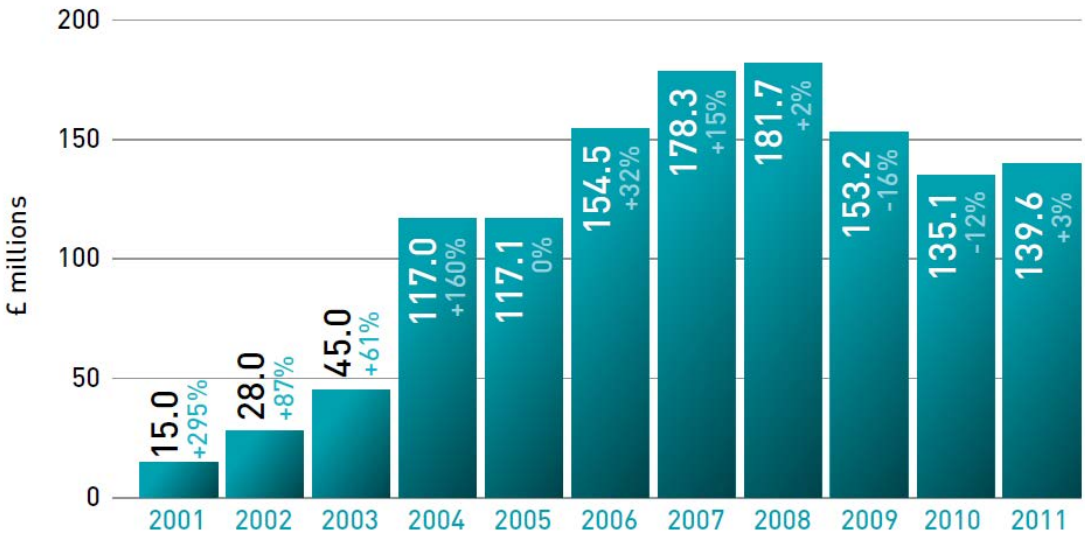


Figure 5 – Internet/e-Commerce Fraud Losses on UK-issued cards 2001-2011

A different way of thinking about the data – and a better way of thinking about risks – is to examine the bank-identified and centrally reported phishing attacks. In the abstract, in line with 'routine activities' models of crime, these data reflect criminals' estimates of the weakness of prevention measures, their skills (which evolve with experimentation and with changes in their networks), and the cheapness of attacks. Financial outlay for criminals is very modest, and the opportunity cost of their time depends on what they would otherwise be doing. The significant rise over time – and the 80% rise since 2010 - indicates how routine these attacks have become, though the absence of corresponding rises in reported losses suggests that their average success is falling significantly, even if this does not matter much to them because the economic and criminal justice costs of attempts are negligible.

NUMBER OF PHISHING WEBSITES* TARGETED AGAINST UK BANKS AND BUILDING SOCIETIES BY MONTH 2005-2011

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	TOTAL
2011	5,803	5,757	6,828	5,698	6,216	6,896	7,402	8,062	23,083	9,397	15,395	10,749	111,286
2010	2.654	3,135	4,810	4,335	5,406	5,277	5,873	5,861	5,689	6,977	4,552	7,304	61,873
2009	4,206	5,161	5,004	3,422	3,917	4,335	4,415	4,845	3,900	4,903	4,191	5,864	51,161
2008	3,144	3,243	3,848	3,719	3,091	3,637	3,584	3,716	4,121	4,536	3,896	3,456	43,991
2007	1,290	974	1,130	1,188	1,274	1,368	3,066	3,268	2,597	3,170	3,277	3,195	25,797
2006	606	669	1,074	947	919	872	970	1,484	1,513	1,596	1,993	1,513	14,156
2005	18	29	27	54	72	122	153	160	190	267	255	353	1,700

* Fraudsters set up a website that is a fake version of a genuine bank website, and then send out thousands or even millions of spam emails trying to convince people to click on a link that will send them to that fake site.

Figure 6

Below are the data on UK banks' statements about the losses to individual customers (instantly or later reimbursed by them) of online banking fraud. They do not include data on fraudulent attacks against banks other than through individual customer accounts. Some interviewees suggested that these losses may not be fully reported centrally because

of concerns that consumers may become 'excessively' fearful, or because not all banks identify losses as fraud rather than as bad debts in the same way. However we are not in a position to assess the validity of such claims, still less to assess what the 'true figure' might be. There are unavailable corporate losses from misconduct by staff at different levels, which are not included in these data.

Figure 7

To place these losses in context, although ecommerce might be (a) greater if people were less concerned about fraud and identity theft arising from internet use, and (b) slightly less if people were less fearful of going out to shop because of general perceived crime risks, the seemingly inexorable rise of ecommerce shows that most adults in the UK are not wholly deterred by risks. (Though the OFT, 2009, highlighted that one in three internet users do not shop online. The most commonly identified reason for shoppers opting not to use the internet was a lack of trust in its security.) We make no attempt here to estimate the 'digital divide' costs of people who are unable or unwilling to purchase online, whether from fear of fraud or from economic (or, more rarely nowadays, technological availability) reasons, though Anderson et al. (2012) estimates possible UK indirect costs at some £450 million. Ecommerce Industry body IMRG states[29]:

- The UK is Europe's leading e-retail economy, with sales of £68.2bn in 2011. Global e-retail sales increased by almost 25% to €591bn in 2010.
- The UK e-retail market grew 16% 2010-11
- The UK's per capita spend was £1,850 in 2011

[29] http://www.imrg.org/IMRGWebSite/user/pages/homepage.aspx

37 million people shop online in the UK, out of 50 million with internet access (around 70% of the population). One of the problems in assessing costs is that in many respects this is a static way of collating the effects of prevention failures (or the absence of prevention attempts). The British Retail Consortium (BRC, 2010: 7) notes that one retailer who uses the services of a third party screening company reports that for every £100,000 online orders a further £30,000 of online transactions are fraudulently attempted. Another retailer estimates that up to 20 per cent of their total web sales would be fraudulent if they did not have anti-fraud systems.

Although in the vast majority of offences customers will be protected under the banking code and, therefore, will not suffer a financial loss. The BRC (2010) notes – without giving details of the firm's turnover or profits – that one retailer has reported that in 2009/2010 they lost £252,000 to fraud. This was in addition to £3.6 million of attempted fraud. Retailers are also required to keep fraudulent transactions below one per cent of turnover to avoid sanctions from their acquiring banks. 3D Secure (e.g. Verified by Visa and MasterCard SecureCode), which prompts customers using these cards online to provide mechanisms to reduce that risk to retailers. The BRC (2012) retail crime survey gives little data, but noted (p.36) that after laptop/PC theft (which we would not consider to be properly included as computer-related crime), the second most common computer-related crime risk was spam email, which affected 47.5 per cent of respondents, followed closely by phishing at 31.7 per cent. However, retailers' top concern was credit card fraud, followed by theft of company data.

Visa-owned technology firm Cybersource (2012) has had an annual online survey for eight years that is not random or representative but contains a fairly even distribution of firm size and a varied set of private sector firms. The report notes that on average, merchants expect to lose 1.8% of revenues to fraud in 2011, slightly higher than the previous year. As in previous years this figure is pulled up by higher expectations in certain industries and amongst some specific merchants; 31% of merchants (fewer than the previous year) expect to lose less than 1%. Fraud losses in the physical goods sector is notably lower than in services. However, the survey sensibly makes no attempt to gross these up into national figures. For around half the firms in the travel and services sectors, the biggest concern is sheer revenue loss. For physical goods retailers, the greatest concern of half the firms is inadvertently turning away good orders. For digital goods businesses the principal challenge is the cost of manually reviewing too many orders (41%). Merchants reject on average 4.3% of incoming orders due to suspicion of fraud – a return to more historically typical figures following a spike to 5% in 2010. Nearly a third of merchants report that they are rejecting more than one in 20 orders on suspicion of fraud (reflecting the transfer of liability to them under card regulations). Unlike previous surveys, where there was a clear differentiation between rejection rates in the various sectors, in 2011, there was rough parity between the physical goods, digital, services and travel industries. As the report states (p.7):

> "The true cost of payment fraud is a combination of many factors beyond the simple losses represented by chargebacks. Alongside these direct revenue costs, the cost of the stolen goods/services and associated delivery/fulfilment costs,

> businesses have to account for: falsely rejected valid orders, manual review staff, fraud claim administration, internal systems maintenance, and third-party tools."

On the basis of non-representative sample research, not-for-profit fraud prevention service CIFAS has stated that in cases where a customer's account has been completely taken over by a fraudster as a 'total hijack' and used for both new and existing credit accounts, this can involve around 20-30 different organisations. More generally, CIFAS data supplied to us show roughly 70,000 people being victimised annually, of whom around a tenth suffer multiple victimisation (on 2-17 separate occasions). It may subsequently take the victim over 200 hours before things return to normal. They may suffer considerable (albeit temporary) damage to their credit status, which can affect their ability to obtain finance or insurance. Large scale data compromises plausibly generate less repeat victimisation for their population, since it is less effort to trawl through easy opportunities, casting aside harder-to-use data, but this is merely a hypothesis. At a minimum of an estimated 20,000 victims a year, the opportunity costs of time, uncompensated collateral expenses, and other social costs are considerable, but no median or average cost data are available, so more realistic aggregate data are not deducible.

The British-based technology firm Detica and Cabinet Office (2011) conducted an interesting study, noting in their summary of their methodology (p.2):

> To address the complexity of less understood cyber crime…we develop a causal model, relating different cyber crime types to their impact on the UK economy. The model provides a simple framework to assess each type of cyber crime for its various impacts on citizens, businesses and the Government. We use the causal model to map cyber crime types to a number of broad categories of economic impact, which are generally consistent with the types of parameters used in macro-economic models of the UK. We then calculate the magnitude of the costs of cyber crime using three-point estimates (worst-case, most-likely case and best-case scenarios), focusing in particular on IP theft and industrial espionage and its effect on the different industry sectors.
>
> Our assessments are, necessarily, based on estimates and assumptions rather than specific examples of cyber crime, or from data of a classified or commercially-sensitive origin. We have drawn instead on information in the public domain, supplemented by the tremendous knowledge of numerous cyber security, business, law enforcement and economics experts from a range of public and private-sector organisations.
>
> In our most-likely scenario, we estimate the cost of cyber crime to the UK to be £27bn per annum. A significant proportion of this cost comes from the theft of IP from UK businesses, which we estimate at £9.2bn per annum. In all probability, and in line with our worst-case scenarios, the real impact of cyber crime is likely to be much greater.
>
> Although our study shows that cyber crime has a considerable impact on citizens and the Government, the main loser – at a total estimated cost of £21bn – is UK

> business, which suffers from high levels of intellectual property theft and espionage. Businesses bearing the brunt…are providers of software and computer services, financial services, the pharmaceutical and biotech industry, and electronic and electrical equipment suppliers.

This is a valuable contribution to thinking through the different dimensions of eCrimes: though as with many attempts (for example, estimating the cost of organised crime to the UK – Dubourg and Prichard, 2009) the realism of the underlying assumptions is difficult to assess, and a different set of assumptions would have produced much larger or (plausibly to us) much smaller figures, and a different *pattern* of harm impacts of eCrimes on different sectors of the population. Since the evidential basis for the assumptions and the models themselves used by Detica are not available, we reluctantly conclude that these data do not meet acceptable quality standards, though the report has considerable heuristic value in alerting us to the range and potential consequences of cybercrimes. Though there are grounds for taking the problem seriously, we doubt whether the high *proportion* and costs of e-espionage are correct (though the figure is more plausible as a 'guesstimate' of the cost of such IP crimes committed via corrupt employees and by external hacking): a sceptical view shared by some of the specialist media and by Anderson et al. (2012).

There is a regrettable if understandable trend in consciousness-raising reports to highlight figures that generate alarming headlines, which (as with money laundering figures) must generally rise over time in order to avoid complacency. These data also highlight (or should highlight) the definitional issue as to whether it is really sensible to call every crime which – at some stage in its process from financing through commission to money laundering – uses electronic signals or transfer in some form. Given the ubiquity of computers in contemporary society, it is rare indeed to find forms of profitable crime that are *not* computer-enabled at some stage of their commission. This is acknowledged in the PwC survey definitions, but it is not clear if it also applies to the Detica or other studies, and it is in any case difficult to apply consistently. In our view, identity frauds should include new credit applications using duplicated identity details but not frauds committed with stolen cards, which wrongly inflate the totals.[30] However, whatever the source of the cards, all numbers used or attempted for on-line purchases should count as eFrauds. In conclusion, taking the field as a whole, contemporary data are too poor in rigorously defined quality to enable us to produce a defensible estimate of the economic cost of eCrimes to the UK (or to anywhere else). **What is plain is that these costs have risen over time, that defending ourselves against them has become more difficult and more expensive, and that there is no reason to expect the costs and impacts to fall without significant intervention.**

[30] Our view is shared by Financial Fraud Action UK, who exclude such offences from their category of identity frauds.

SURVEY FINDINGS

This section of the report features an analysis of the survey conducted with members of the UK Information Assurance Community. It is delineated into the following sections: i) Description of respondents; ii) Perceptions of the eCrimes problem; iii) Perceptions of eCrimes data sources; iv) Perceptions of eCrimes control; v) Perceptions of UKIA organisations; and vi) Perceptions of cooperation.

1. Description of UKIA Organisations

All responding organisations that took part in the study belonged to the UK Information Assurance Community. Table 2 provides details of the organisations who responded to the online survey. The largest group of responding organisations are the private sector (37.6 percent), with IT security suppliers making up the majority, followed by 'other' private organisations and financial services. Just under one fifth of respondents (18.3 percent) originate from government and public sector organisations and just over 13 percent come from groups and regulatory bodies. Just over 10 percent of respondents originate from the police and 12.5 percent from charities/non-profit organisations. Half of responding organisations have 250 employees or more (48.1 percent) and have been in operation for over 20 years (52.9 percent). Small (between 1-9 employees) and young (5 years or less) organisations represent just over one fifth of the sample (20.2 and 19.2 percent respectively).

The majority of organisations provide advice and services regarding eCrime to the police (67.8 percent) and government departments (61.5 percent). Over half of organisations provide advice/services to the private sector, and only 8.7 percent provide no advice or services. Charts 1.1 to 1.3 provide a breakdown of advice/support by type of organisation. Chart 1.1 indicates that groups and regulatory bodies are most likely to provide advice/services to government departments while the finance sector are least likely. In relation to providing advice/services to private sector non-finance organisations, private sector (other) are most likely compared to the finance sector who are least likely. This is in contrast to the provision of advice/services to the general public where the finance sector emerge as most likely compared to the private sector (other) who are least likely.

Table 2: Organisation Characteristics (N=104)

		N	%
Organisation Type	Central Gov - CJ related	6	5.8
	Central Gov - non CJ related	3	2.9
	Local Gov	3	2.9
	Gov-Industry Group	1	1.0
	Other Public Sector Body	7	6.7
	Private Sector - IT Security Supplier	16	15.4
	Private Sector - Finance Services	9	8.7
	Private Sector - Other	14	13.5
	Professional Body	4	3.8
	Industry Group	7	6.7
	Academic/Research Body	8	7.7
	Regulatory Body	2	1.9
	Charity/Not for Profit	13	12.5
	Police	11	10.6
Size	1-9	21	20.2
	10-49	7	6.7
	50-249	25	24.0
	250 or more	50	48.1
Time in operation	Less than 1 year	3	2.9
	1-5 years	17	16.3
	6-10 years	9	8.7
	11-15 years	12	11.5
	16-20 years	8	7.7
	Over 20 years	55	52.9
Provides advice/services to	Government Departments	64	61.5
	Parliament	35	33.7
	Private Sector (Financial)	60	57.7
	Private Sector (Non-Financial)	59	56.7
	SMEs	50	48.1
	The General Public	49	47.1
	The Voluntary Sector	28	26.9
	The Police/Criminal Justice organisations	70	67.8
	The Education Sector	39	37.5
	Other Public Sector Bodies	46	44.2
	Does not provide advice/services	9	8.7
	Other	7	6.7

