Home Office

Cyber crime: A review of the evidence

Research Report 75

Chapter 4: Improving the cyber crime evidence base

Dr. Mike McGuire (University of Surrey) and
Samantha Dowling (Home Office Science)

October 2013

Cyber crime: A review of the evidence

Chapter 4: Improving the cyber crime evidence base

Home Office Research Report 75

October 2013

Dr. Mike McGuire (University of Surrey) and Samantha Dowling (Home Office Science)

Acknowledgements

With thanks to: Andy Feist, Angela Scholes, Ian Caplan, Justin Millar, Steve Bond, Jackie Hoare, Jenny Allan, Laura Williams, Amy Everton, Steve Proffitt, John Fowler, David Mair, Clare Sutherland, Magali Barnoux, Mike Warren, Amanda White, Sam Brand, Prof. Majid Yar, Dr.Steve Furnell, Dr. Jo Bryce, Dr Emily Finch and Dr. Tom Holt.

Disclaimer

The views expressed in this report are those of the authors, not necessarily those of the Home Office (nor do they represent Government policy).

Contents

Cyber crime: A review of the evidence
Chapter 4: Improving the cyber crime evidence base

Challenges of the cyber crime evidence base

Cyber crime is a complex issue. Some of the main challenges in improving the understanding of cyber crime are as follows.

- *Lack of recording mechanisms that accurately distinguish between online and offline crime.*
  Police recorded crime does not distinguish between online and offline offences, making it difficult to identify cyber crimes. Police record crime in accordance with the provisions of the Home Office Counting Rules (HOCR), which set out that the crime to be recorded, is determined by the law. Since there is no specific offence (or offences) of cyber crime – aside from those specified in the Computer Misuse Act 1990 – police recorded crime does not generally distinguish between online and offline offences. Whether or not the offence was committed online or offline, is cyber-enabled or cyber-dependent, the offence recorded is on the basis of the offence in law. For example a fraud committed using a computer would usually be recorded as a fraud under police recorded crime.

  Before the roll out of Action Fraud as the national reporting centre for fraud and financially motivated cyber crime, computer misuse and fraud offences were recorded by individual police forces. Action Fraud completed roll out in April 2013 and has since taken responsibility for the recording of all fraud and computer misuse offences. Action Fraud captures reports from public and businesses on these offences and classifies them in a way which allows distinctions to be made between computer misuse, online fraud and offline fraud offences. Action Fraud also assesses them against the provisions of the law and the requirements of HOCR. Where a report falls short of being recorded as a crime under HOCR, Action Fraud has the facility to record it as an incident, for intelligence and information purposes.

- *Under-reporting of cyber crime, from both the public and business; and a lack of awareness that some cyber incidents are actually crimes.*
  Cyber crimes are under-reported; for example, recent findings from the Commercial Victimisation Survey (CVS; Home Office, 2013) suggest that just two per cent of online crime incidents were reported to the police by businesses. This is considerably lower than for other crime types, for example, 100 per cent of vehicle theft incidents and over 80 per cent of burglary with entry incidents were reported to the police in the same survey. Non-reporting of cyber crimes was largely due to incidents being perceived as too trivial and being dealt with in-house (bearing in mind that three-quarters of incidents were related to viruses). There are also likely to be particular concerns from businesses about reputational damage and negative publicity, which prevent reporting (BERR, 2008; Fafinski and Minassian, 2009).

  Earlier findings from the Crime Survey for England and Wales (CSEW 2006/07, see ONS, 2007) reveal a similar picture for members of the public. For example, just 1 per cent of adult internet users who experienced hacking or unauthorised access to their data in the 12 months prior to the survey reported this to the police (ONS, 2007). This compared with 81 per cent who reported a burglary and 55 per cent who reported a robbery. Under-reporting may occur for a number of reasons:
  - perceptions that the police will not/cannot do anything about online crimes;
  - not knowing where to report;
  - reporting to other bodies such as banks or internet service providers;

  - perceptions that cyber crimes are not ‘real’ crimes like, for example, vehicle theft or burglary;
  - victims not realising or perceiving themselves as victims, for example, because a bank has refunded lost money, or being unaware that malware has infected their computer and stolen their personal details; and
  - some victims simply being too embarrassed to come forward, for example, regarding common scams.

