Executive Summary

Central to developing and monitoring the progress of strategies for combating cyber crime is reliable information about crime volume, in terms of the number of incidents and offenders, the prevalence of cyberspace tools for the commission of crime, as well as the number of victims. This discussion paper assesses the potential for using innovative methodologies to estimate the scope of cyber-fraud, identifies existing data sources and gaps, and suggests novel sources of data that may help provide a more accurate picture of the degree of cyber-fraud in Canada. Further, possible ways to determine the proportions of cyber-fraud attributable to criminal networks rather than single individuals are discussed. This research is informed by a literature review and interviews with law enforcement and Information Technology (IT) personnel.

The literature review and interviews show that the largest impediment to effectively managing the problem of cyber-fraud is the lack of reliable data. The Government of Canada primarily relies on police-reported data for information about cyber-fraud. Yet, there are a number of reasons why fraud incidents are not reported to police. For example, companies may prefer to handle such matters internally, or individuals may only report that they were defrauded to their financial institution.

This research shows that current information about cyber-fraud is being funnelled to a variety of different organizations, including banks, regulatory agencies and various police agencies, or is simply not recorded. There is a clear shortage of data measuring the prevalence and costs of cyber-fraud in Canada and the available information is incomplete and fragmented. The lack of reporting of cyber-fraud incidents by individual and corporate/government victims means that many cases are not recorded or represented in official crime statistics. This research demonstrates a strong need for the creation of a national centre to record and measure data relating to cyber-fraud across Canada. A central databank of known cyber-fraud offenders and cases across the country could facilitate the identification and tracking of suspects in cyber-fraud cases and could further understanding regarding when one individual or group of individuals, is committing fraud all over the country. Ultimately, a national databank on cyber-fraud incidents could give law enforcement officials a better understanding of the types of cyber-fraud being committed in Canada.

Sophisticated technologies and the global distribution of computer networks also increase the difficulty of detecting and addressing cyber-fraud and hinder the ability to find and prosecute criminals operating online. In addition, there are operational challenges related to ensuring that law enforcement officials have the training and resources they need to adequately address the problem and able to identify perpetrators of cyber-frauds. Attempting to locate a perpetrator is problematic in many cases of cyber-fraud because skilled attackers cover their tracks by using proxies and other technical obfuscation methods.

This research suggests that the best source for further information on cyber-fraud is offender populations. Offender interviews may help uncover the network structure of hidden populations and help the law enforcement community to identify key players within the group. Of the options available for hidden populations, a truncated Poisson model is suggested as the most effective model. Ideally, this research could help pave the way for data collection and analysis that would

better inform law enforcement officials, investigators, and policy makers about the extent of cyber-fraud and cyber-criminal populations in Canada. This research may contribute toward the enhancement of prevention and suppression strategies as well as the development of an empirical means for evaluating the effectiveness of initiatives, including elements of Canada's Cyber Crime Strategy

1.0 Introduction

How can information be collected, evaluated, and reported on cyber-fraud offences in a more efficient manner? Clearly, the first step is to identify and define exactly what is being measured. The law typically takes a technology-neutral stance to offences (i.e. fraud is fraud whatever the method). Defining criminal phenomena is important because it enables all stakeholders, including police, prosecutors, and judges to have a common understanding. A universal definition also facilitates the aggregation of statistics, which can be used to create an accurate picture of current cyber-fraud related threats and developments. First, a general overview and definition of cybercrime are provided, followed by a discussion of cyber-fraud in all of its many manifestations.

1.1 The Definition and Classification of Cybercrime

Internet use exploded over the last decade, growing five-fold from 361 million users in 2000 to nearly 2 billion users around the globe in 2010 (McAfee 2010(a), 4). The way that Canadians do business has also changed. The use of cheques among consumers has declined while the use of credit cards, debit cards and Internet transactions to make purchases, conduct sales, and manage finances has dramatically increased (Canada 2005, 7). As many as 60% of Canadians now bank online, and in the United States (US), as many as eight out of ten households use online banking (Symantec 2010,12). As with other aspects of globalization, the Internet's rapid growth has far outpaced mechanisms of regulatory control, and this has led to the emergence of new criminal opportunities and presented significant challenges for policing across all corners of the globe.

