PREVENTING TELECOMMUNICATIONS FRAUD: RESPONSIBILISATION AND GUARDIANSHIP

Dr. Julianne Webster
Griffith University

Superintendent Brian Hay
Queensland Police Service[5]

ABSTRACT

The primary aim of this paper is to discuss how designing third-party policing responses to cyber-fraud – which is facilitated through telecommunications corporations – can better protect consumers and prevent crime. We discuss the prevalence and cost of frauds enabled by cyber environments, we briefly discuss comparative international third-party liability systems and we conclude by questioning the efficacy of the present Australia's approach to prevent cybercrime.

1. INTRODUCTION

Cybercrime is a distinct type of crime which typically does not involve an offender and victim that share the same or similar geographical location (Schruers, 2002, ACC, 2011). For non-cybercrime, traditional law enforcement efforts generally focus investigative attention on the locality of the victim and offender at the time of the offence. However in the context of cybercrime a similar law enforcement focus is rarely possible, due to the predominant transnational nature of these offences. In the cyber environment, for the crime to be committed, multiple actors to enable the crime to occur (AustGovt, 2009). The transnational nature of cybercrime relies upon the engagement of additional actors who facilitate access between the offender and victim (ACC, 2011).

In this paper, we argue that the speed of the internet and the prevalence of cybercrime victimisation demand a new paradigm of thought which encompasses the consideration of these 'other' actors and the roles they play to facilitate cybercrime – and likewise the types of roles they could play to correspondingly prevent this crime. In doing this we question the adequacy of the present response in Australia to cyber-fraud problems with particular reference to third-party liability for responding to illegal content being transmitted through email. Our review of the issue includes consideration of present international legislative response and proposes that measures to strengthen guardianship are necessary to have a greater impact on preventing cybercrime, in particular - cyber-fraud.

[5] The views expressed in this paper are the authors' own.

For the purposes of this paper, we define cyber-fraud as the transmission of a range of email communications that seek to defraud. In this context, the cyber-fraud offender utilises the services of ISPs in the transmission and subsequent delivery of email communications to the victim's computer. Therefore, the ISPs are the vital and necessary link between the fraudulent email communications and the recipient of these communications.

2. PREVALENCE OF CYBER FRAUD

Although the nature of the cyber fraud problem is difficult to ascertain with accuracy[6] , a number of surveys have estimated the prevalence of victimisation.

In 2012, a survey conducted by Norton of 13 000 people from across 24 countries showed that 72 per cent of respondents had been a victim of cybercrime. Crimes ranged from viruses; online credit fraud; unsolicited pornography; phishing and receiving excessive spam. The direct costs associated with these cybercrimes were estimated at US $110 billion for the preceding annual period. The results of the survey highlighted increases in 'new' forms of cybercrime compared to last year – such as those involving social media and mobile devices . In terms of the volume of malicious attacks, Symantec reported that its services blocked 5.5 billion malicious attacks in 2011 up from 3 billion in 2010 – an increase of 81% in one year.

An Australian Bureau of Statistics (ABS) survey published in 2008 estimated 806,000 people in Australia experienced personal fraud in the preceding 12 month period; with personal financial losses of almost $977 million. Victimisation was estimated to be five per cent of the population aged 15 years and over. Of this, identity fraud accounted for 3 per cent or an estimated half a million people (499,500) being victimised(ABS, 2008). In comparison, estimated victimisation jumped to 1.2 million Australians in 2010-2011. The latest estimates place national victimisation for personal fraud at 6.7 per cent of the population aged 15 years and over and the associated costs in Australia from these personal frauds was $1.4 billion in 2010-11 (ABS, 2012). However, one particular nuance of this environment that is not measured is the under-reporting of cybercrime. Perhaps this is best illustrated by the work undertaken by the Fraud and Corporate Crime Group, Queensland Police Service; with respect to Nigerian Advance Fee Fraud facilitated via the internet. In 2009, 200 people were interviewed about the circumstances involved in their sending money to Nigeria. Of these, at least 186 were victims of fraud and had collectively lost more than $21 Million. Perhaps the most alarming aspect of these losses is that no one had made a complaint to police.