Note: All percentages are valid

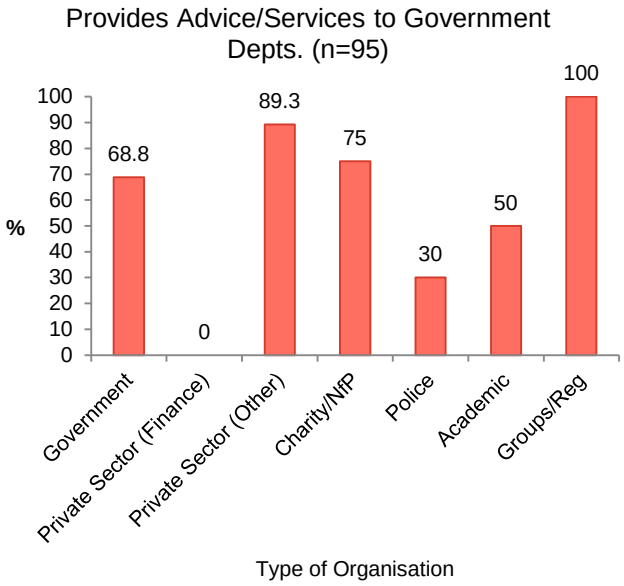


Chart 1.1

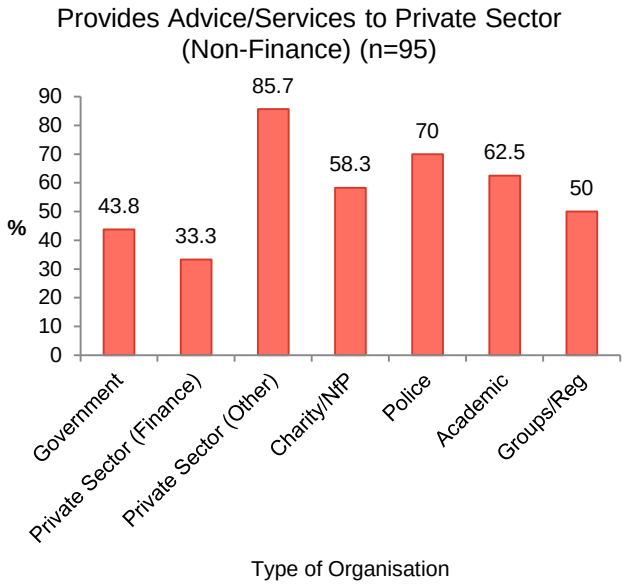


Chart 1.2

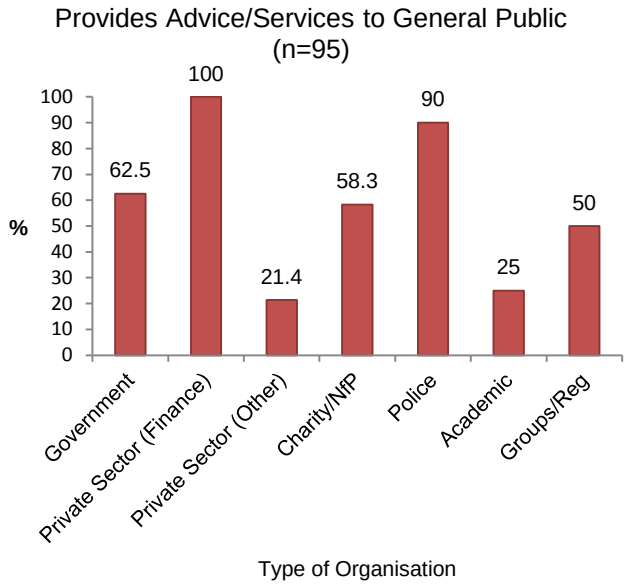
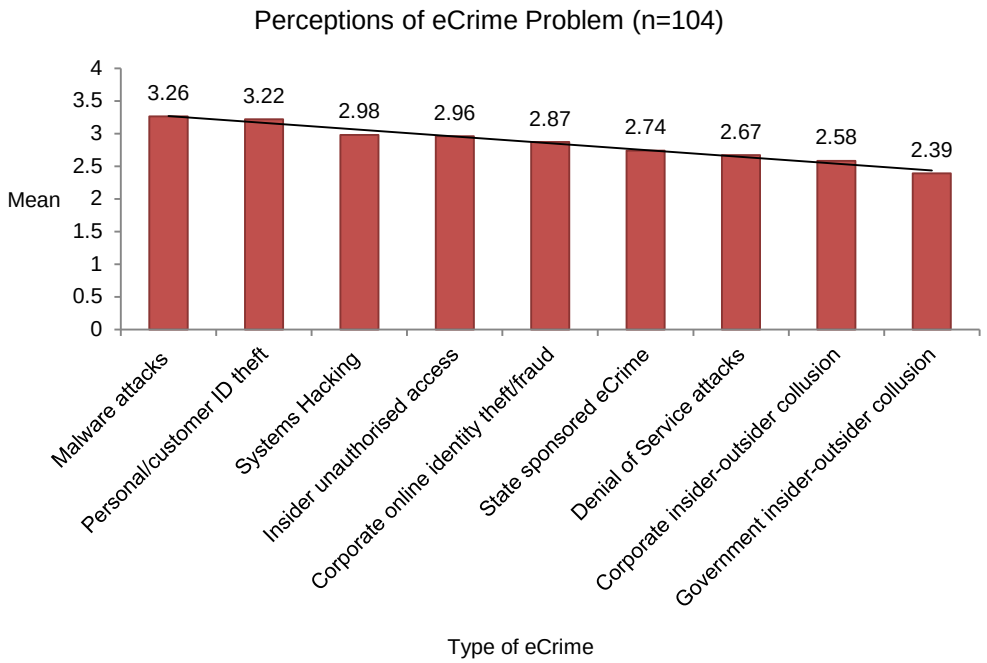


Chart 1.3

2. Perceptions of the eCrime Problem

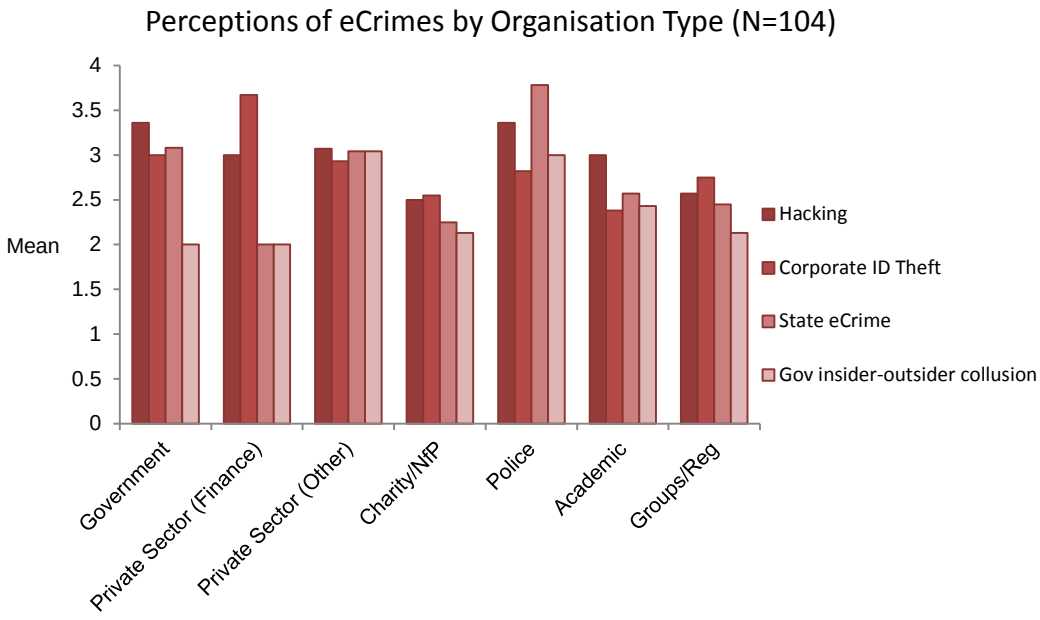
The survey gathered data on the perceived current eCrime problem. On a scale of 1 to 4 (where 1 is not at all a problem and 4 is a very serious problem) UKIA organisations were asked to indicate their perception for each type of eCrime. Chart 2.1 details the results by type of eCrime. The majority of organisations indicate that malware attacks are the most problematic at this point in time. This mirrors data provided by the ISBS 2010 and the Oxford Internet Survey 2011 that both indicate malware infections are increasing. Perceptions of the current problematic nature of customer ID theft, hacking and insider unauthorised access are also commensurate with recent increases in their prevalence as recorded by both surveys. State sponsored eCrime[31], DoS attacks and corporate and government insider-outsider collusion emerge as lesser concerns. It is interesting to note that state sponsored eCrime features in the lower half of concerns, despite recent media and political attention on the topic. However, it is prudent to remain clear that the means for eCrimes perceived as less problematic rest relatively high on the overall scale, between 'somewhat of a problem' and 'quite a serious problem'.



(1=Not a problem; 2=Somewhat a problem; 3=Quite a serious problem; 4=Very serious problem)

Chart 2.1

[31] We acknowledge that state sponsored eCrime is an organisational locus rather than a form of eCrime itself, and therefore differs from the other categories used. Given the recent concern with information warfare we believed it prudent to include a question on the topic, to gauge the opinion of the UKIA community. It is included in this chart to indicate its relative place in the hierarchy of overall eCrime concerns. Its exclusion from the chart would not impact upon the overall ordering of the hierarchy.



*(1=Not a problem; 2=Somewhat a problem; 3=Quite a serious problem; 4=Very serious problem)

Chart 2.2

Chart 2.2 provides a breakdown of perceptions of the eCrime problem by organisation type. Systems hacking, corporate ID theft, state eCrime and government insider-outside collusion emerge most significant in producing divergent perceptions (there is relative homogeneity in perception for all other types of eCrime by organisation type). The police and government departments are most likely to perceive hacking as most problematic, whereas groups (e.g. government-industry groups and industry groups), regulatory bodies and charities/Not for Profits (NfPs) perceive it to be less problematic. The finance sector perceives corporate ID theft as most problematic, by contrast with academic and research organisations who perceive it as less problematic. In relation to state sponsored eCrime the finance sector perceive it as least problematic compared to the police who perceive it as most problematic. Government insider-outsider collusion is perceived as most problematic by private sector (other) and least by government departments and the finance sector.

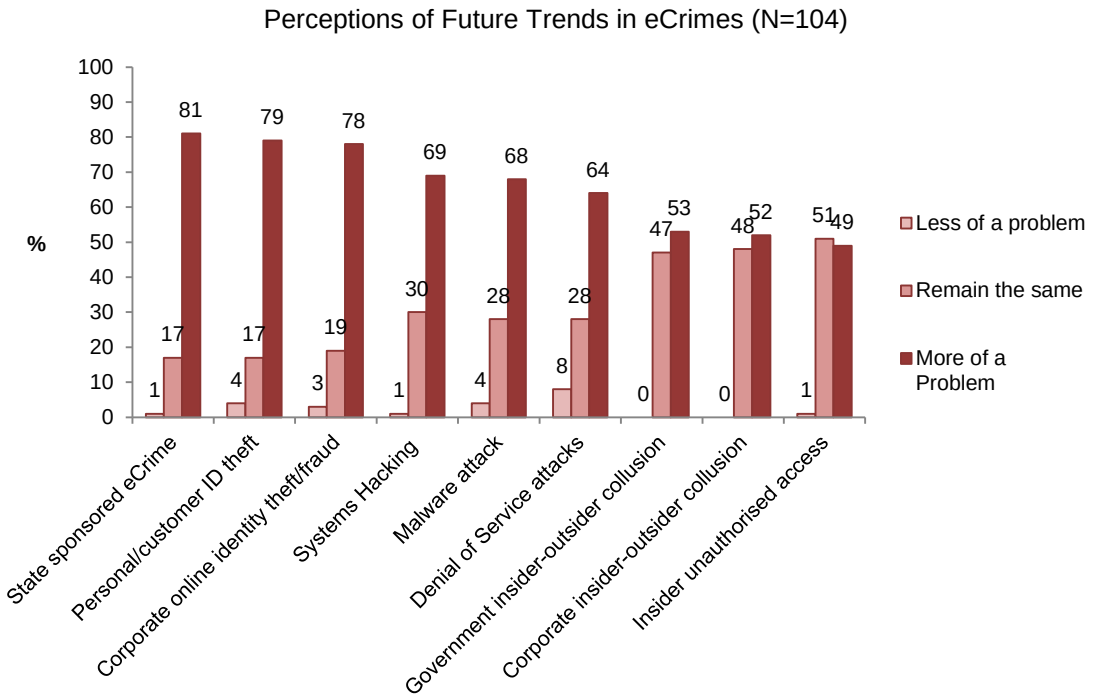


Chart 2.3

The survey also invited all the UKIA organisations in the sample to indicate which eCrimes they thought would become more of a problem, less of a problem or remain the same in the future. Chart 2.3 shows most organisations indicate all eCrimes would either become more of a problem or remain the same[32]. It is interesting to note here the asymmetry of future trends when compared to perceptions of the current problem in relation to some eCrimes. In perceptions of future trends state-sponsored eCrime has jumped six places to first, with 81 percent of organisations rating it likely to become more of a problem. Malware attacks are relegated to fifth place from first in current concerns, while insider unauthorised access is relegated to last place from fourth. Personal ID theft/fraud remains in second place, while the other eCrimes remain relatively commensurate with current perceptions. The asymmetry expressed in relation to state eCrime is likely to be an artefact of the 'unknown' future nature of the problem and the recent media attention. The relegation of malware from first to fifth place is not commensurate with recent trends indicating a significant rise in infection, both in the business sector and domestically. However, given the downward trend of infection between 2004 and 2008, it is not surprising respondents' expectations for the future follow a similar, if out-dated pattern.

[32] It is important to reiterate that this ranking reflects *relative* perceived harms, not absolute levels.

3. Perceptions of eCrime Data Sources

UKIA organisations were asked which eCrime data sources they consulted and valued. Given the paucity of 'good' eCrime data it is important to understand what organisations with a responsibility in eCrime control are consuming. Chart 3.1 shows that the top three most consulted data sources are academic, private security national and international surveys[33]. The least consulted are UK Payments, CIFAS Fraud Prevention Service and virtual market sources. Over 70 percent of UKIA organisations report consulting Academic research which is almost twice as likely to be consulted compared to VMS sources and CIFAS data. Just under two thirds of UKIA organisations consult private security surveys. Police recorded eCrime data and the Information Security Breaches Survey are consulted by just over half of UKIA organisations in our sample.

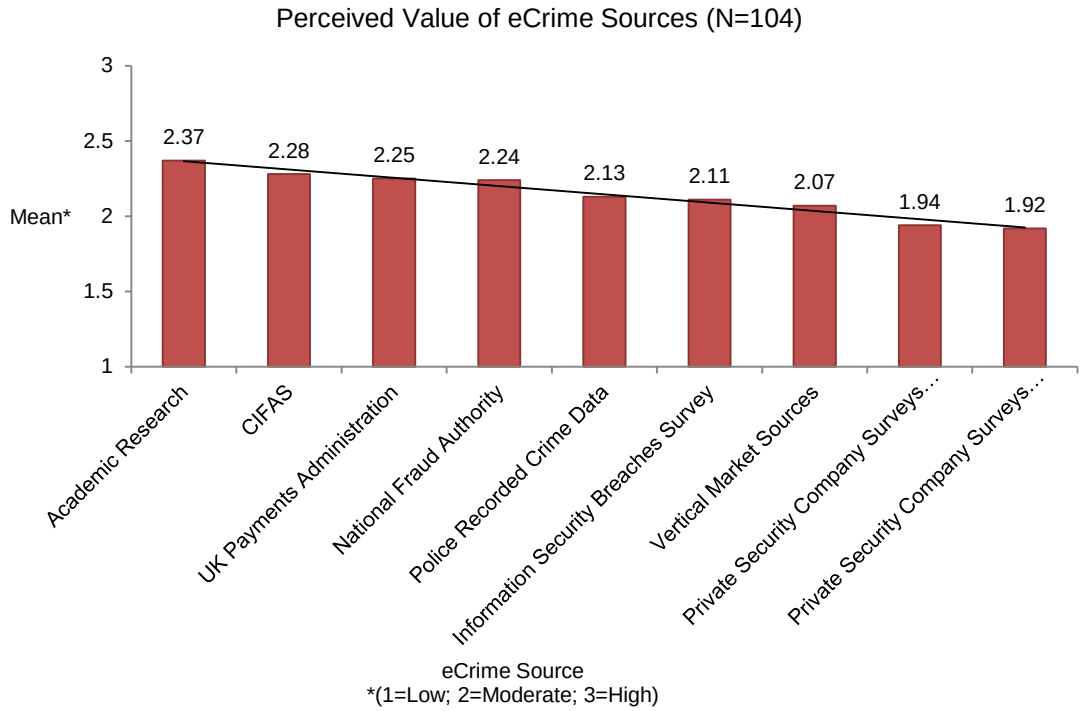


Chart 3.2

UKIA organisations were also asked to rate the value of eCrime data sources on a three-point scale (1=Low value; 2=Moderate value; 3=High value). An interesting asymmetry emerges between what is consulted and what is most valued. Although consulted widely, Chart 3.2 shows that private security surveys are least valued. Conversely, UKPA and CIFAS sources, while less popular in terms of consumption, appear highly valued. A possible explanation for this asymmetry might be that while private security surveys provide valuable vendor data, consumers are aware of their limitations and potential bias. Furthermore, given the paucity in data source choices, UKIA community members may think it prudent to consult as much data as possible, no matter what value they may place on a source. The lack of consultation of UKPA and CIFAS sources may relate to their narrow data collection remit (principally financial services). Their high value is likely to stem from the nature of the data and the method of collection as well as the non-commercial

[33] We stress that this chart represents what data is consulted, not what is most valued.

sponsorship of the organisations. The overall mean (2.14) indicates that the majority of respondents see the value of eCrime sources on the whole to be just above moderate. This reflects the conclusions of the review of eCrime data sources we outlined earlier in this report.

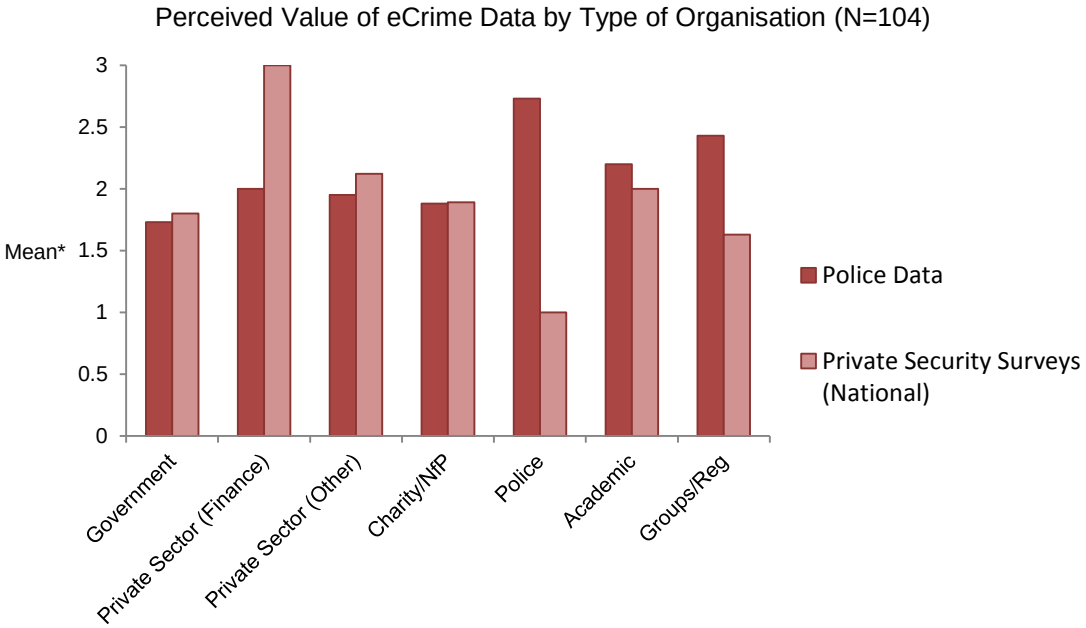


Chart 3.3

Chart 3.3 disaggregates perception of value by UKIA organisation type. Perceptions of police and private security (national) data are most divergent producing significant differences between UKIA organisations. Not surprisingly, the police are around one and a half times more likely to value police data compared to government and charities/NfPs who value them least. However, most stark is the significant difference in value of private security data. The finance sector are three times as likely to value this source compared to police who indicate the least value. It is clear there is little consensus amongst UKIA organisations with regards to these data sources. Given this divergence in perception we recommend further investigation to confirm these patterns.