Cybercrimes come in a variety of forms and there is no standard way of

(1) offences against the confidentiality, integrity and availability of computer data and systems;
(2) computer-related offences;
(3) content-related offences; and
(4) offences related to the infringement of copyright and other related rights.

Cybercrime can also include massive and coordinated attacks against the critical information infrastructure of a country, such as the cyber attacks against Estonia in 2007 (Schjolberg 2008, 9). Not only is the number of threats on the rise, the complexity of attacks has increased precipitously over time (Walther 2004, 7).

One of the central differences between cybercrime and traditional crime is that traditional crime typically occurs in one space and has an impact on one set of victims, whereas cybercrime can have a global impact (United Kingdom 2010, 5). Offenders can operate from anywhere in the world, targeting large numbers of people or businesses across international boundaries. This poses an obvious challenge for law enforcement, and those who commit cybercrime often seek to exploit this challenge, simultaneously undertaking their activities in one country against individuals in many different jurisdictions. Their activities are deliberately targeted in or through jurisdictions where regulation is known to be weak, or where investigative cooperation is known to be poor (United Kingdom 2010, 5). This allows for the minimization of the risk that their activities will be discovered, traced or result in punishment.

Given the breadth of cybercrime activity and the potential pool of potential victims, it is difficult to arrive at an accurate estimation of the number of cybercrime incidents per year. It is clear that the US had the most overall malicious activity worldwide in 2009, and was the top country of attack origin in 2009, accounting for 23% of worldwide activity (Symantec 2010, 16).[1] However, Symantec reports that malicious activity continues to be pushed to developing countries and in 2009 this trend became more pronounced (Symantec 2010, 7). For the first time since Symantec began examining malicious activity by country in 2006, a country other than the US, China or Germany ranked in the top three.[2] The primary reason is that information security and related laws and policies are less well-developed in emerging economies, providing an environment in which criminal activities can be carried out with less of a risk of detection and apprehension (Smith and Urbas 2001, 2). It is noteworthy that Canada did not rank within the top ten countries for overall malicious activity observed by Symantec in either 2008 or 2009, suggesting that Canada has not become a safe-haven for cybercrime offenders, despite that it has been comparatively slow to enact laws to address the problem.[3]

---

[1] This is a slight decrease from 25% in 2008.
[2] In both 2008 and 2009, the United States ranked number one for attack origin, malicious code, phishing hosts and bots and China ranked number two for attack origin. In 2009, Brazil ranked number three for malicious activity, with Germany ranking fourth (after ranking third in 2008). Symantec reports the top malicious activity by country for 2009

1.3 Defining ‘the Victims’ of Cyber-Fraud

While individuals (i.e. the general public) are the primary victims of most fraud insofar as they typically bear the financial costs through higher insurance premiums, credit card fees, interest rates, and so on, other victims also exist. A distinction can be made between primary victims, including individuals and businesses or public bodies, who initially suffer the harms of fraud, and secondary victims, or those who ultimately pay for the economic losses associated with the crime (Levi and Burrows 2008, 304). These include financial institutions, insurance companies, and others who, by contract or regulation, agree to reimburse some or all of the costs to primary victims. It must be stressed that some cyber-frauds are confined to a single class of victims, whereas others overlap, depending on the circumstances of the case (Levi and Burrows 2008, 304). For example, in the case of payment card frauds, victims can include the individual cardholder, the issuer, and the merchant.

The primary purposes of this discussion paper are to assess the potential for using innovative methodologies to estimate the scope of cyber-fraud, as well as existing data sources and gaps, and to suggest novel sources of data that might help provide a more accurate picture of the degree of cyber-fraud in Canada. Thus, it is important to consider the various costs of fraud to different victims, including:

- direct losses suffered by victims as a result of fraud (i.e. the actual amount defrauded);
- costs to the victim(s) of preventing fraud before the event (i.e. both public and private sector entities take certain defensive measures to safeguard against fraud, such as shredding documents or employing IT security measures); and
- costs of responding to fraud after the event (i.e. costs to the criminal justice system, including police, prosecutors and court services, as well as, in the case of organizations, internal private investigations, increased security measures and consumer notification) (Levi and Burrows 2008, 305).