- *Inconsistencies in the measurement and definition of cyber crime within the relevant research.*
  Cyber crime data are often categorised and measured in different ways across different sources, with various (or even no) definitions. This limits an ability to apply and compare findings. The multifaceted nature of cyber crime means that there are various units of measurement that could be considered, for example:
  - number of incidents or crimes;
  - levels of ‘harms’ or costs;
  - individual or business victims;
  - private or public sectors; and
  - awareness levels or actual experiences.

  These measures will also differ depending on which form of cyber crime is of most interest. There are particular challenges with industry-based reports for cyber-dependent crimes (see below).

- *Information from industry sources often lacks transparency and comparability.*
  Cyber crime data are dominated by reports from the security industry, for example, anti-virus (AV) providers. Whilst these sources are useful for understanding the nature of threats posed, they should be viewed with caution given the lack of transparency in how AV providers calculate their estimates of infections and attacks – it is often unclear what is being counted and how this has been done. John Viega, Vice-President of the US Perimeter E-Security company, summarises the technical challenges and ways in which industry reports can over-inflate the scale of malware.[1] He concludes that “*the reality is the problem isn’t as big as we think – but we don’t really have a good way of quantifying it”* (Viega, 2012*,* p 15).

  There is also a lack of comparability between reports from different providers. For example, different AV producers/reports may adopt:
  - different names for malware families and the variants or strains of these in their enumerations;
  - different units of measurement, such as unique incidents, whether malware is ‘in the wild’ versus those that are confined to AV laboratories, zero day attacks, detections and removals from AV systems;
  - different geographical and customer base coverage; and
  - largely ill-defined terms (such as ‘attacks’), along with a lack of transparency in how figures are produced and their implications for the wider public.

  Most reports often present an international picture and there is limited evidence about the UK specifically. Furthermore, concerns have also been raised (see Wall, 2007; Fafinksi and Minassian, 2009; Viega, 2012) about the possible vested interests of these companies in selling security products when reporting these figures and the British Society of Computing (BSC) recommended ‘caution’ with use of industry figures (House of Commons Science and Technology Committee, 2012). Viega (2012) suggests that

[1] For example, one ‘core’ piece of malware can show up hundreds of thousands of times in a vendor’s system, and few vendors try to state how many ‘core’ pieces of malware there are a year (Viega suggests thousands not millions).

there is a need to put the *"science back into computer science"* (p 15) and recommends more robust and publicly verifiable experimental approaches and use of statistical methods when testing security features.

- *Few methodologically sound surveys of victims exist.*
  Aside from a few exceptions, for example, the CSEW and the Oxford Internet Institute surveys (see ONS, 2012; Dutton and Blank, 2013), surveys of victims are often based on small, unrepresentative samples, from which inferences to the wider population cannot be made. In some cases the exact survey methodology is also difficult to verify. However, methodologically robust surveys such as the CSEW have other limitations:
  - in terms of the depth and range of questions asked (as cyber questions are just one part of a larger crime survey); and
  - because the incidents reported relate to 'negative online experiences' rather than criminal activity per se (these experiences would often not be classed as 'crimes' under the usual Home Office Counting Rules).

  Surveys of victims more generally will always be limited by individuals *knowing* that they have been victimised and understanding what has happened to them – for example, identifying if they were victim of a phishing attack, a virus or a hack. Distinguishing between these methods of attack and related outcomes such as fraud, is likely to be difficult.

  Surveys of financial loss can be particularly challenging to interpret. As outlined by Florencio and Herley (2011) many of the survey-based estimates of loss that have been undertaken to date face a number of common issues. These include the use of unverified self reports, the inclusion of high-value single outliers, which heavily skew and exaggerate results, and the reliance on a handful of respondents to formulate the majority of the estimate. This can then lead to inappropriate extrapolation of grossed-up findings to the wider population.