4. Perceptions of eCrime Control

Perceptions of control formed a key aspect of the survey. On a scale of 1 to 4 (where 1 is very easy to control and 4 is a very difficult to control) UKIA organisations were asked to indicate their perception of control for each type of eCrime. Chart 4.1 shows that aside from state eCrime, there is little difference between all other eCrimes in terms of perceived control. The overall mean (2.97) indicates that the majority of respondents find eCrime quite difficult to control. Both types of insider-outside collusion feature towards the top end of the scale, while malware and systems hacking are perceived easiest to control. Data on insider-outsider collusion are rare precluding a comparison of this finding with any sound source. However, it is possible the human element present in these types of eCrimes results in the perception that they are more difficult to control in comparison to more technology dependent eCrimes. The perception amongst UKIA organisations that malware and hacking attacks are easier to control may relate to their technological dependency and that the ISBS shows their control was relatively effective between 2004 and 2008.

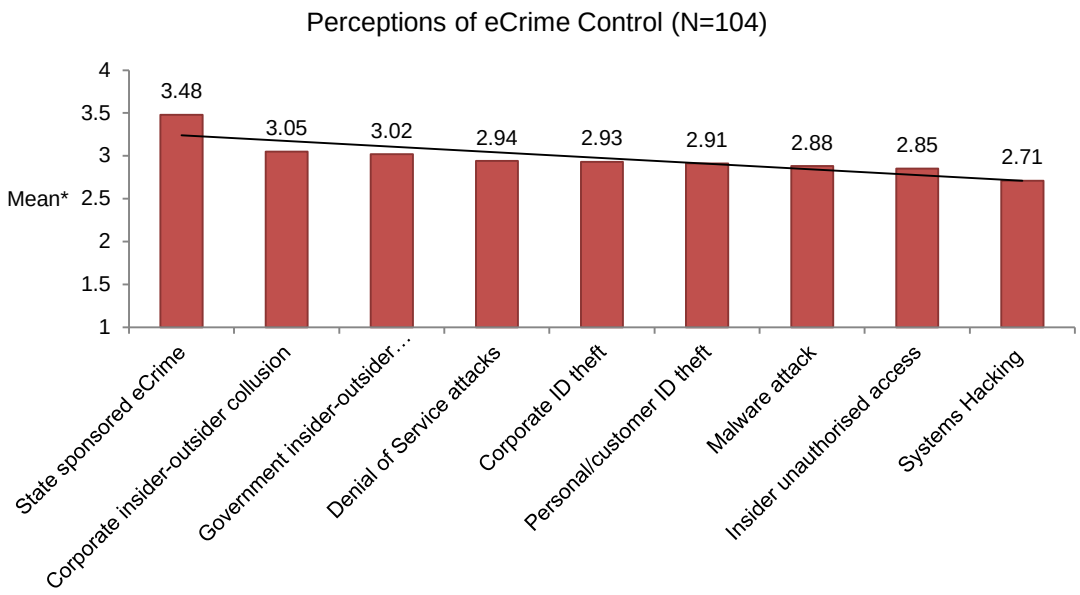
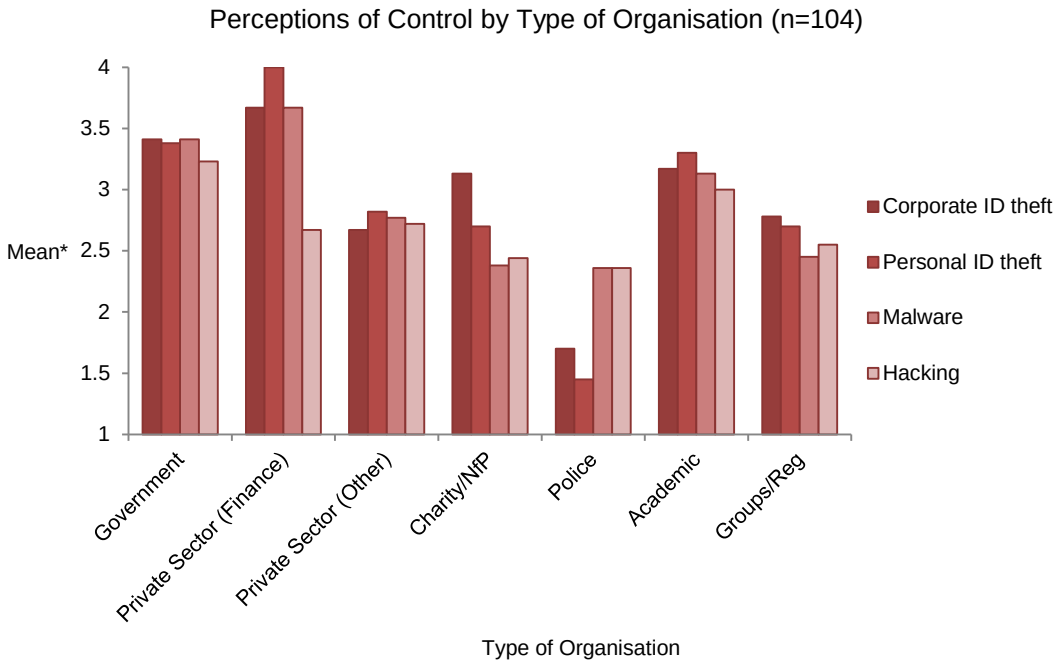


Chart 4.1

Chart 4.2 presents a disaggregated overview of perception of control by type of UKIA organisation. There are stark significant differences by organisation type in relation to control of personal identity theft and malware attack. Private sector (finance) and government departments are over twice as likely to see personal identity theft as more difficult to control compared to the police. Furthermore, this pattern repeats in relation to the perception of the control of malware – private sector (finance) and government departments are nearly one and a half times as likely as the police to see malware as more difficult to control. **Accounting for these differences in perception is difficult without further research; however one might assume differences in occupational culture and technological understanding may play their part in perception formation. If it is found that these differences are borne out in further research it will be necessary to identify how these perceptions relate to action (or inaction).**



*(1=Very easy to control; 2=Quite easy to control; 3=Quite difficult to control; 4=Very difficult to control)

Chart 4.2

5. Perceptions of UKIA Organisations

Perceived Importance of Organisations in Tackling eCrimes

The next section of the survey asked respondents to rank UKIA organisations in terms of their *perceived* importance[34] in tackling the eCrime problem (where 1=unimportant through 4=important). Perceived importance was interpreted subjectively by respondents and chart 5.1 shows a ranking of perceptions of organisations from most important to least. It is important to note that the overall mean is high (3.34), meaning the majority of organisations are rated as quite important or important in tacking the eCrime problem. Central government (criminal justice related) departments, such as the Home Office, are perceived as most important along with the private sector (IT). Perceived as nearly equally important are the finance sector and the police. Organisations perceived as less important include various groups (industry and government-industry), professional bodies, local government and charities/NfPs. However, it is notable that even those at the bottom of scale score well (around quite important) which may be explained by the excellent work of organisations in devolved administrations (e.g. eCrime Wales Project) and local government (e.g. Yorkshire eCrime Business Centre).

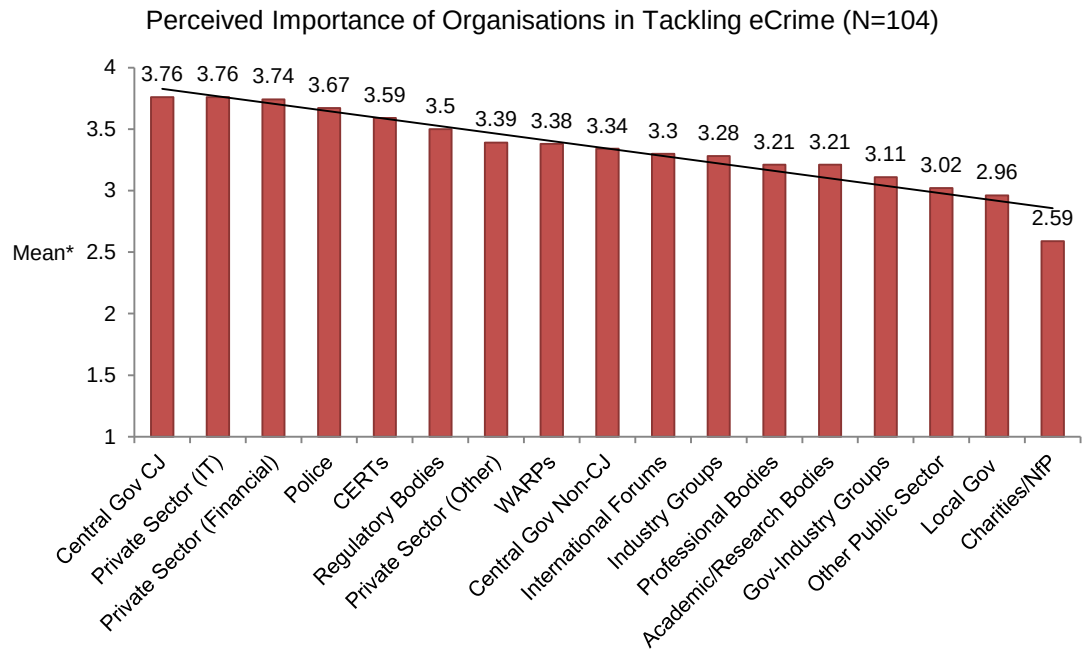
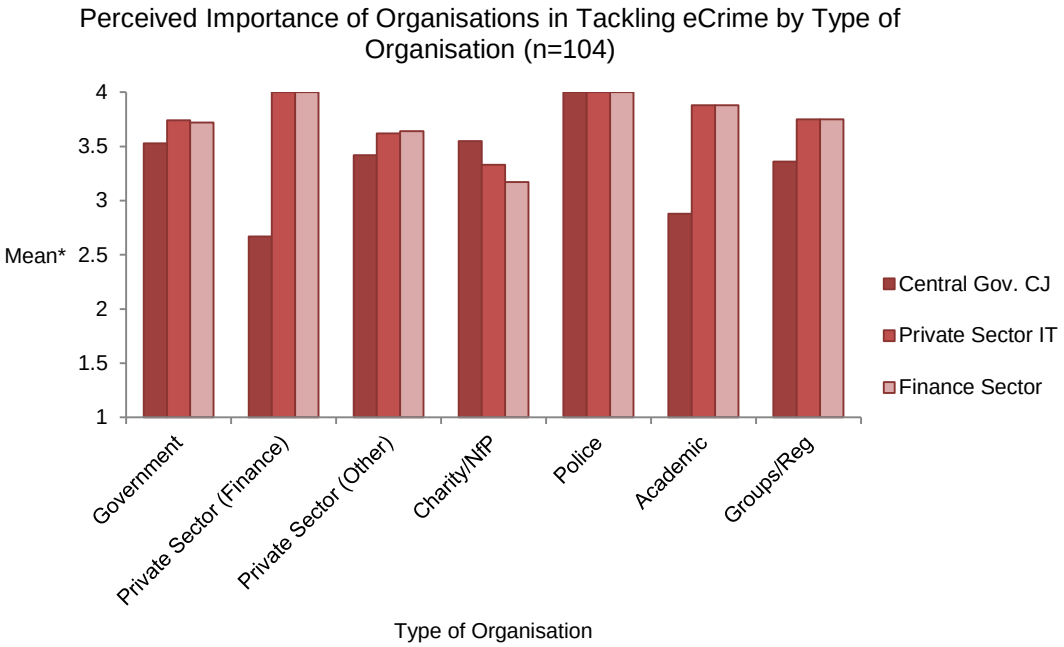


Chart 5.1

[34] In this section of the survey we separated perceived 'importance', 'expected responsibility' and 'effectiveness' providing three measures of perception of other organisations in their battle against the eCrime problem. Each measure can be interpreted independently.

Chart 5.2 provides a more detailed view of perceived importance of the top three by type of organisation. The police and government organisations are around one and a half times more likely to rate central government (criminal justice related) departments as important compared to the finance sector, which rates them the least important out of all responding organisations. Both the finance sector and the police are most likely to rate the private sector (IT) as most important, while charities/NfPs are least likely.

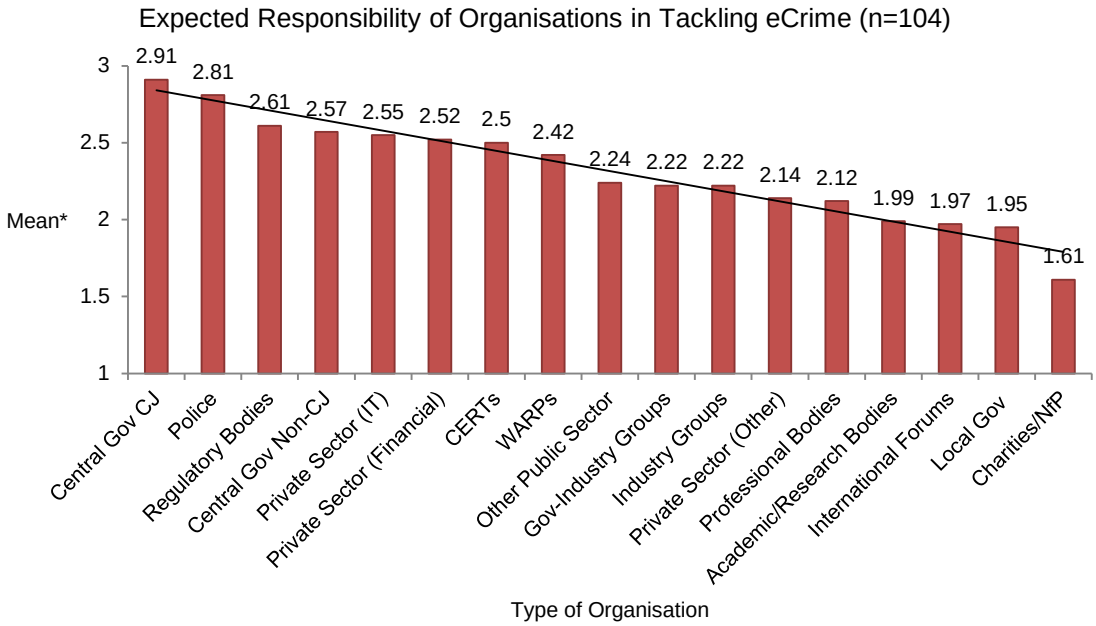


*(1=Unimportant; 2=Quite Unimportant; 3=Quite Important; 4=Important)

Chart 5.2

Expected Responsibility of Organisations in Tackling eCrimes

The survey also asked respondents which UKIA organisations should have the most responsibility for tackling the eCrime problem (where 1=low responsibility through 3=high responsibility). These data are potentially of relevance to the establishment of the public/private information sharing 'hub' as detailed in the recent UK Cyber Security Strategy (Cabinet Office, 2011), insofar as they reflect the expectations of the UKIA community in relation to organisational responsibility. Chart 5.3 shows that the majority of organisations indicate that central government (criminal justice related) departments should have the highest level of responsibility. Contrastingly, the private sector (finance and IT) who placed top in terms of perceived importance are replaced a by police, regulatory bodies and central government (non- criminal justice related) in terms of expected responsibility. However, there is little change at the bottom of the scale where the perceived importance of organisations and their expected responsibility remain relatively symmetrical. Note that private sector (other) has dropped from seventh position in terms of perceived importance to twelfth position in terms of expected responsibility. Given that two thirds of private sector (other) organisations in our sample identified as SMEs it is important to ensure their representation in an eCrime Reduction Partnership scheme, irrespective of these perceptions.