Australian payments and clearing association (APCA) figures show that in 2011, losses on Australian issued credit cards through 'card not present' fraud was more than $197m, with a further $58 million lost through counterfeit card skimming and the use of counterfeit cards[7] .

Costs of fraud victimisation internationally show similar characteristics with the United States Internet Crime Complaint Center stating in their 2012 report that over 314 000 (314 246) complaints were received in 2011. Of these, nearly 116

[6] Underreporting is very common for these crimes, due to the potential for financial corporations to suffer loss of consumer confidence.
[7] http://www.apca.com.au/payment-statistics/fraud-statistics/2011-calender-year?CreditandChargeFraud

000 (115 903) involved financial loss, with the total loss being over $485m ($485 253 871); with an average loss of $1544 per person (IC3, 2012).

In the United Kingdom a December 2011 nationally representative study by the National Fraud Indicator (NFA), conducted face- to-face interviews with 1,775 people aged 16 years and over. The study found that approximately 6 per cent of participants identified that they had been a victim of some type of cybercrime within the preceding two years. Figures reported by the NFA calculated the overall cost to the UK economy from cybercrime at 27 billion pounds in 2011 (UKGovt, 2011).

More specifically, in respect to email deliveries, organisations such as RSA report on monthly 'phishing ' attacks perpetrated internationally (RSA, 2012). These data show that in the 12 months from November 2011 to November 2012 a total of 345 278 separate 'phishing' attacks were detected.

The extent of the cyber fraud problem is significant and the data suggests that current strategies need to be improved; as the number of victims and the amount of losses continues to increase annually.

3. CURRENT RESPONSE TO THE PROBLEM

In December 2010 , Australian ISPs were able to support a national and voluntary scheme called the ICODE to help protect their customers and their networks (AustGovt, 2009). The ICODE provides a consistent approach to help ISPs inform, educate and protect their customers in relation to the cyber security issues. The ICODE is not a statutory obligation – it is a voluntary measure designed to encourage individuals and ISPs to promote a better cyber security culture.

Previously, Australian lawmakers have imposed duties to access providers to prevent the accessibility of objectionable content governed by the Broadcasting Services Act 1992. However, the Act does not relate directly to the issue of cyber fraud and provides only guidelines for family friendly filtering arrangements, which are also voluntary for ISPs to adopt (ACMA and AISI) .

Internationally there has been extensive consideration of the liability of Internet Service Providers (ISPs) with regard to the content made available via their services (Carlye, 2000). However, much of the commentary has revolved predominately around defamatory material, pornographic images and little has been done to address the ISP's liability for acting as a vehicle of fraud and cybercrime.

In the European Union, an ISP is liable if they are found to deliberately collaborate with one of the recipients of their service in order to undertake illegal acts (Kleinschmidt, 2010) . Finland has a takedown notice relating to copyright and related rights infringements (Verbiest, 2007) and Hungary has implemented a notice and take down procedure with regards to infringement of intellectual property rights (Spindler, 2007). The United Kingdom's E-commerce Directive is legislated and confers liability to service providers concerning content transmitted if they are aware of the information and fail to remove or disable access to the information . In addition, the United Kingdom has mandatory data breach disclosure legislation. In particular this protects consumers who have had their personal details compromised or stolen from a third-parties database. The implications of this legislation are that it makes the

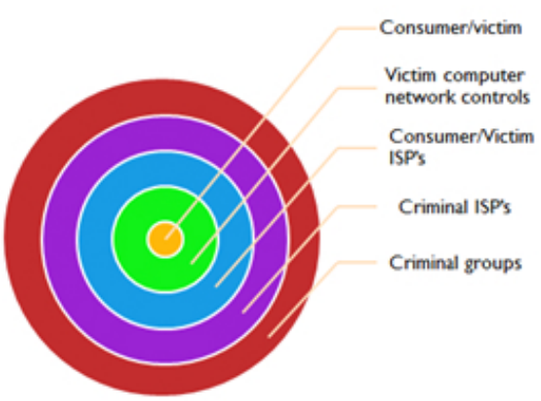
third-party holding that information more accountable for that information, and hence they take the security of that information seriously and acting accordingly. However, the United Kingdom ISP will not be liable if they did not initiate the transmission; did not select the receiver of the transmission; and did not select or modify the information contained in the transmission (The Electronic Commerce (EC Directive) Regulations UK 2002). In Japan, an ISP is liable if it was "technically possible to take measures" to disable or remove illegal content . It appears the United Kingdom and Japan are the most proactive countries when it comes to reducing customers' vulnerability to being exposed to illegal content via email transmissions.