- *Cyber crime is global in nature. It is not constrained by national boundaries.*
  Cyber crime offences and their perpetrators may originate outside of the national jurisdiction they impact on. For example, a computer virus may be written in the Far East but cause damage in Europe, or a downloading site may be located in Russia but accessed in the UK. This presents as many problems for accurate measurements of cyber crime as it does for identifying offenders and bringing them to justice – particularly where other jurisdictions have different legislation.

- *Cyber crime can be undertaken on a large scale, potentially resulting in a relationship between victims and offenders that is very different to 'offline' crime.*
  Unlike most traditional crimes, cyber crimes can be undertaken on a large scale and one offender may be linked to a vast number of smaller crimes (for example, a botnet which is able to send out masses of phishing emails). In most of these situations the offender would be perceived as largely anonymous by the victim. Furthermore, when aggregated, these smaller offences may still create a substantial return for the offender. Data collection and recording in this area will therefore face particular challenges in linking together seemingly isolated incidents. Part of the work of the National Fraud Intelligence Bureau seeks to draw together the linkages and commonalities between seemingly isolated incidents into 'packages' of intelligence for local police and other partner agencies to investigate.

Improving the quality and range of cyber crime measures

There are two basic and important measures of interest for cyber crime:

- measurements in terms of its overall *prevalence* or *volume;* and
- measurements in terms of its overall *impact (i.e. harm or cost).*

Improving measurement and recording is critical to understanding whether the scale of cyber crime is increasing or decreasing and how the nature of the problem is evolving over time. Without a better understanding, it is hard to allocate the right resources to different issues and to recognise what is working and what is not. Only when the quality and range of measures for various types of cyber offending are improved, will some of the remaining evidence gaps around the scale and nature of cyber crime begin to be resolved.

There are key questions that need resolving to improve measures of cyber crime.

- What are the priority offences that need to be measured in relation to cyber crime? Considering the wide range of possible offending categories covered by cyber crime, some offence types may be of greater interest or concern than others.
- What are the best and most reliable indicators to use, considering the limited data in this field? How could these indicators be improved?
- Is a general measure for cyber crime – one that serves as a summary indicator for all varieties of cyber offending as whole – appropriate or even desirable? Given the different facets of cyber crime and the challenges within each, a general measure would appear to create some major difficulties.

The introduction of Action Fraud reporting is one key element to improving the understanding of the scale and nature of cyber crime, but other improvements are also needed, including the following.

- *Systematically improving the quality and range of individual measures of cyber crime.* An overall measure of cyber crime (especially one that is built on poor quality sub-measures) is not likely to have much value. Whilst a general measure might seem an appealing exercise – if only to acquire a snapshot of the overall threat – cyber-related offences are, by their nature all quite different and reflect a broad range of offences. Focusing on improving the individual measures of different types of cyber crime would therefore seem a more productive first step. Markedly improving and expanding data on prevalence will also be a prerequisite to developing more informed estimates of cost. Cost measures will only be as good as the building blocks upon which they are based. Improving measures of prevalence is therefore where the Home Office has been placing most of its recent efforts. The introduction of Action Fraud means that some types of cyber crimes are more systematically identified and recorded. In order to capture more information on types of cyber crimes not covered by Action Fraud, the Home Office:
    - has introduced a voluntary cyber ‘flag’ onto police recorded crime;
    - is encouraging new questions to be added to the Commercial Victimisation Survey and the Crime Survey for England and Wales; and
    - will continue to review the effectiveness of these improvements.

- *Improving transparency and knowledge of the security industry sources and other private sector companies.* Estimates from security companies such as AV providers often lack transparency and yet these companies, along with wider stakeholders in the private sector, may hold a wide range of other information regarding the scale and nature of these crimes. Improving understanding of the data that industry partners hold and the assumptions/methods behind their research would help to improve knowledge of the area. As Viega (2012, p 16) states: *"if industry can get our act together, get ourselves connected with unified reporting, and get AV companies to participate as well, we could end up with a better picture of computer crime than we have of overall crime"*.