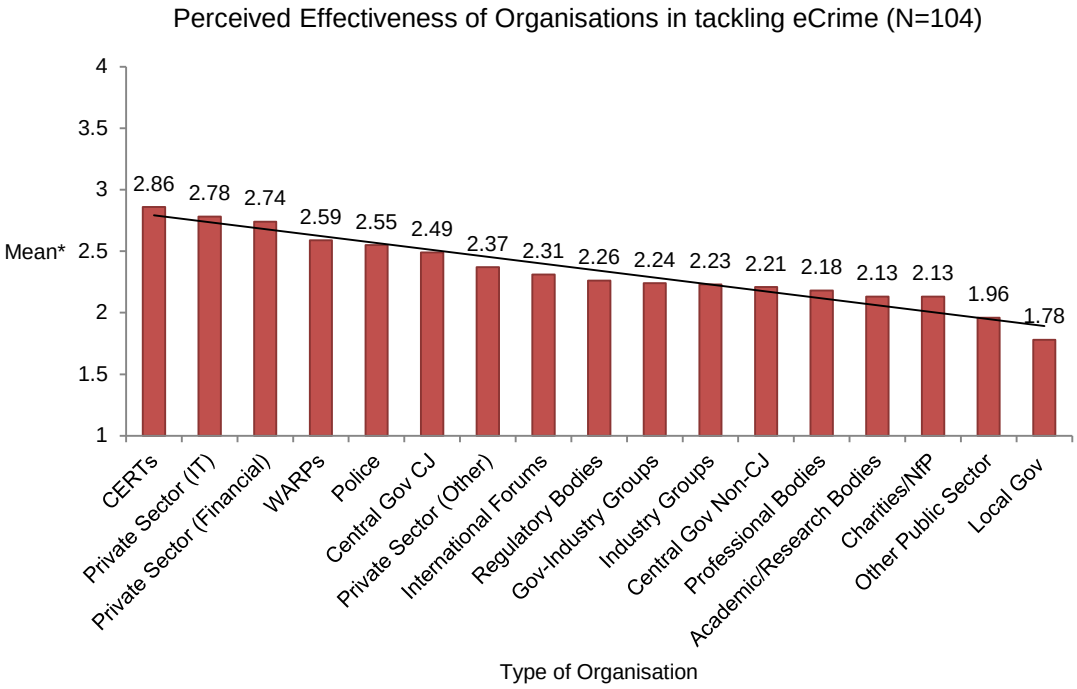
*(1=Low; 2=Moderate; 3=High)

Chart 5.3

Perceived Effectiveness of Organisations in Tackling eCrimes

The final question on perceptions of UKIA organisations asked about the perceived effectiveness of organisations in tackling eCrimes (where 1=ineffective through 4=effective). Chart 5.4 shows those organisations perceived as most effective to least. Perceived as most effective in tackling eCrime are CERTs[35], the private sector (finance and IT) and WARPs[36], while charities/NfPs, public sector (other) and local government emerge as least effective. Again it is important to note the good work of organisations in devolved administrations (eCrime Wales Project) and local government (Yorkshire eCrime Business Centre) which may fail to gain effective national exposure. Comparison with the importance and responsibility scales reveal some interesting asymmetries. While the perceived importance and responsibility of central government (criminal justice related) is high, in terms of perceived effectiveness they place only sixth out of the 17 organisations listed. Private sector (IT) and the finance sector place high in perceived effectiveness as they did in importance and expected responsibility. Again the low end of the effectiveness scale remains relatively symmetrical with the two previous measures, with the exception of private sector (other) placing lower in terms of effectiveness, compared to importance and responsibility. It is interesting to note that very few respondents rate organisations as the maximum score of 'effective'. The mean for the effectiveness scale (2.34) places overall perception just above 'quite ineffective'.

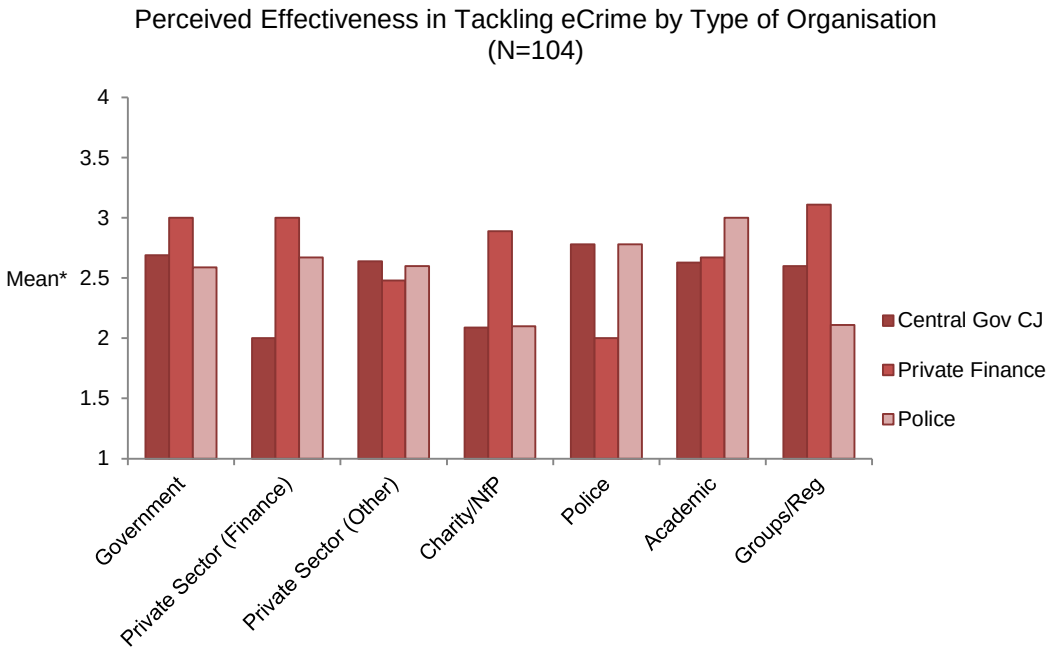
[35] Computer Emergency Response Teams (see: http://www.ukcert.org.uk/)
[36] Warning, Advice and Reporting Points (see: http://www.warp.gov.uk/)



(1=Ineffective; 2=Quite ineffective; 3=Quite effective; 4=Effective)

Chart 5.4

A breakdown of the perceived effectiveness of the police, central government (criminal justice related) and the finance sector is provided in Chart 5.5. Central government (criminal just related) departments are seen as most effective by the police and least by the finance sector whereas the police are seen as most effective by academics and least by charities/NfPs. However, the most significant difference in perception emerges with the finance sector – groups and regulatory bodies are most likely to perceive finance as effective, while the police rate them least effective out of the responding organisations. As 'effectiveness' was interpreted subjectively by responding organisations it is difficult to tease out the complexities of these perceptions. Further research is needed to understand why the police in this study hold such perceptions in relation to the effectiveness of finance organisations.



*(1=Ineffective; 2=Quite ineffective; 3=Quite effective; 4=Effective)

Chart 5.5

6. Perceptions of Cooperation with the UKIA Community

A key driver for the commissioning of this research was to attain the views of UKIA organisations on the possibility of setting up an eCrime Reduction Partnership. To accomplish this we attempted to measure: i) existing patterns of cooperation; ii) the perceived quality of that cooperation; iii) the desire for future cooperation; iv) desired aids to eCrime reduction; and lastly v) perceived national and international barriers to cooperation. These data may be useful in informing the key deliverables around establishing public/private partnerships as outlined in the UK Cyber Security Strategy.

Two overall scores of cooperation were compiled: ***subjective*** and ***target***. *Subjective* scores were compiled from organisations' ***self*** perceptions of cooperation frequency and quality i.e. who the respondent from the organisation thought they cooperated with, how often and how well. *Target* scores were compiled by taking the mean of cooperation and quality scores across responding organisations e.g. the target cooperation scale allows us to create a list of organisations ranging from most cooperated with to least.

Chart 6.1 shows how organisations rated themselves in relation to frequency of cooperation with other UKIA organisations[37]. It is important to stress again that organisations were asked to rate themselves in terms of cooperation with other organisations – making these scores a subjective measure i.e. we did not 'count' the frequency of interaction over time[38]. Respondents were asked to rate their frequency of cooperation on a 4-point scale (where 1=no cooperation through 4=a lot of cooperation). The overall mean of cooperation (2.89) indicates the majority of respondents have 'some cooperation' with other UKIA organisations. This overall mean is a barometer of cooperation meaning an upward trend over time would indicate more cooperation amongst the UKIA community. This measure can be used to partly evaluate the impact the public/private information sharing 'hub', piloted in 2011 by HM Government, will have on the overall cooperation within the UKIA community when rolled out nationally. At senior level, there is already significant interaction between GCHQ and the financial services and other major corporate sectors, but this aims at systematising and formalising these relationships within a trusted community.

The finance sector rate themselves as the most cooperative, followed closely by academic/research institutions and the police. Those perceiving themselves as least cooperative include government, private sector (other), and group/regulatory organisations. However, it is important to note that the low score for government organisations is due to the conflation of central government, other public sector and local government organisations (as can be seen in target cooperation score in chart 6.2).

[37] Of course, our list of cooperatees is not exhaustive, meaning these scores should only be interpreted in relation to the organisations specified.

[38] While this method would produce more reliable results, it is time and resource intensive and beyond the scope of this study.

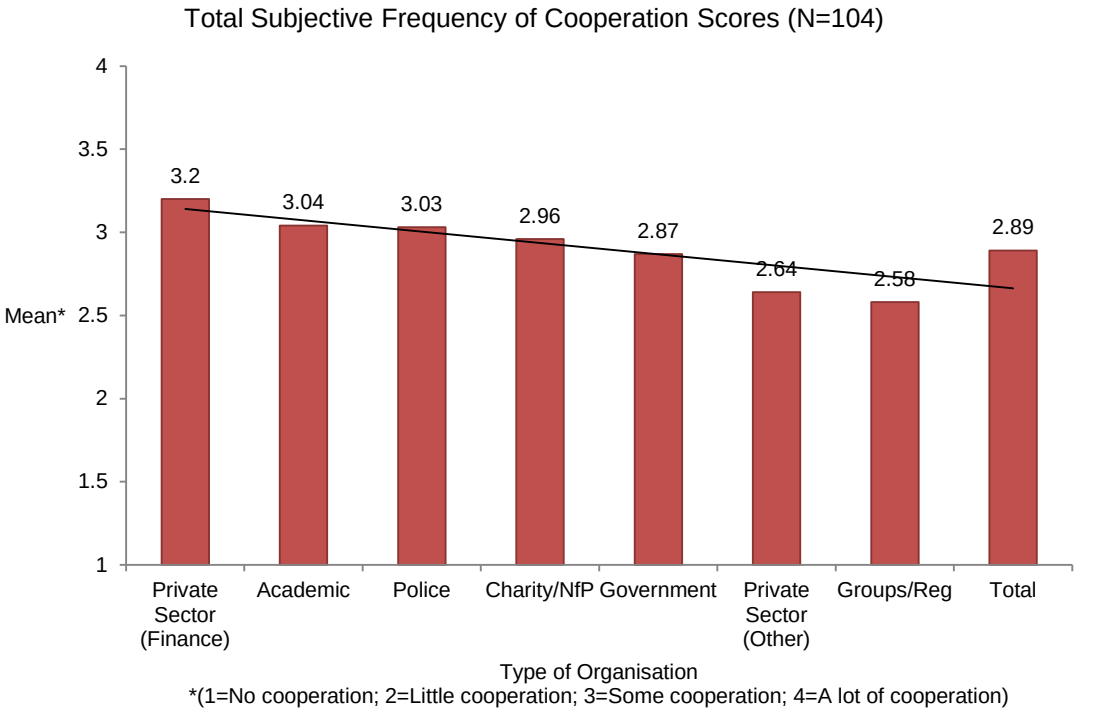


Chart 6.1

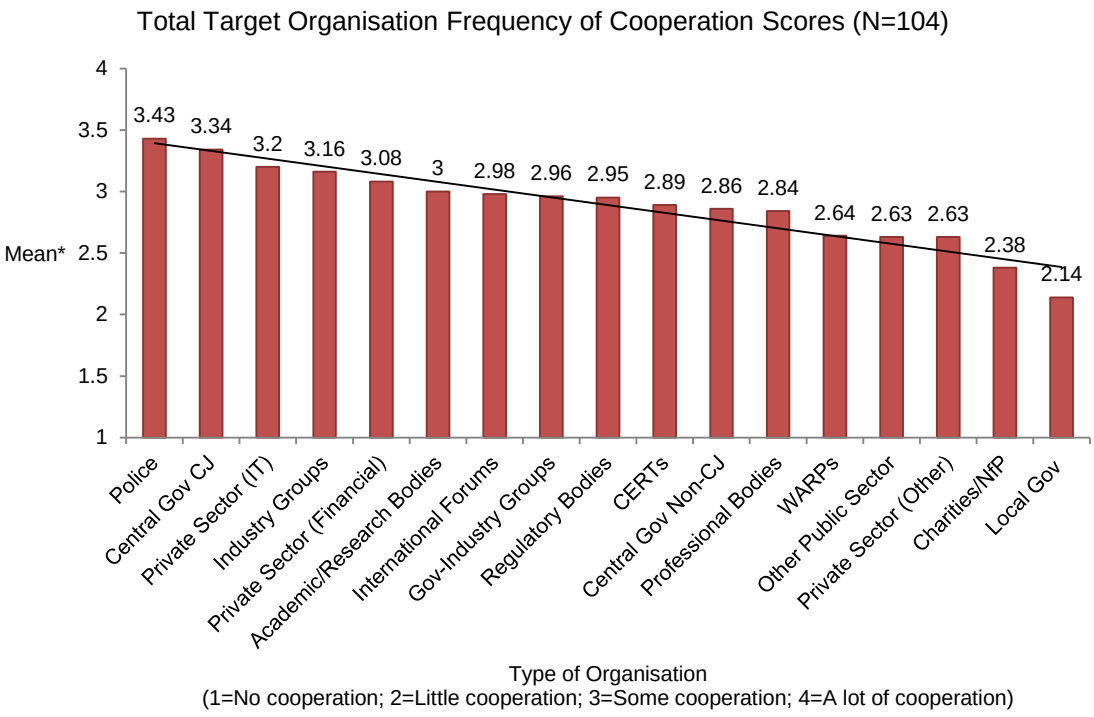


Chart 6.2

Chart 6.2 details the list of organisations targeted for cooperation by frequency of that cooperation. Police, central government (criminal justice related) and private sector (IT) organisations emerge as the most cooperated with. Conversely, private sector (other), charity and local government organisations emerge as the least cooperated with. It is important to note here that central

government (criminal justice related) place second. The subjective measure of cooperation conflated all government organisations, which impacted upon the mean. This is corroborated by central government (non-criminal justice), public sector (other) and local government placing 11th, 14th and 17th respectively on the target scale. It is also important to note that private sector IT and finance organisations place in the top five targeted organisations, yet private sector (other) place third from last.

Chart 6.3 details cooperation as perceived by all responding organisations with the various types of government department. The police, government, group, regulatory and charity/NfP organisations all score highly in terms of cooperation with central government (criminal justice related). Conversely, the private sector (finance and other) claim least cooperation. In relation to central government (non-criminal justice related) departments, the police and government organisations emerge as most cooperative, whereas private sector (other) and academic/research organisations emerge as least cooperative. Finally, the police and government organisations perceive themselves as more cooperative with local government, while the private sector (finance and other) perceive themselves as least cooperative. Overall the police emerge as most consistent in terms of perceived frequency of cooperation with all types of government organisation, whereas private sector (other) organisations perceive themselves as performing least well across the board.

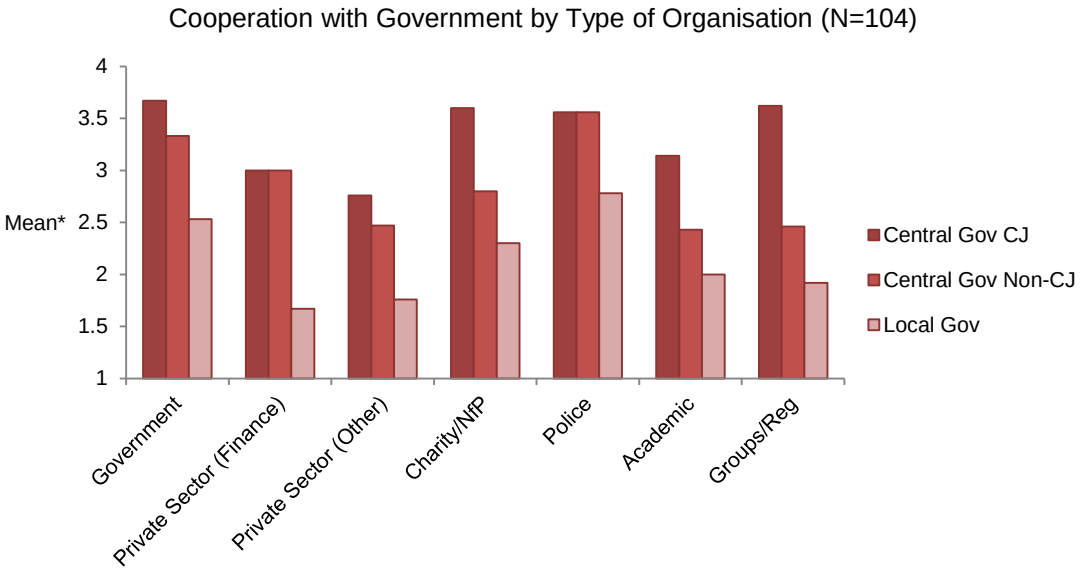


Chart 6.3

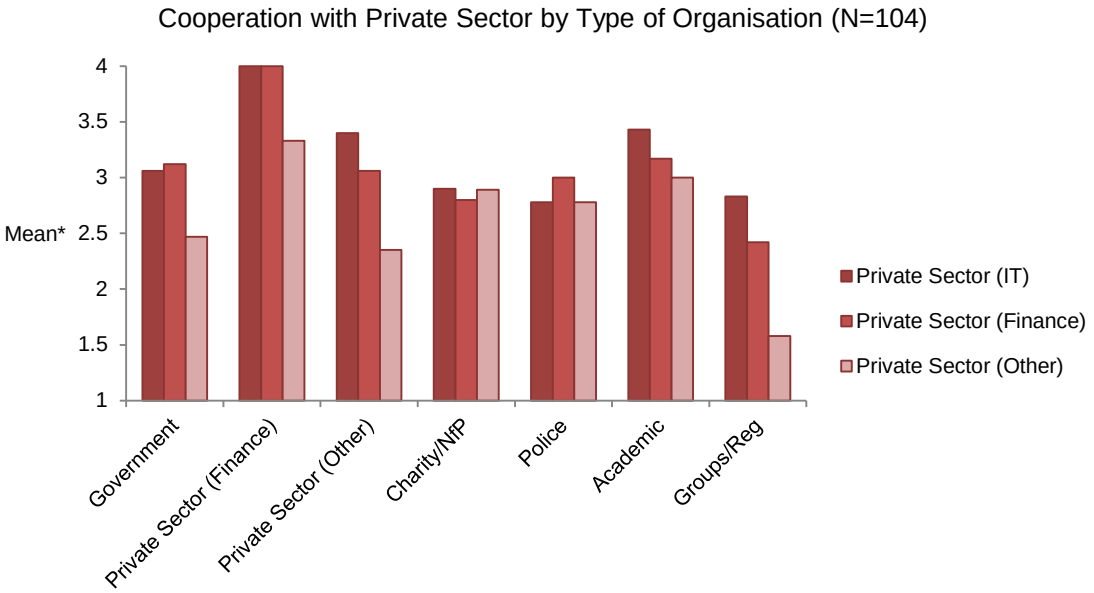


Chart 6.4

Chart 6.4 details type of organisation by cooperation with the private sector. In terms of frequency of cooperation with private sector (IT) organisations, finance, private sector (other) and academic/research organisations emerge as perceiving themselves as most cooperative. Perceiving themselves as least cooperative are charities/NfPs, groups, regulatory bodies and the police. Not surprisingly the finance sector emerged as perceiving themselves as most cooperative with themselves, closely followed by academic/research and government organisations. Charities/NfPs, groups and regulatory bodies emerge as perceiving themselves as least cooperative. Finally, private sector (other) organisations attract most cooperation from finance, academic/research institutions and charities/NfPs. Counter intuitively, private sector (other) emerge as one of the least likely to cooperate with themselves, along with groups and regulatory bodies. The finance sector out-performs all other organisations across the board in relation to perceived cooperation with all types of private sector organisations. Groups and regulatory bodies perceive themselves as performing least well across all private sector organisations. In light of this evidence and the emphasis placed on public/private partnerships in the UK Cyber Security Strategy, it may be prudent to further investigate why some organisations report low levels of cooperation with the private sector in relation to eCrime control.