We believe that in the context of a growing problem, it is timely and important to ask "Does the ICODE work?" We believe Industry would definitely say "yes" based upon the premise that the last desired action of government is regulation. Nevertheless, it is important that after two years of operation, the ICODE could benefit from being subject to a comprehensive evaluation.

4. INCREASING GUARDIANSHIP AND RESPONSIBILISATION TO IMPROVE PREVENTION OUTCOMES

Australia as well as other countries have acknowledged the pivotal role of ISP's in cybercrime (Kleinschmidt, 2010, AustGovt, 2009). The crime triangle originated by Marcus Felson describes how crime occurs when offenders, places and victims converge in space and time, in the absence of capable guardians (Felson, 1987). The routine activity approach typically depicted through the crime triangle, illustrates that when capable guardians are mobilised that crime opportunities can be reduced; and crime can be prevented. Often the application of the crime triangle is in the context of a single crime prone place; for example, an intervention targeted to a drug house (Green, 1995). However, with cybercrime there are multiple access points. Figure one illustrates the number of access points that offenders need to go through to reach their target in the context of cyber fraud delivered via email. According to the routine activities approach, if guardianship if mobilised at these access points there can be increased greater likelihood that crime can be prevented (Felson, 1995).

FIGURE 1: Cyber-fraud access points



When we consider the types of responses to fraud and cybercrime occurring internationally it raises questions as to whether there are response methods capable of strengthening the Australian response. When the Routine activity approach – involving the identification of guardians at access points – is coupled

with a third-party policing framework, to consistently mobilise these guardians –the enablers to cyber fraud can become the disablers of cyber fraud. By using a third-party policing model to mobilise a consistent response from third-parties, research shows a strengthened approach to prevention can be achieved (Webster, 2012, Ransley et al., 2012, Gilling, 2005, Hollis-Peel et al., 2011).

Some other examples of where third-party policing has shown to be a powerful crime prevention and law enforcement tool are financial reporting requirements (Deitz and Buttle, 2008), mandatory reporting of child abuse and neglect (Bird, 2011); and preventing the diversion of pseudoephedrine from pharmacies (Webster, 2012). In all of these examples, a third-party performs a specific role on behalf of the State to control and or prevent crime.

Arguably, preventing cyber fraud also needs one or more third-party champions to extend the response and responsibility beyond voluntary and ad hoc measures geared toward the provision of education, awareness and security of internet users. The complexity of this technical environment and the pervasiveness of cyber fraud dictates that it is beyond the ability of the average citizen to achieve the highest levels of protection and prevention at an individual level. The response needs to be based upon a multi-actor approach –industry, Government, community and individuals.

The benefits of a third-party policing model is that it empowers the third-party to take specific action; it provides a model which coerces unwilling or less willing third-parties to comply; it improves the consistency of the approach; makes better information available about crime prevalence and it is enforceable through specific regulations (Webster, 2012).

Cyber fraud is a problematic crime issue and it presents an important opportunity to design a better preventative response.

See full paper for full discussion.

REFERENCES

ABS 2008, Personal Fraud 2007, Catalogue Number 4528.0, Australian Bureau of Statistics, Canberra.

ABS 2012, Personal Fraud 2010-2011, Catalogue Number 4528.0, Australian Bureau of Statistics, Canberra.

ACC 2011, Organised Crime in Australia, Australian Crime Commission, Canberra.