- *A new external working group will be set up by the Home Office, focusing on improving the estimates of the cost of cyber crime*. The group will seek to agree on the best available data for formulating any estimates, develop an agreed model for assessing costs and look to improve these estimates over time. Given that cyber crime relates to multidisciplinary yet complementary areas (for example, cyber security, criminology, law, psychology and economics) the group is likely to benefit from bringing together and drawing upon multidisciplinary expertise. The group may also consider further engagement and partnership with private sector businesses and industry partners (including AV companies) in order to help explore the potential use of a wider range of data sources.

- *Filling other knowledge gaps*. The review identified a number of areas where there is little evidence available, for example:
  - online drug dealing (both illegal and prescription drugs);
  - online hate crime, defamation and 'trolling';
  - online stalking;
  - use of the internet for human trafficking/smuggling;
  - second life or 'virtual world' crimes (for example, online 'crimes' undertaken by avatars [a manifestation of an individual's online identity, controlled and created by the user] in virtual and game play worlds); and
  - online or virtual currency (such as BitCoin [untraceable digital banknotes with financial value which can be traded online for goods and services or exchanged for offline, real-world currency]) .

These topics have not, as yet, been extensively researched in the published literature. However, they are areas that are likely to present increasing and new challenges for legislation and law enforcement, and will need consideration as part of future measures of cyber crime.

References

BERR (2008) *Information Security Breaches Survey.* London: Department for Business, Innovation and Skills. Retrieved from BIS, September 2013. Available at: <http://www.bis.gov.uk/files/file45714.pdf>.

Computer Misuse Act 1990.

Dutton, W. H. and Blank, G. (2013). *Cultures of the Internet: The Internet in Britain.* Oxford: Oxford Internet Institute, University of Oxford. Retrieved September 2013. Available at: <http://oxis.oii.ox.ac.uk/sites/oxis.oii.ox.ac.uk/files/content/files/publications/OxIS_2013.pdf>.

Fafinski, S. and Minassian, N. (2009) *UK Cybercrime Report.* Retrieved September 2013. Available at: <http://www.garlik.com/file/cybercrime_report_attachement>.

Florencio, D., and Herley, C. (2011) 'Sex, lies and cyber crime surveys', *Economics of Information Security and Privacy III*, pp 35-53.

House of Commons Science and Technology Committee (2012) *Malware and Cybercrime.* London: The Stationery Office Ltd.

Home Office (2011) *The National Crime Recording Standard (NCRS): What you need to know.* London: Home Office. Retrieved August 2013. Available at: <www.gov.uk: https://www.gov.uk/government/publications/the-national-crime-recording-standard-ncrs-what-you-need-to-know>.

Home Office (2012) *Counting Rules for Recorded Crime*. London: Home Office. Retrieved September 2013. Available at: <http://homeoffice.gov.uk/science-research/research-statistics/crime/counting-rules/>.

Home Office (2013) *Crime against businesses: Headline findings from the 2012 Commercial Victimisation Survey.* Retrieved September 2013. Available at: <http://www.homeoffice.gov.uk/publications/science-research-statistics/research-statistics/crime-research/crime-business-prem-2012/crime-business-prem-2012-pdf?view=Binary >.

ONS (2007) *Crime Survey for England and Wales* (formerly known as the British Crime Survey, 2006-2007 [computer file]). Data set available at UK Data Service [distributor]. Retrieved September 2013. Available at: <http://discover.ukdataservice.ac.uk/catalogue/?sn=5755&type=Data%20catalogue#variables>.

Viega, J. (2012) 'Ten Years On, How Are We Doing? (Spoiler Alert: We have no clue)', *IEEE Computer and Reliability Societies*. Retrieved September 2013. Available at: < http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06375718>.

Wall, D. (2007) 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace', *Police, Practice and Research: An International Journal*, 8 (2) pp 183-205.

ISBN: 978-1-78246-245-3