Perceptions of Cooperation Quality

The second cooperation question asked respondents to rate the perceived quality of cooperation with other organisations on a scale of 1 to 5 (where 1=very poor through 5=very good). Again this is a subjective scale based on respondents' opinions of the quality of their organisation's cooperation. As with the frequency scale, it is important here to note the overall mean as indicated in Chart 6.5 (3.64), showing the majority of respondents rate their quality of cooperation as just below quite good. This overall mean can be used in conjunction with the frequency mean as barometer of quality of cooperation meaning an upward trend over time would indicate higher quality

cooperation amongst the UKIA community. Such measures might be used as part of a baseline against which to evaluate the effectiveness of public/private partnership initiatives stemming from the UK Cyber Security Strategy, though it would be important to be clear about which changes had occurred only after those initiatives.

Academic/research institutions, finance organisations and the police rate themselves as having the highest quality of cooperation. Government, charities/NfPs and private sector (other) organisations self identify as having poorer quality cooperation with the UKIA community. Again however, it is important to note the conflation of all types of government organisation in this score may impact upon the mean for the overall government category.

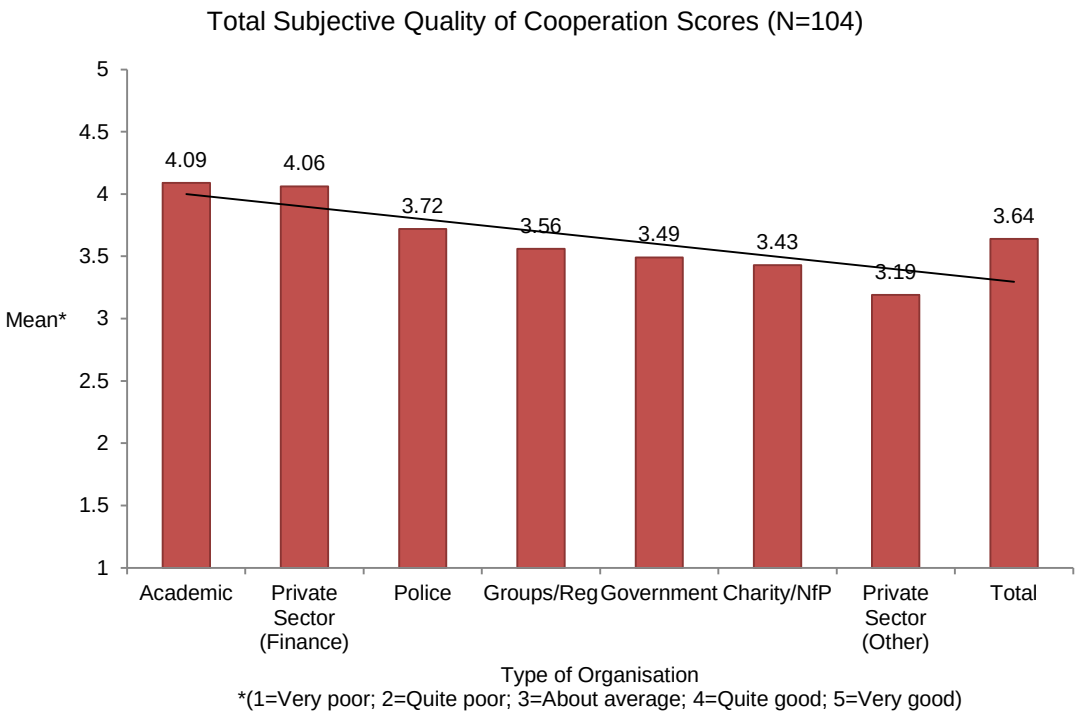
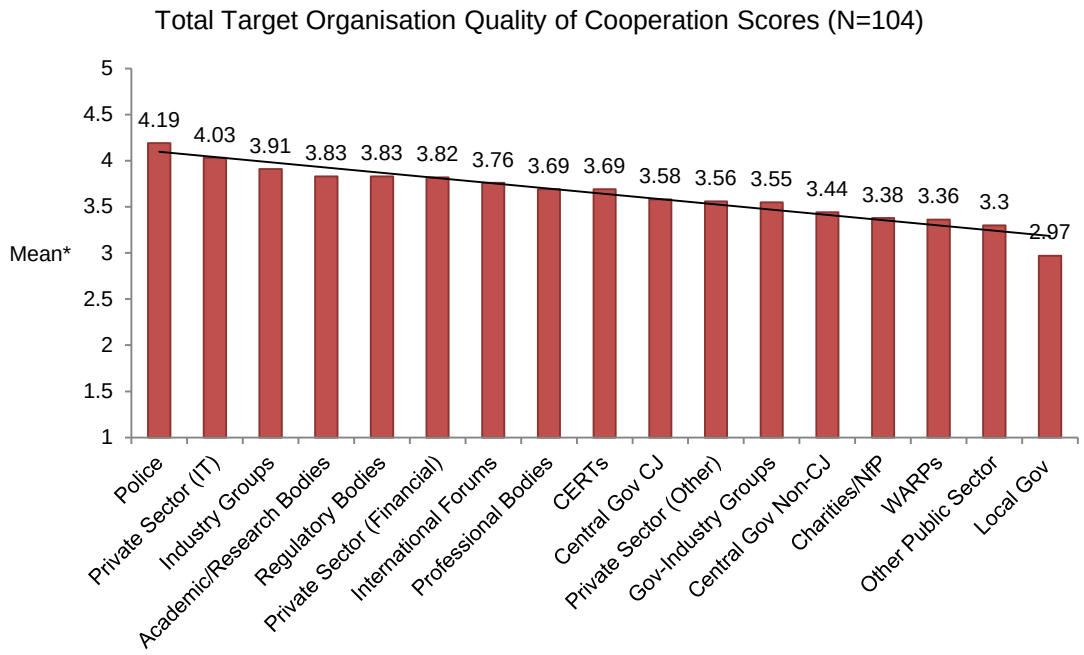


Chart 6.5

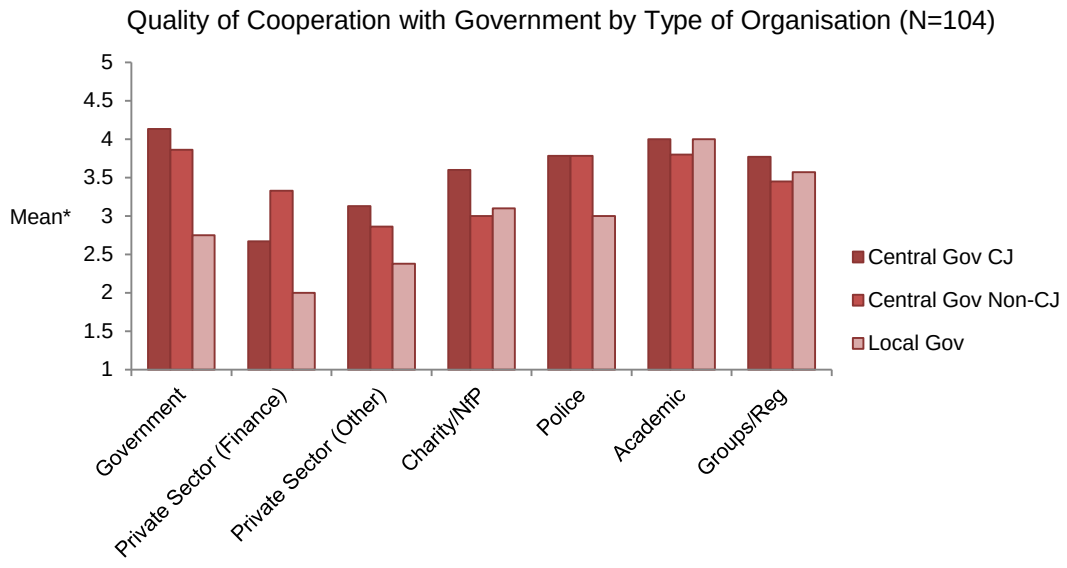
Chart 6.6 details the organisations targeted for cooperation by quality of that cooperation. The police and private security (IT) organisations are identified as delivering the highest quality of cooperation. Local government emerge as having the lowest quality of cooperation by quite some margin. There is asymmetry with respect to the placement of central government (criminal justice related) in this measure of cooperation compared to the measure of frequency. In the target frequency cooperation scale they placed second, while in this target quality of cooperation scale they place 10th out of 17. Both other government organisation categories (non criminal justice and public sector other) also place in the lower half of the scale. This pattern helps corroborate the low placement of the collated government category in the subjective quality of cooperation score. Therefore, it is safe to conclude, both on measures of self-identification and appraisal by external organisations, government departments perform below average on quality of cooperation. It is

perhaps most surprising to see criminal justice related government departments so low on the quality scale, given they placed high on the target frequency of cooperation score. For the remaining organisations there is relative symmetry between the quality and frequency target cooperation scales. It would be prudent to further investigate the reasons for the relatively poor quality of cooperation scores in relation to government departments before the full roll-out of the public/private information sharing 'hub' detailed in the UK Cyber Security Strategy (Cabinet Office, 2011).



*(1=Very poor; 2=Quite poor; 3=About average; 4=Quite good; 5=Very good)

Chart 6.6



*(1=Very poor; 2=Quite poor; 3=About average; 4=Quite good; 5=Very good)

Chart 6.7

Chart 6.7 details quality cooperation as perceived by all responding organisations with government departments. Not surprisingly government organisations score highest in terms of quality of cooperation with central government (criminal justice related) departments. These are followed closely by academic/research institutions, the police, groups and regulatory bodies. Both private sector finance and other have the lowest perceived quality of cooperation with central government (criminal justice related). However, this trend might have changed since the introduction of the public/private information sharing 'hub' pilot, and may be further mitigated once the full roll-out of the 'hub' commences. Those who express highest quality cooperation with non-criminal justice related government departments include government departments, academic/research institutions and the police. Expressions of lower quality cooperation emerge from private sector (other) and charitable organisations. Finally, across the board quality of cooperation with local government is far below average. Those expressing best quality cooperation include academic/research institutions, groups and regulatory bodies, while those indicating poor quality cooperation include private sector finance and other. Overall academic/research institutions emerge as most consistent in terms of quality of cooperation with all types of government organisation, whereas private sector (finance) organisations perform least well across the board.

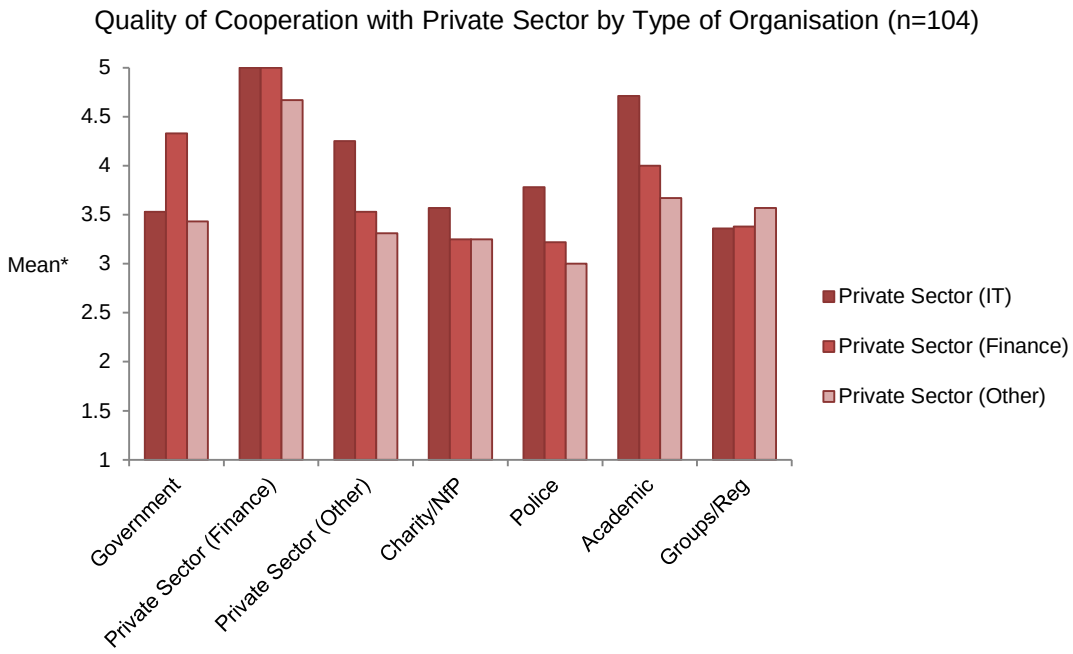


Chart 6.8

Chart 6.8 details type of organisation by quality of cooperation with the private sector. What is first noticeable, in comparison to Chart 6.7 is that the overall pattern of quality of cooperation is much higher. In terms of quality of cooperation with private sector (IT) organisations, finance, academic/research institutions and private sector (other) organisations emerge as the most effective cooperators. Organisations with less effective cooperation are groups, regulatory bodies, charities/NfPs and government departments. Again it is not surprising to find the finance sector emerge as most effective cooperator with themselves, closely followed by academic/research and private sector (other) organisations. The police and charities/NfPs emerge as having the least

quality of cooperation. Finally, private sector (other) organisations attract best quality of cooperation from finance, academic/research institutions, groups and regulatory bodies. Again, counter intuitively private sector (other) emerge as one of the least likely to have good quality cooperation with themselves, along with the police. As with frequency of cooperation, the finance sector out-performs all other organisations across the board in relation to quality of cooperation with all types of private sector organisation. Group and regulatory bodies, charities/NfPs and police perform least well across all private sector organisations.

Wishes for Future Cooperation

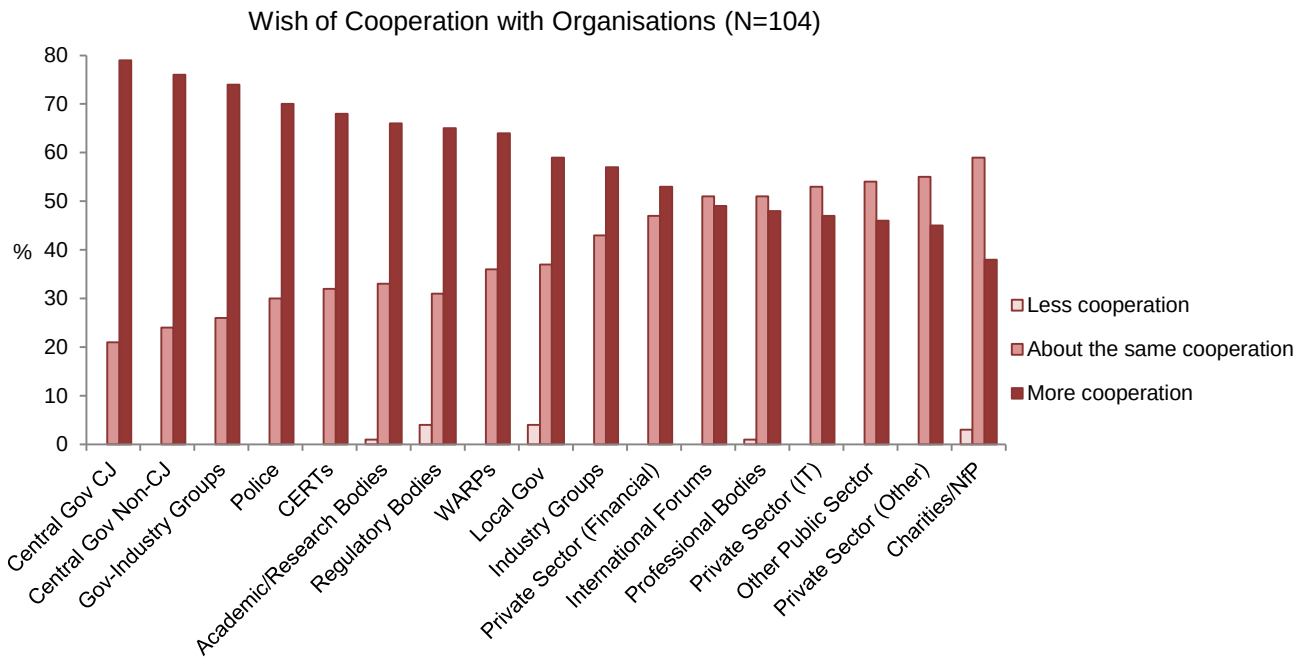


Chart 6.9

Following the questions on cooperation we asked UKIA organisations to indicate their desire to increase, decrease or maintain their existing levels of cooperation with external partners. Chart 6.9 shows that the majority of organisations (just under 80 percent) desire increased cooperation with central government (criminal justice related) departments, followed closely by non-criminal justice related departments, government-industry groups and the police. Public sector (other), private sector (other) and charities/NfPs emerge at the bottom end of the scale. Interestingly, while local government score poorly on all of the previous measures (perceived importance, effectiveness, frequency and quality of cooperation) they emerge mid scale here, above private sector (finance and IT), groups and professional bodies. There is a clear message here that the UKIA community wishes to further engage with this sector of government. This should be reflected in the full roll-out of the public/private information sharing 'hub' outlined in the UK Cyber Security Strategy (Cabinet Office, 2011).