Other indirect losses, which are more difficult to quantify, can result from the reduction in the use of online banking services (assuming that this is more cost-effective for the victim bank) or harm to the defrauded organization’s reputation in the marketplace (assuming that this leads customers and other firms to avoid doing business with them). Ultimately, the question of which group or entity shoulders the cost of cyber-fraud is complex and presents a challenge to aggregating the costs of fraud to the Canadian economy (this issue is discussed in detail below).

1.4 The Most Common Types of Cyber-Fraud

Fraud involves purposefully obtaining the property of another through deception, and its popularity as a crime of opportunity is growing. This is largely due to the fundamental shift in the methods by which many forms of property are owned and stored, owing to rapid developments in technology, communications and globalization (Albanese 2005, 7). For example, in Canadian society, credit and debit card transactions are taking cash transactions in value, and the rise and growth of the Internet, which facilitates wireless transactions, has made theft, as well as the conversion of stolen property into cash, relatively effortless (Albanese 2005, 7).

Today, identity-related offences are the most common form of consumer fraud. Other examples of Internet fraud include advance fee scams, such as Nigerian scams, lottery scams and inheritance frauds, online auction frauds, and other identity-related and payment card frauds. Internet fraud has been facilitated by obtaining credit card numbers from various online services, which can then be used to fraudulently pay for goods and services ordered online. Included below are examples of some of the most current and pervasive fraud scams on the Internet.

Scareware

Misleading pop-ups suggest that a user's computer is infected with a virus, and prompt them to purchase fake antivirus software to fix the problem. When the victim agrees to the purchase, they provide credit card details to the persons behind the scam. Scareware remains one of the most common Internet threats because it manipulates the psychology of victims (McAfee 2010(a), 7). By playing to Internet users' fear that their computers and their information is at risk, individuals have been able to gain access to users' machines, directly defrauding victims of millions of dollars. In 2009, Symantec observed a dramatic increase in scareware that in the first six months of the year compared to the last six months of 2008; they further identified 250 variants of scareware being circulated on the Internet (Symantec 2009).

Phishing Scams

Phishing is one of the most prevalent Internet threats today. Recently, attacks have become more advanced in their technical sophistication, by making use of well-known vulnerabilities in popular Web browsers, including Internet Explorer, to install malicious software that collects sensitive information about the victim. Phishing attempts come in a variety of forms, such as through spam emails, or instant messages, and fake requests on social networking sites, often with a link to a realistic but phony Website designed to steal the victim's password, credit card number, or bank account numbers by mimicking the look and feel of a legitimate online banking Website. As discussed below, phishing has been greatly facilitated by the abundance of phishing software kits with easy-to-use point-and-click interfaces being sold inexpensively in the online underground economy. One of the reasons why phishing is so successful is that ordinary consumers are easily

Canadians have been fraud victims, the same incidence as reported in 2006 and 2007 (Ipsos Reid 2009, 6). Canadians are most commonly targeted for investment fraud through email (33%), by a stranger on the telephone (28%), or through a friend, family member or coworker (18%) (Ipsos Reid 2009, 5). The amount invested in fraudulent investments has also apparently increased. In 2009, 38% invested in $5,000 or more, compared to 32% in 2006. The average amount invested is $7,634 across Canada. Most money is never returned to victims.

One in-four Canadians (26%) say that they reported the attempt to authorities, compared to 17% in 2007, and 14% in 2006 (Ipsos Reid 2009, 5). Yet, among Canadians thinking that it is important to report suspicions that someone has approached them with an investment fraud has declined since 2006.[5] Those who did not report the attempt most likely did not do so because it was email spam (16%), they did not think that reporting it would do anything/make a difference (12%), they were not sure it was fraud (12%), they felt they had nothing concrete to report (11%), and/or they preferred to just ignore it (11%) (Ipsos Reid 2009, 5).