AUSTGOVT 2009, Cyber Security Strategy, Attorney General's Department, Canberra.
Bird, S 2011, 'Child abuse: Mandatory reporting requirements', Australian Family Physician, vol. 40, pp. 921-926.

Carlye, P 2000, 'Legal regulation of Telecomunications: The Impact on Internet Services', in Edwards, L & Charlotte, W (eds.), Law & the Internet: a framework for electronic commerce, Hart Publishing, Portland.

Deitz, A & Buttle, J 2008, Anti-money laundering handbook, Thomson Lawbook Co., Pyrmont, N.S.W.

Felson, M 1987, 'Routine Activities and crime prevention in the developing metropolis', Criminology, no. 25, pp. 11-932.

Felson, M. (1995) 'Those Who Discourage Crime', in Eck J & Weisburd D (eds.), Crime Prevention Studies, vol. 4, Willow Tree Press, Monsey, NY.

Gilling, D 2005, Partnership and crime prevention, in Tilley N (ed.), Handbook of crime prevention and community safety, Willan Publishing, Cullompton.

Green, L 1995, 'Cleaning up Drug Hot Spots in Oakland, California: The Displacement and Diffusion Effects', Justice Quarterly, vol. 12

Hollis-Peel, M, Reynald, D, Van Bavel, M, Elffers, H & Welsh, B 2011, 'Guardianship for crime prevention: a critical review of the literature', Crime Law Social Change, vol. 56, pp. 53-70.

IC3 2012, 2011 Internet Crime Report, Internet Crime Complaint Center, Washington.

Kleinschmidt, B 2010, 'An international comparison of ISP's Liabilities for Unlawful Third Party Content', International Journal of Law and Information Technology, Vol. 18, 1-24.

Ransley, J, Mazerolle, L, Manning, M. McGuffog, I & Webster, J (eds.) 2012, Reducing the Methamphetamine Problem in Australia: Evaluating Innovative Partnerships between Police, Pharmacies and Other Third Parties, NDLERF, Canberra.

RSA 2012, Phishing and the social world, Hopkinton, MA 01748-9103, RSA Anti-Fraud Command Center, EMC corporation.

Schruers, M 2002, 'The History and Economics of ISP Liability for Third Party Content', Virginia Law Review, pp. 205-264.

Spindler, G 2007, 'Study on the liability of internet intermediaries: Country report - Hungary', University of Göttingen, Germany.

UKGOVT 2011, Fighting Fraud Together, National Fraud Authority, United Kingdom Home Office.

Verbiest, T 2007, Study on the liability of internet intermediaries: Country report - Finland, ULYS, Finland.

Webster, JL 2012, Innovative police responses to drug problems: Exploring a third-party policing partnership between police and community pharmacy, Doctor of Philosophy, Griffith University.

[i] Source: http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02. Accessed on 3/1/13
[ii] Source: http://www.homeoffice.gov.uk/agencies-public-bodies/nfa/ (accessed 4 January 2012)
[iii] 'Phishing' is broadly defined by the ABS (2012) as 'a fake notification or offer from a bank or other financial institution' and 'a fake notification or offer from an established business'. 'Advance fee fraud' is defined as 'an unsolicited request to transfer funds into a person's bank account in return for a commission or fee'. The definition of 'phishing' was broadened in 2010-2011 from the 2007 definition: 'a fraudulent request, purporting to be from a business or bank, to confirm a person's bank account or personal details'.
[iv] A single 'phishing' attack comprises typically many thousands of recipients of an email.
[v] Source: http://www.acma.gov.au/WEB/STANDARD..PC/pc=PC_310317 (accessed 4 January 2013)
[vi] Australian Communications and Media Authority (ACMA) and Australian Internet Security Initiative (AISI) http://www.acma.gov.au/WEB/STANDARD..PC/pc=PC_310317
[vii] Source: EU Directive on Electronic Commerce 2000/31/EC is the general framework for issues considering ISP's liabilities. Section 4 Liability of Intermediary Services.
[viii] The Electronic Commerce (EC Directive) Regulations 2002
[ix] Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Act No.137 of 2001)