Desired Aids to eCrime Reduction

UKIA organisations were also asked to indicate which aids they needed to better tackle the eCrime problem. Chart 6.10 shows that just under half indicated they need increased cooperation with the UKIA community, followed by an improved knowledge base/more training and increased cooperation with the international IA community. At the bottom end of the scale there is a marked drop in the last two least desired eCrime aids. Just under 10 percent of respondents want more UK legislation, and less than 5 percent desire more effective non-criminal justice reporting mechanisms. Mid scale, just over one third of organisations want more arrests and prosecutions, while just under one third desire more effective criminal justice reporting mechanisms.

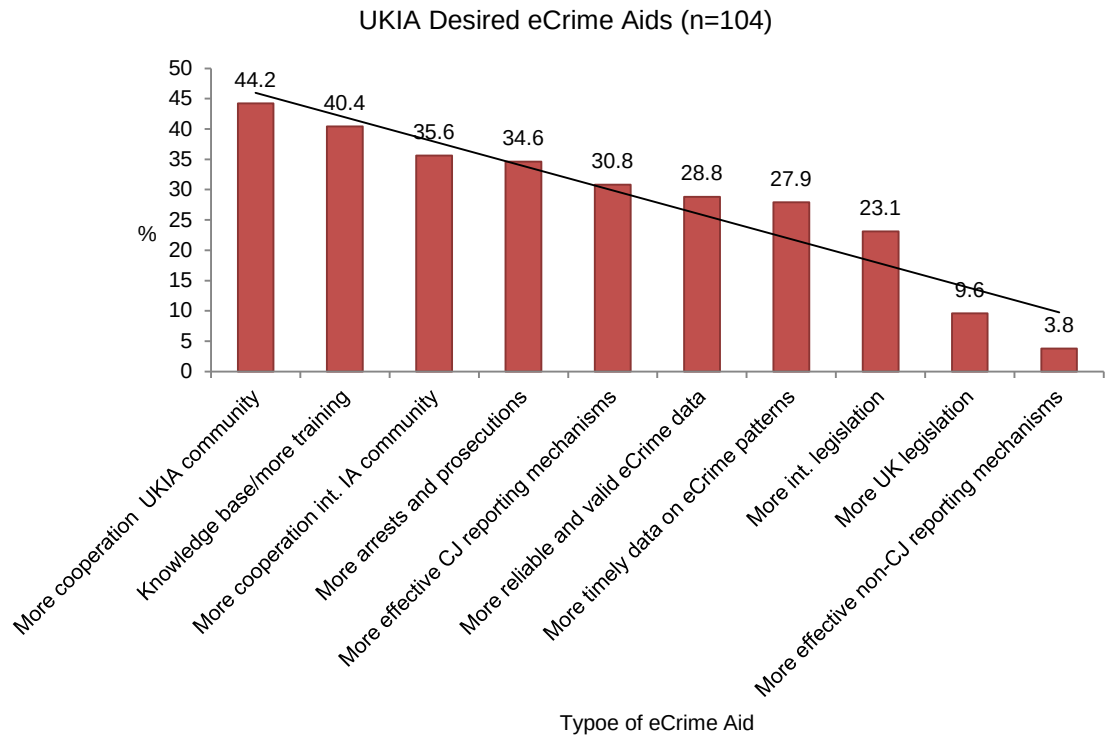


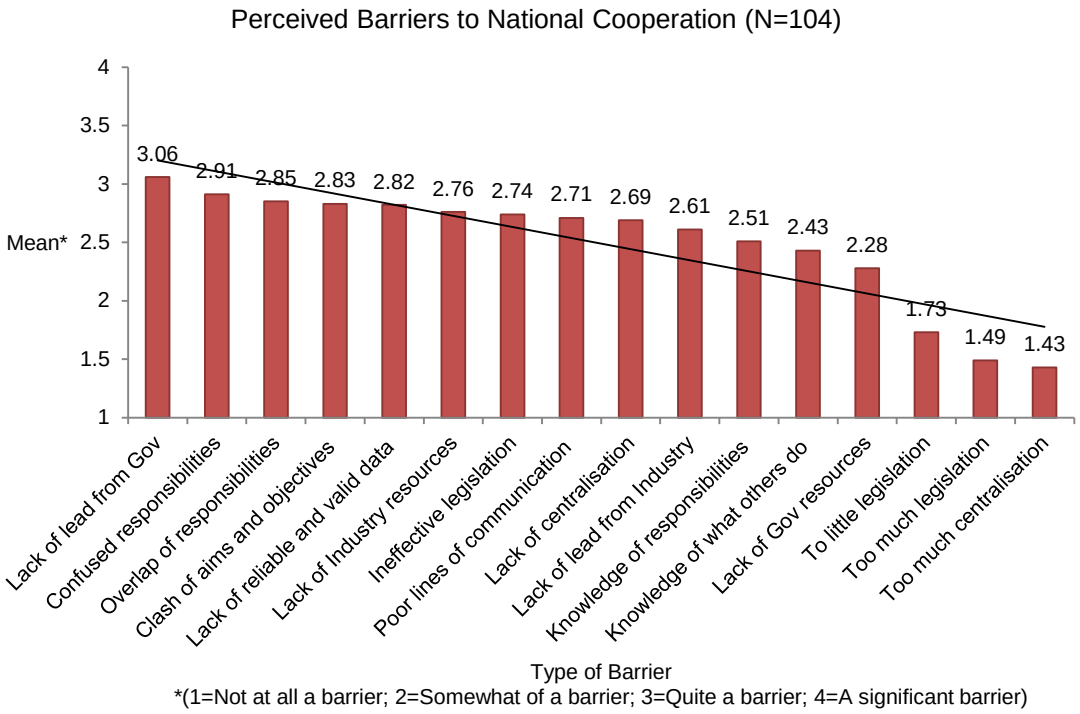
Chart 6.10

Barriers to Cooperation

Perceived National Barriers

The final section of the survey questioned respondents on their perceptions of the national and international barriers to effective UKIA community cooperation. A list of 16 national barriers were listed and respondents were asked to rate each on a scale of 1 to 4 (where 1=not at all a barrier through 4=a significant barrier). Chart 6.11 shows the majority of organisations identify a lack of lead from government as the most significant barrier to cooperation. Confusion and overlap of responsibilities also feature high, along with a clash of aims and objectives with other UKIA organisations and a lack of reliable and valid eCrime data. Poor lines of communication feature half way down scale, but it is important to note the stability of ratings surrounding the mid-point (i.e. there is very little difference in ratings with most at the mid-point resting near 'quite a significant barrier'). A sharp decrease is evident at the end of the scale where respondents indicate legislation

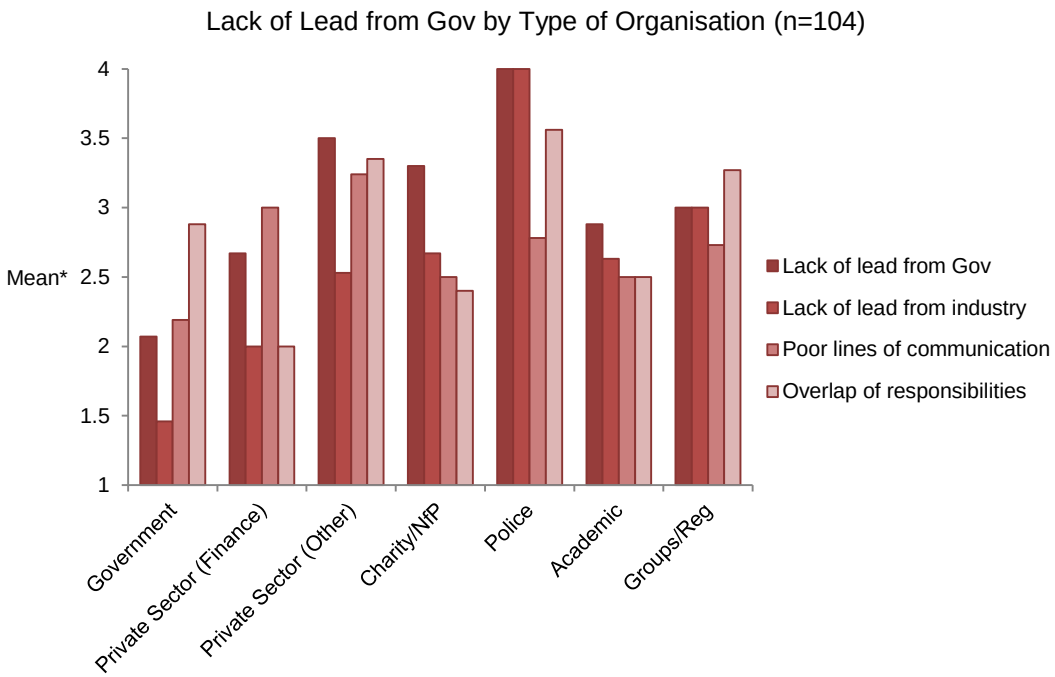
(either too much or too little) and too much centralisation are not significant barriers to effective cooperation.



*(1=Not at all a barrier; 2=Somewhat of a barrier; 3=Quite a barrier; 4=A significant barrier)

Chart 6.11

Chart 6.12 shows divergent opinions between UKIA organisations in relation to four national barriers. The police, private sector (other) and charities/NfPs are most likely to perceive a lack of lead from government as a significant barrier, whereas academic/research institutions, the finance



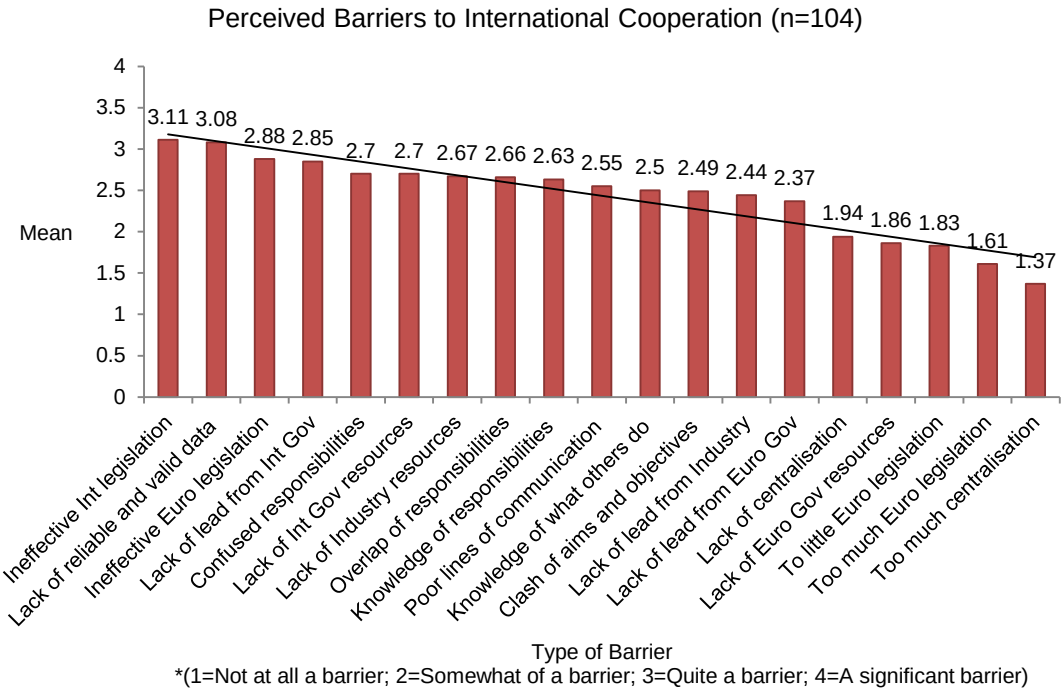
(1=Not at all a barrier; 2=Somewhat of a barrier; 3=Quite a barrier; 4=A significant barrier)

Chart 6.12

sector and the government are least likely. Similarly, the police also emerge as most likely to perceive a lack of lead from industry as a significant barrier along with groups, regulatory bodies and charities/NfPs. The private sector (finance and other) and government organisations are least likely. Poor lines of communication are identified as a significant barrier by both private sector finance and other. Government organisations, charities and regulatory bodies see this as less of a barrier. Lastly, the police and private sector (other) are most likely to see an overlap of responsibilities as a barrier, compared to the finance sector and charities/NfPs. Overall it emerges that the police are most likely to perceive all these factors as barriers, compared to all other organisations.

Perceived International Barriers

Chart 6.13 shows that in terms of *international* cooperation international legislation is identified by respondents as the most significant barrier. This contrasts with national barriers, where ineffective national legislation ranks 7th (a mean of 3.11 compared to 2.74). The top national barriers of lack of lead from government and confused responsibilities are relegated to 4th and 5th respectively in the international scale. Interestingly a lack of reliable and valid eCrimes data features as the second most significant barrier to international cooperation (it places 5th in national cooperation). The bottom end of both national and international scales are more symmetrical, featuring too much centralisation, too much legislation and lack of government resources.



*(1=Not at all a barrier; 2=Somewhat of a barrier; 3=Quite a barrier; 4=A significant barrier)

Chart 6.13

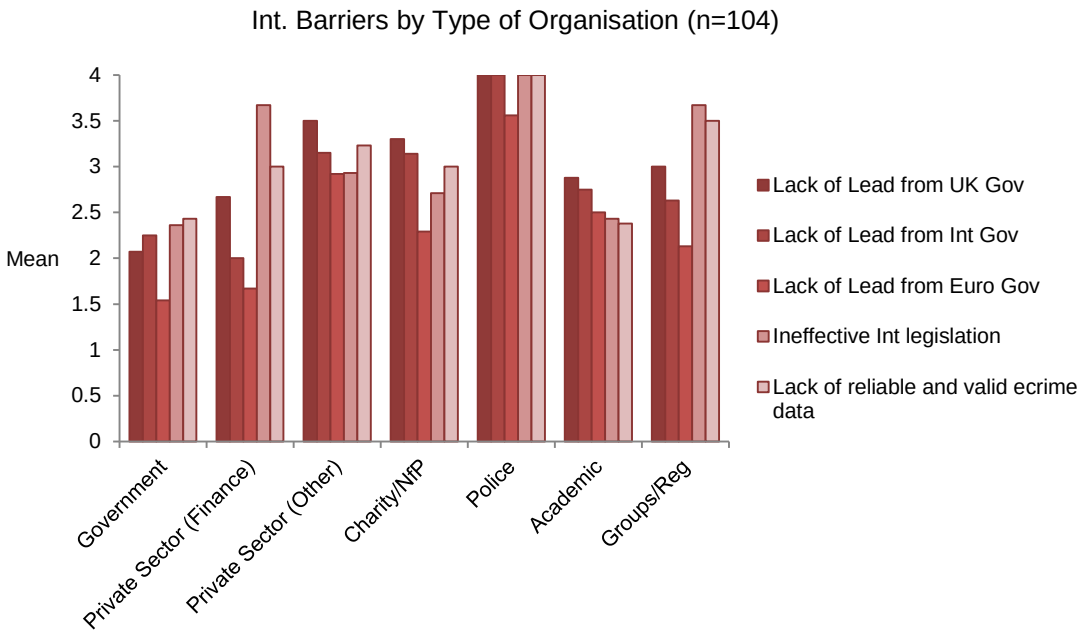


Chart 6.14

Chart 6.14 details the most divergent opinions between UKIA organisations in relation to five international barriers. Again the police emerge as most likely to perceive all these factors as significant barriers compared to all other organisations, whereas government organisations are least likely. The police, private sector (other) organisations and charities/NfPs are significantly more likely to perceive a lack of lead from all types of government (national, European and international) as a barrier as compared to government, private sector (finance) and academic/research organisations. Ineffective international legislation is seen as the most significant barrier by groups, regulatory bodies, public sector (finance) organisations and the police. In comparison academics and government are more likely of see this as less of a barrier. Lastly, the police, groups, regulatory bodies and private sector (other) are significantly more likely than government and academics to see that lack of reliable and valid eCrime data as a significant barrier.

QUALITATIVE FINDINGS

Bolstering and building new operational partnerships between the public and private sectors is at the heart of the UK Cyber Security Strategy (Cabinet Office, 2011). This study asked respondents to comment on the cooperation that currently exists in the UK and to highlight the barriers they perceived to be a significant problem in relation to cooperation in efforts to tackle the eCrime problem. Three themes emerged in the qualitative response around barriers: first, the challenges posed by the internationalisation of the eCrime Problem; second, perceived Government inertia; and third, Ineffective UK criminal justice responses. We stress that these are perceptions and that those managing responses might disagree with them; but they are expert consumer/participant perceptions and therefore should be given some weight as informed rather than as pseudo-opinions. Of course, it can be argued that some of our respondents (for example in the business sector) could and should do more themselves, but one of the benefits of triangulating judgments is that if this is a major issue, others should mention it too.