Identity-Related Fraud

One of the most common strategies to perpetrate fraud is the creation of false documents for misrepresenting identity. Once a fraudulent identity has been convincingly established, it is then possible to steal money or otherwise act illegally and evade investigation and prosecution. The Internet facilitates this sort of fraudulent activity by making it easy to manipulate email and Internet addresses, and to obscure the source of a message through the use of technological tools, such as anonymizers, anonymous remailers and the like.

Credit card fraud is the most common incident of identity-related fraud (Berg 2009, 227). For example, the UK Government reported that losses from credit card fraud where the consumer's card was used without them present were £328 million pounds in 2008 (an increase of 13% from the previous year) (United Kingdom 2010, 5). In this scenario, the offender uses the victim's identity in order to apply for and obtain new credit cards or fraudulently uses an existing card belonging to the victim. Other examples of identity-related fraud include using the stolen identity to obtain phone services, or other utility; opening bank accounts using the victim's information or writing cheques against the victim's account

frequently willing to trade-off their privacy concerns in return for benefits such as convenience (Chellappa and Sin 2005, 181). This trend is problematic because goods and services can easily be obtained using active cards that have been obtained through illicit means. Also, they can be obtained using counterfeit credit cards created from stolen information, such as through the online underground economy, discussed below. Credit cards can also be cloned using illicit card readers (known as 'skimming') during an otherwise legitimate transaction, or from discarded credit card receipts (Wall 2010(a), 70).

The online credit card fraud (or 'carding') market place has evolved significantly in recent years. As discussed below, there are large, heavily moderated forums devoted to enabling offenders to buy and sell stolen information and products, share tips and techniques, and post cybercrime related news stories (Howard 2009, 28). Several high-profile law enforcement operations (most notably 'Operation Firewall' in 2004) caused many once prominent carding operations to move underground; hence, much of the current online communication about carding is conducted through secure channels, such as Internet Relay Chat (IRC) rooms, messaging services and email (Howard 2009, 26). In 2009, combined losses due to payment card fraud in Canada decreased slightly from $512.2 million in 2008 to $500.7 million in 2009 (CISC 2010, 29). At the same time, losses due to debit card fraud increased by 36% from $104.5 million in 2008 to $142.3 million in 2009 (CISC 2010, 29).

Insider Fraud

Internal employees can use the Internet to anonymously gain access to data that is not related to their jobs and misuse it for personal gain (Campbell 2009). Opportunities have arisen for employees of both public and private sector entities to commit a variety of online frauds, such as manipulating electronic claims processing systems, compromising digital signature keys, or altering/diverting electronic fund transfers away from legitimate recipients (Smith and Urbas 2001, 54). Rogue insiders can also gain electronic access to the records of customers and other employees and use those records to fraudulent ends. These malicious acts are commonly perpetrated by current employees and contractors as well as disgruntled former employees who have been dismissed, laid off, or who have resigned.

It is also significant that 'well-meaning' and/or negligent insiders pose an additional threat by disclosing data that can be used by malicious outsiders against the organization (Wall 2010(b), 3). Indeed, in 2009, in the US, 40% of data breaches, and 46% in the UK, were estimated to result from insider negligence (Wall 2010(b), 3). In some cases, insiders use very simple passwords, or may use one password for all of the secure sites they access. Alternatively, they might write down passwords on post-it notes attached to computer screens or circulate them to colleagues to check their email messages for them (e.g. if they are away on vacation) (Wall 2010(b), 9). Others knowingly take risks to bypass security processes in order to become more efficient at work (Wall 2010(b), 9). In other cases, employees can be duped by malicious outsiders into sharing sensitive information or giving access to systems through 'social engineering' scams because they genuinely believe that they are being helpful and acting in good faith (Wall 2010(b), 10).