1. Internationalisation of the eCrime Problem

Several UKIA organisations stress the importance of international cooperation in tackling eCrime, acknowledging the cross-border nature of the problem. Several issues are highlighted, including

- the existence of safe-haven nations that reside outside of the global network of eCrime controllers
- unharmonised substantive and procedural criminal legislation, despite the advances made by the Council of Europe (CoE) Cybercrime Convention (which is available for ratification globally), and
- the increasing internationalisation of most large and some medium sized companies, making their corporate nationality and even 'nations' themselves less self-sufficient in the global fight against eCrime.

Alongside other corporate crime issues such as counterfeiting and piracy, this creates resource and powers difficulties for the police and even for use of civil law:

> 1.1 "Largely the comms lines are very good and within the international space there is significant and quality outreach. There do however remain hard to reach countries or countries that have little or no capability where Cybercrime can flourish. Despite the Budapest Convention, there remains a desperate need to harmonise international legislation, recognise the unique and fleeting nature of web based comms and ensure that investigators have 21st century legal tools that enable fast lawful police-to-police enquiries to facilitate the capture of evidence and intelligence and to minimise the ability for states to become safe harbours."
>
> Central Government – Criminal Justice

> 1.2 "The legislation exists but when dealing with cross border issues with a country who does not share our resources or values, this makes life tricky."
>
> Local Government

1.3 "...the eCrime problem is a global one, while at the same time major international trading organisations (such as Amazon) and service organisations (such as Symantec at one level and mobile phone operators at another level) now operate on the global scene, all of them seeing individual countries as increasingly irrelevant."

Private Sector - Other

1.4 "eCrime measurement, legislation and how eCrime is dealt with on an international basis needs to be more detailed and countries need to work more collaboratively. This is one of the biggest fields of crime and is only going to grow. Governments should be one step ahead of criminals, rather than always being a few steps behind. The feel of the eCrime arena still tends to be reactive rather than proactive. Much improvement needs to be made."

Charity/NfP

1.5 "Law enforcement need to get involved more with international standard setting bodies, but there is not enough widespread interest from either side."

Law Enforcement

However, some respondents stress the need to remain focused on domestic and European issues before tackling the international dimension of eCrime control. In particular, concern is expressed over the 'multitude' of UKIA organisations involved in eCrime control and the challenges presented by Europe-centric solutions:

1.6 "We need to sort our own house out before resolving any wider, international based concerns. The multitude of bodies involved is inexcusable given the austere times. At last count there were over 100 bodies with an "interest" in all things security and thus there are ultimately too many cooks. So most people end up paralysed by the volume of noise and choice and very little actual useful action gets followed through. The level of progress in the last decade, given the volume of available material, is pretty shocking. The two do not correlate."

Private Sector - Other

1.7 "UK needs to sort out its needs and legislation and implement these effectively, it is then an international problem not a purely European one, and trying to do things on a European basis is irrelevant and possibly harmful as European norms and cultures may lead us to the wrong international solutions."

Charity/NfP

1.8 "Getting the correct balance between international - regional and national regulation is always going to be a challenge. However a great deal of what appears to come from the EU does little to enhance the fight against e-crime and more to put ticks in boxes."

Group/Regulatory Body

2. Government Inertia & Criminal Justice Response

Respondents also identify lack of government lead and inadequate resources as barriers in their comments. In particular a lack of understanding of the eCrime problem within the policy arena and beyond has resulted in inadequate levels of education, training and resource allocation, and a lack of expansion in key areas of eFraud prevention and victim support:

> 2.1 "There is such a fundamental lack of priority, education and resources towards e-crime. Government has waited too late to take action. There simply aren't enough individuals with authority that understand e-crime so they tend to avoid addressing it. There is a complete lack of strategy, help for consumers in this area. The NFA, Consumer Direct etc. provide superficial answers often leaving victims at risk of other crime. The legislation is in place but there is an unwillingness to prosecute unless it is a multi-million fraud. Other non-financial crimes such as stalking, harassment are mostly ignored."
>
> Charity/NfP

> 2.2 "The key to this issue is not arrests and prosecution as much of it is globally-based and therefore not amenable to UK CJ resolution, but more importantly is the need to be proactive and preventative, NOT reactive and CJ centred. The lack of accurate and timely information, and the failure of the UK and other governments to get clarity about central agencies to deal, not allowing them to interact, and denying them the resources they need has led to a critical situation that is getting worse."
>
> Private Sector - Other

> 2.3 "Lack of support by government and others for the nine regional Fraud Forums and the National Fraud Forum, both financially and in terms of supporting their development and expansion."
>
> Charity/NfP

> 2.4 "Lack of financial support in the creation of the National Fraud Desk, National Fraud Intelligence Bureau and "Action Fraud". Financial Sector's determination to keep the scale and types of problem hidden."
>
> Charity/NfP

Similar comments are expressed in relation to the criminal justice system. Again barriers centre on a lack of knowledge on the part of law enforcement, and a lack of political support from senior criminal justice organisations:

> 2.5 "To be honest it is my view that the majority of UK bodies, in particular law enforcement know little of the eCrime problem. Law enforcement is completely ineffective in this sector and there is a lack of any effective regulation. This has resulted in a massive gap between central Government policy and most industry sectors."
>
> Private Sector - Other

2.6 "Lack of ACPO support to address the level of fraud perpetrated utilising e-crime methods and a failure to recognise the emerging threat the internet poses."

Law Enforcement

2.7 "One big problem facing policing is uncertainty about the relationship between eCrime and economic crime. Other than some porn networks, all their work is 'economic crime', and although police are constantly told that cyber 'underpins' all areas, it is not obvious what that means in practice." Law Enforcement

Problems were also identified in relation to the 'localism agenda'. For example, the Office of Fair Trading currently deals with internet scam cases in relation to its role in reducing consumer detriment. As this role is devolved to local Trading Standards offices, although there is a national responsibility co-ordinating e-fraud office with laboratory in Yorkshire, the question remains over how well linked this will be internationally and nationally to law enforcement. This is a public-facing function and there is a risk of greater 'market failure' in consumer protection.

One commonly identified judgment was that a police response to many cyber attacks was not feasible, though there would have to be a greater increase in cyber skills in general policing if the 'e' component of crimes was to be coped with, as well as some reallocation of staff to cyber policing, both in headquarters and local agencies. We did not attempt any benchmarking of the UK against other countries, but some respondents made some interesting comparisons:

2.8 "The most noteworthy distinction between UK and US law enforcement practice is the far greater coherence and centralization/consolidation of functions in the UK. On e-crime reporting, the UK has Action Fraud; the US has IC3, Consumer Sentinel, and independent channels into the US Secret Service and Postal Inspectorate, and the pooling of data among those disparate sources is highly incomplete and inconsistent. On e-crime investigation, the UK is more centralised also. The biggest advantage of the US is the sheer volume of agents that can be directed at different types of e-crime; but because of FBI prioritisation, a hacking case gets more attention than an internet fraud case."

Law Enforcement

2.9 "Where the US has a distinct advantage is in e-crime prosecution. Every U.S. Attorney's Office has typically at least two Assistant U.S. Attorneys who are designated as Computer Hacking and Intellectual Property (CHIP) Coordinators. Informational and human support, coupled with the "glitz factor" associated with cybercrime, tends to ensure that e-crime gets lots of prosecutorial attention and support, and not just in the biggest cities or districts."

Law Enforcement

Perceptions of an eCrime Reduction Partnership

In February 2011 the Prime Minister met with industry leaders to discuss the threat of eCrime to the UK economy. Out of this emerged a public private partnership approach to the proactive and reactive control of cyber threats. A public/private information sharing 'hub' was established and

piloted in five sectors that will inform a roll-out of a national scheme. Data collected in this study specifically asked UKIA members to outline their thoughts on how eCrime Reduction Partnerships should operate. These data may assist in informing the development of the new Government scheme in 2012. Several themes emerge from the qualitative data: i) Information Sharing; ii) Engagement with the Private Sector; iii) Clear roles and responsibilities; iv) Resources for effective cooperation; v) Engagement with the public; vi) The international dimension; and vii) Intelligence led. These themes are discussed in more detail below.

3. Information Sharing

The UK Cyber Security Strategy (Cabinet Office, 2011) correctly asserts that information sharing between public and private sectors is imperative to ensuring effective partnerships in the control of eCrime. Most partnership approaches to crime and harm reduction (such Crime and Disorder Reduction Partnerships, Violence Reduction Partnerships[39] and Multi-Agency Risk Assessment Conferences[40]) rely on effective information sharing protocols between member organisations, as well as on informal network relations. This principle is recognised by several respondents in this study. In particular UKIA organisations highlight the importance of joined-up sharing of information, the utility of confidentiality agreements, and a reasonable degree of symmetry in data sharing—all of which are necessary for effective cooperation and which, through diffusion of benefits, will assist in building a better picture of eCrime:

> 3.1 "Enforcement agencies completely joined up sharing information as far as reasonably practicable. A clear line of sight as to which organisation can and will do what. Industry prepared to do all in their gift to protect the public."
>
> Government – Non Criminal Justice

> 3.2 "The problem should be segmented; at a minimum to macro-strategy/micro strategy and also professional activity and public awareness in terms of micro strategy and the financial services, both formal and informal eCrime reduction/information sharing forums already exist and are very effective (the closed door, remote banking eCrime group which operates under the auspices of UK Payments is incredibly effective - in part because membership is limited to 'practitioners' and in part because it operates under confidentiality agreements)."
>
> Private Sector - Finance

> 3.3 "The operational channels should also work both ways. It should not be a case where all information is disseminated downwards; more importantly, information should be passed upwards through the chain too ensuring that the real issues faced on the front line by businesses and individuals are raised to the highest authority. In doing this, crime data is also being gathered to give a more realistic picture of what is going on in the UK, regionally and locally as currently, data about eCrime is very thin on the ground."

---

[39] See Shepherd, J. (2007) *The Cardiff Model - Effective NHS Contributions to Violence Prevention*, Cardiff University. Available here: http://www.alcohollearningcentre.org.uk/_library/projects/files/The_Cardiff_Model_Effective_NHS_Contributions_to_Violence_Prevention_260.pdf

[40] MARACs are most common in the fields of Domestic Violence and Hate Crime prevention and harm reduction.

Charity/NfP

4. Engagement with the Private Sector

Crime reduction partnerships draw their membership from a variety of sectors. Depending on the remit of the partnership these can include criminal justice, voluntary, health, education, local government and in some cases private sector organisations. Unlike volume 'terrestrial' crimes, eCrimes have a disproportionate impact on businesses and can stifle economic growth if left unchecked. Therefore, private sector involvement in an eCrime reduction initiative is imperative to ensure effective data sharing, and up-to-date information on threats and cutting-edge eCrime control mechanisms. Respondents in this study are conscious of the need to involve the private sector in an eCrime reduction partnership and outline several requirements in their comments. Many note that the partnership must engage with SMEs, moving beyond the mere rhetoric, operating with a federated structure that focuses on the variety of needs from small to large organisations. This includes work on metrics of demonstrating levels of harm and levels of harm reduction, such as funds in bank accounts that were at risk of being compromised. Further comments outline the desire for more effective government-industry partnerships unhindered by legislation, and a need for board level involvement:

> 4.1 "From an industry perspective, we should look at providing a risk management strategy for SMEs - otherwise e-crime will be a barrier to investment in these companies and will stagnate the economy. There are too many organisations looking at, and dealing with e-crime - and this only provides confusion and uncertainty. SME outreach has been neglected for well over a decade, despite the rhetoric, and there is little follow-up on guidance. Frankly, I lose patience with decision-makers who take years to make decisions. The electronic economy requires us to make fast decisions as the law NEVER catches up with reality."
>
> Private Sector - Other

> 4.2 "There is still a lack of awareness amongst the private sector and individuals about the threat posed to them, and how they can best protect themselves. This is especially the case with regards to SMEs and individuals. Large and medium-sized organisations are more aware of the threat and they have a greater ability to employ technically-mined people to ensure their systems are adequately protected. A key part of the public sector's focus on fraud is the 'cyber dimension' which is being built into forthcoming online service delivery programmes. However, the threat is ever-changing thus constant vigilance is necessary."
>
> Law Enforcement

> 4.3 "Difficulties getting SME's to join and engage as well as our ability to deliver the right product to them."
>
> Charity/NfP

> 4.4 "Government agencies should aim to partner with private industry more. But, legislation inhibits this." Government – Criminal Justice

4.5 "Balance between public, private and civil sectors, perhaps with sub groups depending on theme or role (e.g. suppliers, victims, etc.). Should aim to reduce duplication and fracturing between actors in this space - no point in setting up something that cuts across existing work/groups."

Government – Criminal Justice

4.6 "Should have a federated structure as particular industry sectors will have different needs. Needs to link with the very senior level of engagement following the recent No 10 event, otherwise it will become an isolated group of experts without the links to achieve outcomes at board level."

Government – Non Criminal Justice

4.7 "Equal partnership between Government, Law Enforcement and the Private Sector. With an equal responsibility and control."

Charity/NfP

4.8 "Any partnership formed also needs to be 'federated' to allow it to focus on different sections e.g. SMEs versus the large financial institutions."

Law Enforcement

4.9 "There are lots of good things going on. The police and private sector have brought into being an active search mechanism for all data breach cards and card numbers around the world with UK issuers, and repatriate those so that the banks can incorporate the numbers into their risk mitigation models. They are also helping to work out the points of compromise and going to the breach companies – who normally only report breaches once they have board approval to do so – to discuss what should be done about their controls."

Law Enforcement

5. Clear Roles and Responsibilities

Some UKIA organisations express that both roles and responsibilities within their networks of eCrime control need to be better defined and communicated, including the role of government. Some concern is expressed over the suitability of central government to coordinate eCrime control efforts alone, noting how the problem is beyond its limits. This point mirrors the Government's perspective on partnership working as set out in the UK Cyber Security Strategy (Cabinet Office, 2011). It notes that as much of the infrastructure that supports cyberspace is owned and maintained by the private sector, it is business that must take a sizable amount of the responsibility. UKIA members in this study advocate tiered systems that incorporate government, but are not solely dependent on state-led co-ordination. Instead clear roles and responsibilities are proposed at the national and regional level for public, private, criminal justice and voluntary eCrime controllers:

5.1 "My responses are based on a belief that the networks and coordination need to be improved before gaps can be identified. At present, not all organisations are aware of each other's roles, remits, priorities and referral mechanisms. Until this is clear, and effective referral and liaison can take place, I can't comment on whether the legislation is adequate or the response of the criminal justice system is adequate."

Government – Non Criminal Justice

5.2 "There is also a need to emphasise 'prevention' and 'awareness' strategies alongside the law enforcement response. For example on the law enforcement side there is a need for clearer definition of the *roles* of national capabilities and of how they are considered by organisations such as the Police Central E-Crime Unit, the Serious Organised Crime Agency, and - to a lesser extent - the City of London Police."

Law Enforcement

5.3 "In essence I don't believe that this is a problem for 'government' to take a lead on. In my experience government departments are out of touch, and insufficiently dynamic to take a lead in this area, with the exception of enhanced legislation and 'macro strategic' solutions in respect of possible international internet governance. In addition, it is also my experience that there is a lack of co-ordination between government departments 'rushing' to the 'cyber' threat. For example; during a recent conversation with the National Fraud Authority, it was apparent that there was insufficient knowledge of what the private sector was doing or even what other (government) departments were doing. The idea that central government could lead and co-ordinate responses ignores the cultural and other limitations of central government."

Private Sector - Finance

5.3 "There should be a national level membership body, which drops down into regional memberships. The national body should include Government Office for Cyber Security, the Police Central e-Crime Unit, regional e-Crime specialists with additional regional Policing leads for the same regions. Members from other national bodies should also be part of that membership, i.e. Serious Fraud Office, CIFAS, Nominet, etc. Regional bodies should incorporate industry members, in addition to members from all Police forces in a region, local government and technology interest bodies. This is to ensure all eCrime messages are disseminated through both Government/Policing authorities and business support organisations (i.e. regional offices), using relevant skilled people."

Charity/NfP

5.4 "[An eCrime partnership should include] membership from Industry representatives, Law Enforcement, Academic specialists, Central Government, and current initiatives in e-crime prevention and detection. [Any partnership should be] responsible for the support of Digital Britain Strategy. [The partnership should have a] remit to co-ordinate a national response and government/industry funding of appropriate initiatives in e-crime awareness, prevention and detection." Academic/Research Institution

6. Resources for Effective Cooperation

The funding of an eCrime reduction partnership emerges several times in respondents' comments. The message is clear, even if the mechanisms by which it can be achieved are not: adequate funding targeted at priorities is essential to the success of a partnership. In particular, some respondents urge the need for funding to support not-for-profit, academic and civil society groups to get involved in partnerships. Such funds could also be used to support the inclusion of SMEs:

6.1 "This is a perception that much could be achieved to improve effectiveness if the funds were available to support communications and cooperation."

Academic/Research Institution

6.2 "[A partnership should not be] another old boys network. The e-Crime community already suffers from cliques. Membership should be free and include government, business, consumers groups and civil society groups. There needs to be funding for groups such as not-for-profits and academics to attend so that it isn't biased towards large organisations that can afford to fund public policy people."

Charity/NfP

6.3 "A partnership would need to quantify the resources required to address specific aspects of e-crime (perhaps compare to other governments) identify successful approaches from other organisations."

Charity/NfP

6.4 "It needs a great deal of budget and someone to co-ordinate all the groups involved in eCrime to see what is already being done and how it can be improved."

Private Sector - IT

6.5 "Funding needs to be focused on priorities."

Academic/Research Institution

6.6 "We have a Regional Business Crime Reduction Centre (RBCRC) that is fighting to retain European and other funding previously promised, they have already made a significant contribution in delivering training on e-crime to the business sector. This is the ideal construction to provide a public/private partnership to fight all manner of crime types by education and prevention. We work closely with the RBCRC but could with the right support be much more effective."

Charity/NfP

7. Engagement with the public

Education, awareness raising and engagement with the public emerge as priorities for several UKIA organisations. Respondents' acknowledge that the public and in particular employees are often the key weakness in security systems and an eCrime reduction partnership must engage with civic bodies and local government in some form. However, a word of caution is expressed in relation to privacy, echoing the key concern of balancing security with freedom and privacy outlined in the Government UK Cyber Security Strategy (Cabinet Office, 2011):

> 7.1 "I would like to see part of the remit address educating individuals. If individuals are better educated then it would help improve all organisations security as the weakest element of a company's security is employees not understanding risks and how to prevent them."
>
> Charity/NfP

> 7.2 "A compact between Government, Industry, Academia and the Public, all with different but important responsibilities and parts to play. This does need co-ordinating as a one stop shop that should declutter the space, which I know will be confusing to the average member of the public. The work of the National Cyber Security Programme via OSCIA has a vital role in co-ordinating and trying to remove the significant amount of duplication."
>
> Government – Criminal Justice

> 7.3 "Clear governance, working to a common strategy, and overseeing of national e-crime capabilities. The main emphasis needs to be on awareness, education, and self-protection with a concerted effort to design-out emerging risks to new IT systems. The approach going forward should aim to be balanced between prevention, disruption and enforcement."
>
> Law Enforcement

> 7.4 "From our point of view an e-crime Reduction Partnership would need a strong element of privacy expertise because there is a fine line between e-crime prevention and mass-surveillance. Public sensitivity is also very high in this area."
>
> Group/Regulatory Body

8. International Dimension

Most crime reduction partnerships are national in scope. Thus, for example, The Anti-Phishing Working Group (APWG) and National Cyber Security Alliance (NCSA) led the development of the STOP. THINK. CONNECT. Campaign in the US, to which was added the U.S. Department of Homeland Security, which provides the Federal Government's leadership for the campaign. This is aimed at Americans but, like other things available on the Internet, it can be accessed globally (http://stopthinkconnect.org/). The UK Cyber Security Strategy acknowledges the transnational dimension of eCrimes and sets out a road map for partnerships with overseas Governments, in part to help shape an international consensus on 'norms of behaviour' in cyberspace. The UKIA organisations that took part in this study also recognise the challenges posed by the international

dimension of eCrime and note how a UK based eCrime Reduction Partnership must address concerns beyond national boundaries and engage with partners in Europe and beyond. Respondents also stress the need for local and national organisation, with clear links and communication channels with international partners:

> 8.1 "[The] responsibility [of an eCrime reduction partnership] should be to increase international co-operation."
>
> Charity/NfP

> 8.2 "[an eCrime reduction partnership should] Initially [be organised] on a community basis and then on a national basis and finally internationally."
>
> Charity/NfP

> 8.3 "It should be a multi-stakeholder, international partnership with clear lines of command down to local community partnership level. It ought to prioritise and categorise eCrime according to seriousness - perhaps evaluating political, economic, social, technological and environmental impacts. A risk-based approach will help to deliver education and training at multi-levels amongst key stakeholders."
>
> Private Sector - Other

> 8.4 "If it isn't international, it will hardly matter."
>
> Academic/Research Institution

9. Intelligence Led

The UK Cyber Security Strategy (Cabinet Office, 2011) places emphasis on intelligence gathering and sharing between government departments, and the private, voluntary and academic sectors. Many respondents in this study voice the need for an eCrime reduction partnership to be intelligence-led. Specifically UKIA organisations indicated that it would be important for the partnership to function as a forum to receive, discuss and action the most up-to-date information regarding current and emerging threats (as the National Fraud Intelligence Bureau aims to do *operationally* for fraud generally). To this end the partnership must be supported by intelligence and analysis from all members, including inter-disciplinary academic contributions (social sciences, as well as computer sciences and informatics). Furthermore, respondents suggest systems should also be put in place to facilitate better data-linking across private business and government/criminal justice systems. This may in part be established by the public/private sector information sharing 'hub' (piloted in defence, finance, telecommunications, pharmaceuticals and energy) outlined in the UK Cyber Security Strategy (Cabinet Office, 2011). The respondents also felt that the partnership should be outcome orientated and engaged in the development of action plans that are measurable:

> 9.1 "The main aim of the partnership should be to bring together all enforcement agencies, industry and the Government in a forum that enables discussion and focus on current and emerging threats. The forum needs to be supported by intelligence analysis and its aim

should be to develop action plans to address priority threats, with industry, Government and enforcement agencies sharing efforts to support an appropriate response to the threat. The emphasis should be on targeting existing effort in a more coordinated and intelligence-led fashion rather than requiring new capacity to meet these needs. Whilst working in this way, the forum will be able to identify gaps in the response framework and Government should be developing solutions to these gaps where a significant harm could arise."

Government – Non Criminal Justice

9.2 "The expertise of the UK's academic research base should be utilised as far as possible. Partnerships between research organisations, government and industry will be essential if medium to long-term challenges are to be tackled effectively. This requirement extends across the whole research spectrum as the problems faced are complex and unlikely to be solved without inter-academic collaboration."

Government – Non Criminal Justice

9.3 "The trust issue for criminals was solved online because market entrants had to give a sample of their products which would be tested and price depended on the reliability and completeness of the sample. Like a criminal eBay. There was a good international effort with SOCA to disrupt such venue [DarkMarket]. It is a good thing for individuals to try to secure themselves a bit by being less reckless about what they put online about themselves. But botnets are so sophisticated that it is illusory to aim to kill them – the point is to monitor attempts in the zone of experimentation to track their activities. The Home Office has ownership of cyber in formal terms. However no-one has any real oversight or overview of e-issues as a whole, nor any desire for it, as they are trapped in their own silos and ambitions. There will be competition, but we have to find ways of sharing."

Law Enforcement

9.4 "The main challenge in this area is linking data on criminal attacks against individuals and businesses on one hand, and Government systems on the other. A significant amount of E-Crime is fraud-orientated therefore the National Fraud Authority (through the National Fraud Intelligence Bureau and Action Fraud) are working to enhance intelligence capabilities through better channels of reporting. Reporting channels for individuals and businesses do exist, and thus we need to ensure they are kept up-to-date to enable efficient collection of cyber crime data."

Government Criminal Justice

9.5 "Any partnership formed needs to be closely linked into intelligence gathering, law enforcement, and prevention agencies. It should have clear objectives (which are measurable and which the partnership itself is responsible for measuring / reporting progress) to avoid being a 'talking shop'." Law Enforcement

CONCLUDING REMARKS

The National Statistician (2010) was very critical of the Home Office for its failure to address statistics on fraud in general and eCrimes in particular. In our view, attempts to measure *all* cybercrimes and their costs *precisely* are doomed to failure. However, better statistics than we have at present on their costs and impact to individuals, businesses of different types, and government are important and are possible. In addition to their inherent value in helping us understand the risks that we face, these data would help us to more rationally direct our prevention efforts and assess their impact. This assessment is much more difficult where estimates are speculative, because if the estimates fall or rise, we seldom know whether this is due to measurement error or to real changes in the phenomenon. However for some components that are inherently difficult to define and identify as eCrime, and/or where the survey instruments do not exist or are distrusted, there will always be an element of uncertainty.

We must therefore work out which areas of cost and impact – forms of eCrime and categories of actual/potential victim - we wish to focus upon, which areas have the greatest risk of 'market failure' in provision for compensation and prevention, and how we are to generate and allocate different forms of resource. Currently, for example, there is no clear methodology which links police interventions to impacts on levels and organisation of crime, so it is hard to assess the impacts of marginal changes in police resource such as staffing of the proposed Cyber Crime Unit within the National Crime Agency. This does not overlook the critical importance of policing to social reassurance and the value of sending signals to the varied sets of offenders in different countries who comprise the overworked and misleading phrase 'the criminal community', which overstates its level of harmony. Analytical problems also arise in measuring the *behavioural* impacts of important practical and reassurance bodies such as GetSafeOnline, which offer not just prevention advice but also a place to which individuals and SMEs can turn for more neutral advice on remediation. The eCrime advice space is a very crowded and perhaps confusing one for the public, as it is difficult for people to assess the absolute and relative validity of competing advice they are offered.

Detailed analysis helps individuals, firms, industry bodies and government to work out where the market for security needs supplementing, both for prevention and for after-the-fact civil and criminal investigation, including technical recovery. We have left out Critical National Infrastructure issues from our work because these are already prioritised in the National Security Strategy and the Cyber Security Strategy, though the operationalization of these high level aims remains a large problem.

We should aim to look at eCrimes as a whole, not least to discover where provision is weak, but we also must break them up into sub-categories in order to provide a sensible focus for intervention in the 'here and now' as well as in the longer run. To take an analogy from fraud in general, if the OFT (2006) had not carried out a national representative sample study of scams against individuals, the study of the costs of fraud for ACPO by Levi *et al.* (2007) and its subsequent iterations by the National Fraud Authority's Annual Fraud Indicator would have had little idea of the scale of that area of fraud and there would have been a large blank about frauds of great social significance to ordinary people, perhaps especially to the retired and/or socially vulnerable people targeted by

scammers.[41] All we could have done was to point it up as a 'known unknown', in the estimable typology of Donald Rumsfeld. We therefore welcome the broad approach taken by Detica and Cabinet Office (2011) to eCrimes, even though some components of their work are speculative, and their focus on economic cost alone leaves out the 'affordability to recover' component which is an important dimension of harm and impact analysis for crime generally.

One of our objectives was to examine if we could generate an analysis of cybercrime risks and costs analogous to that done for violent and household crimes (Dubourg et al., 2005) and some other forms of crime (van Dijk et al, 2007; DoJNI, 2010; Levi et al., 2007). This is overambitious for most parts of the eCrime spectrum in the light of our present published knowledge (see Anderson et al., 2012). Furthermore, the geography of the victim-offender relationship in online crime is radically different from that in interpersonal violent crime and household and street crime, where the offender has to be in the same location as the victim and/or their property at the time of offence commission. But just as our micro-knowledge of violent crime has increased in leaps and bounds, so too can our understanding of the different components of eCrime. In particular, detailed understanding of how victimisation *and attempted victimisation* occur is a crucial prelude to enhancing effective intervention, and this needs to be done for multiple categories of victim: individual, business (of varied scale), and other organisations. Data sharing – especially across borders – is currently inhibited by asymmetric data protection regulations in Europe and beyond, and some of our knowledge of threats arises from data integration in software programmes that search for hidden networks behind what might otherwise be viewed as non-criminal commercial losses or disorganised fraud and hackings. But without constructing an over-coherent enemy in the form of hierarchical rather than more flexible 'organised-enough' market models of 'organised crime', co-operation between corporate and individual eCrime victims, and third parties (for profit and not-for-profit) acting on their behalf, has produced and can produce some eCrime reduction. We must then focus on what sorts of eCrimes against what sorts of victims are being reduced, and how the different sub-types might be driven down. As with the reduction of alcohol-related violence and disorder, some interventions can be purely local, while others require more central decisions: however the geographical disintermediation of many e-offenders and e-victims makes this task of eCrimes reduction very much more difficult and complex to negotiate[42].

We cannot but agree with Detica and Cabinet Office (2011: 2), who conclude:

> Although the existence of cyber crime in the UK economy appears endemic, efforts to tackle it seem to be more tactical than strategic. The problem is compounded by the lack of a clear reporting mechanism and the perception that, even if crimes were reported, little can be done. Additional efforts by the Government and businesses to build awareness, share insights and measure cyber crime would allow responses to be targeted more effectively.

[41] For understandable cost reasons, that study has not been replicated in full, and the losses cited are repeated in later national fraud estimates as if they are constant, which seems unlikely.

[42] This is not to underestimate the economic and political difficulties in changing alcohol policy and taxation at a national and transnational level.

REFERENCES

Anderson, R., Boehme, R., Clayton, R., and Moore, T. (2008) *Security Economics and the Internal Market,* ENISA. http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec.

Anderson, R., Barton, C., Boehme, R., Clayton, R., Levi, M., Moore, T. and Savage, S. (2012) *Measuring the Cost of Cybercrime*, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

BAE Systems Detica and the John Grieve Centre for Policing and Community Safety (2012) *Organised Crime in the Digital Age* http://www.baesystemsdetica.com/uploads/resources/ORGANISED_CRIME_IN_THE_DIGITAL_AGE_EXECUTIVE_SUMMARY_FINAL_MARCH_2012.pdf

BitDefender (2011) *H1 2011 E-Threat Landscape Report: MALWARE, SPAM AND PHISHING TRENDS*, http://www.bitdefender.com/media/materials/e-threats/uk/H1_2011_E-Threats_Landscape_Report.pdf

British Retail Consortium (2010) *Future Online Security: Tackling eCrime and Fraud*, London: BRC.

British Retail Consortium (2012) *BRC Retail Crime Survey 2011*, London: BRC.

Cabinet Office (2011) *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, London: Cabinet Office.

Casper, C. (2007), *Examining the Feasibility of a Data Collection Framework*, ENISA.

Chaplin, R., Flatley, J. and Smith, K. (2011) *Crime in England and Wales 2010/11*, London: Home Office.

Cornish, P., Hughes, R. and Livingstone, D. (2009) *Cyberspace and the National Security of the United Kingdom: Threats and Responses,* London: Chatham House.

Cornish, P., Livingstone, D., Clemente, D., and Yorke, C. (2011) *Cyber Security and the UK's Critical National Infrastructure*, London: Chatham House.

CyberSource (2012) Eight *Annual UK Online Fraud Report 2012*, London: CyberSource.

Detica and Cabinet Office (2011) *The Cost of Cyber Crime: A Detica and Cabinet Office Report In Partnership With The Office Of Cyber Security And Information Assurance In The Cabinet Office.* http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf

van Dijk, J. Manchin, R. van Kesteren, J., Hideg, G. with the assistance of Nevala, S. (2007) *The Burden of Crime in the EU: Research Report: A Comparative Analysis of the European Crime and Safety Survey* (EU ICS) 2005, http://www.europeansafetyobservatory.eu/downloads/EUICS%20-%20The%20Burden%20of%20Crime%20in%20the%20EU.pdf

DoJNI (2010) *Cost of Crime in Northern Ireland*, Belfast: Department of Justice Northern Ireland.

Dolan P. and Peasgood, T, (2007), "Estimating the Social Costs of the Fear of Crime, *British Journal of Criminology*, Vol. 47, pp.121-132

Dubourg, R., Hamed, J., & Thorns, J. (2005). *The economic and social costs of crime against individuals and households,* London: Home Office.

Dubourg, R. and Prichard, S. (eds) (2009) *Organised Crime: Revenues, Economic and Social Costs, and Criminal Assets Available for Seizure*. London: Home Office.

Empirica (2007) *Benchmarking in a Policy Perspective: Security and Confidence*, Report No.8, Brussels: Empirica.

Financial Fraud Action UK (2012) *Fraud: the Facts 2012*, London: Financial Fraud Action UK.

Glenny, M. (2011) *DarkMarket*, London: Bodley Head.

HM Government (2011) *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, London: Cabinet Office.

i2010 High Level Group (2006), *Benchmarking Framework*, Brussels: European Commission.

ITFRC (2010) *Identity Theft: The Aftermath 2009*, http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2009_20100520.pdf.

Kanich, C., Chachra, N., McCoy, D., Grier, C., Wang, D., Motoyama, M, Levchenko, K., Savage, S. and Voelker, G. (2011) 'No Plan Survives Contact: Experience with Cybercrime Measurement', http://cseweb.ucsd.edu/~savage/papers/CSET11.pdf.

Kleemans, E. and De Poot, C. (2008) 'Criminal Careers in Organized Crime and Social Opportunity Structure', *European Journal of Criminology*, 5 (1): 69–98.

van Koppen, M., de Poot, C. and Blokland, A. (2010) Comparing Criminal Careers of Organized Crime Offenders and General Offenders, *European Journal of Criminology*, 7(5) 356–374 7.

Langton, L. (2011) *Identity Theft Reported by Households, 2005-2010*, Washington, DC: Bureau of Justice Statistics.

Langton, L. and Planty, M. (2010) *Victims of Identity Theft, 2008*, Washington, DC: Bureau of Justice Statistics.

Levi, M., Burrows, J., Fleming, M. and Hopkins, M. (with the assistance of Matthews, K.) (2007) *The Nature, Extent and Economic Impact of Fraud in the UK.* London: Association of Chief Police Officers.
http://www.cardiff.ac.uk/socsi/resources/ACPO%20final%20nature%20extent%20and%20economic%20impact%20of%20fraud.pdf

National Statistician (2011) *National Statistician's Review of Crime Statistics: England and Wales*, London: Government Statistical Service.

OFT (2006) *Research on impact of mass marketed scams: A summary of research into the impact of scams on UK consumers*, London: Office of Fair Trading. http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft883.pdf

OFT (2009) *Findings from consumer surveys on Internet Shopping: A comparison of pre and post study consumer research*, London: Office of Fair Trading.

PwC (2011a) *Cybercrime, Protecting Against the Growing Threat: Global Economic Crime Survey 2011*, London: PriceWaterhouse Coopers.

PwC (2011b) *Combating Cybercrime to Protect UK Organisations: Global Economic Crime Survey 2011*, London: PriceWaterhouse Coopers.

Funding :

Backing from
nominet trust
www.nominettrust.org.uk

Practical support :

UK
Internet Governance Forum

www.pictfor.org.uk
parliamentary internet communications and technology forum

The Information
Society Alliance
EURIM

nominet®