2.0 The Prevalence and Cost of Cyber-Fraud

Is cyber-fraud, in all of its manifestations, a serious problem in Canada? How does it compare to the frequency and costs of other kinds of crime? While there are many accounts of cyber-fraud documented in the electronic and print media, the frequency with which cyber-fraud occurs and the losses that result are extremely difficult to ascertain with precision. Canada does not have a uniform method of collecting data on cyber-fraud.

As with other kinds of fraud, Internet fraud is rarely reported to law enforcement authorities. This makes it extremely difficult to quantify the scale and scope of the problem. The shortage of valid and reliable statistics has severely hampered our understanding of the nature, prevalence and impact of cyber-fraud, as well as the ability of law enforcement to respond to it. The principal sources of information concerning fraud are business victimization surveys, and consumer reporting centres, as well anecdotal accounts of successful criminal prosecutions that are reported through the media. The incidents of Internet cyber-fraud that are disclosed to the public represent a small proportion of the total number of incidents that occur, which means that there is a need for more systematic data to be collected on the nature and extent of Internet fraud in Canada.

There are a variety of important reasons why businesses elect not to report fraud to the police. They may be reluctant due to the fear that the incident was too minor or that it will be impossible to recover losses successfully through legal channels and that the time and resources needed to report an incident to the authorities and to assist in its prosecution do not justify the potential return on this investment (Smith and Urbas 2001, 41). In such cases, they may decide to rely on other means, such as using internal or private investigators and/or reporting the incident to entity other than law enforcement (e.g. PhoneBusters, FINTRAC, or the Better Business Bureau) (Taylor-Butts and Perreault 2008, 12). The other major disincentive for organizations to report is the disinclination to publicize the victimization because of a fear of losing business or harming their commercial reputation in the marketplace (Smith and Urbas 2001, 42). Governments, for their part, are reticent to disclose IT security breaches due to the risks of alienating voters and losing trust in the public service.

There is clearly a need for more systematic data to be collected about the nature and amount of cyber-fraud in Canada and for extensive analysis of the problem. It is also significant that, in the limited cases where research does exist, there are numerous data-related and methodological problems (White and Fisher 2008, 13). For example, there is no consistent definition or use of the terms ‘identity theft,’ ‘fraud,’ and ‘cyber-fraud’ across agencies or organizations. This means that when data are available, they may not be comparable. Data is also affected by a number of agency-specific variables, including budgets, staffing, resources, awareness of the problem and national response. There is also the difficulty of generating a random sample of victims of cyber-fraud or identity theft because those who do contact law enforcement or an agency are not necessarily representative of all victims. Thus, studies that identify victims based on prior contact with an agency, law enforcement, or even by survey, are not likely to capture all fraud/identity theft victims and offences.

Indeed, there are few reliable statistics on the prevalence of fraud, and there is no precise way of assessing how much of this type of activity occurs, largely because a significant proportion of

establishing a common body of knowledge about the optimum practices to maintain information security.

The study indicated that Canadian IT security professionals consider colleagues and personal networks to be their primary sources of IT security information (Wenneker 2008). It is significant that these individuals reported feeling highly comfortable with using personal networks. Among personal networks there is less chance of appearing uninformed or technically challenged, and those who are part of a personal network are likely seen as credible sources of information. These findings substantiate the research evidence cited by Canadian IT security professionals, as discussed below in subsection 9.2. These findings suggest that new initiatives, such as creating an online database of best practices which IT security professional members can add to and view, and/or developing an online community (e.g. send out advice and tips) and holding best practice information sessions/conferences within specific industry sectors, could be instrumental to proactively responding to cyber-fraud threats, as well as gathering reliable information about current threats and vulnerabilities.

Another source of information on cyber-fraud is Statistics Canada's Survey of Fraud Against Businesses in 2008, which focused on 4,330 Canadian businesses in the retail, banking and insurance industries (Taylor-But

3.0 Cyber-Fraud, Organized Crime and the Online Underground Economy

From a policy and law enforcement perspective, it is critical to unders

Many such groups have adapted to technological change and used computer technologies to facilitate their offline criminal activities, such as drug trafficking and money laundering. Online auctions provide a means to move money through seemingly legitimate purchases, and as e-money and electronic banking become more pervasive, opportunities to hide the movement of the proceeds of crime in an increasing array of financial transactions are likely to increase. In other cases, organized criminals have used the Internet to develop new crimes and expand upon traditional ones.[11] Examples of traditional organized crime groups engaging in technology-enabled crime include the Asian Triads and Japanese Yakuza whose criminal activities have included computer software piracy and credit card forgery/fraud (Choo 2008, 273).

Criminal groups have been able to focus their efforts on publicizing software vulnerabilities they discover, writing malicious code and developi

This process is understandable given that secrecy is usually a central aspect of any organized crime activity, and the Internet provides a higher degree of concealment to those who use it. Faced with the perpetual threat of identification and apprehension, many participants in criminal organizations try to reduce the likelihood of detection by police or betrayal by accomplices by trying to build trust and group solidarity between participants (Morselli 2011, 26). In the case of many online criminal networks, members rarely meet in person and individuals are often known only by their cyber-aliases or nicknames (Morselli 2011, 26). Individual members can connect with other individuals with the requisite technical skills on an as-needed basis, masking their identities and significantly reducing the risk of being caught. Many Web forums are self-policing and have safeguards that can be used as protections, such as weeding out disloyal 'rippers' (i.e. scam artists who prey upon other criminals by ripping them off) (Morselli 2011, 26).

Many online crime groups also have a home base in states with few or no laws directed against cybercrime. This provides an additional layer of protection against law enforcement and enables

underground economy, are making it easy for novice hackers to compromise computers and steal information (Symantec 2010, 11).

A crimeware kit is a toolkit that allows people to customize a piece of malicious code designed to steal data and other personal information (Symantec 2010, 11). The success of these kits as a means of cyber-attack was demonstrated in 2009 when the top five phishing kits observed by Symantec were responsible for a combined average of 23% of all observed phishing attacks for the year (Symantec 2010, 18). The lowering of barriers for neophytes to enter

forwarding the balance through an anonymous money transfer service (such as a wire transfer service like Western Union). Mules are often individuals who

most part, micro-frauds tend to be too small in impact to warrant the expenditure of police resources, even within local jurisdictions (Wall 2010(a), 80). Clearly, the most effective response to micro-frauds is a combination of technological and education solutions, including ensuring that individual computer users make their systems more secure and remain on the lookout for scams. However, as Wall points out:

> A major problem experienced to-date in policing the micro-frauds that result from the likes of scareware has been has been the lack of an effective, consistent and easy reporting system. This has long meant that crucial strategic intelligence which identifies 'the bigger picture' of impact at a national level has been lost, as has the important tactical criminal intelligence relating to the offenders, which hampers the police ability to investigate (Wall 2009, 64).

It is important that organized cybercrime groups are decentralized and do not provide a single target or point of failure for law enforcement, largely because they rely on many different actors in various countries, particularly within unregulated environments (Etges and Sutcliffe 2008, 91). The global nature of these organizations, and the fact that they are constantly changing geographic location, increases the difficulty of locating the perpetrators behind their operations and shutting them down (Symantec 2009, 56). The Internet also provides more secrecy and anonymity than any real-world physical environment. The non-hierarchical and network-based structure for coordination and cooperation is ideally suited for criminals in the digital age. This is evidenced by the increased number of computers used to perpetrate crime remotely (i.e. 'bots').[15] The online underground economy also provides global opportunities for the distribution of intangible goods (e. g. malicious software code and stolen identity information) and specialization in individual products and services (e.g. network and application attack vectors, data hiding, financial fraud, identity theft, credit card fraud, and others) (Etges and Sutcliffe 2008, 92). To combat these sophisticated and network-based criminal structures operating on the Internet, governments must form coalitions between law enforcement, government agencies, private sector organizations, NGOs, and professional organizations across jurisdictional boundaries (Etges and Sutcliffe 2008, 93). Combating cyber-fraud is a perfect example where financial intelligence and interaction between public and private sectors is required (Gottschalk 2010, 268).

4.0 Cyber-Fraud Legislation in Canada and Elsewhere

4.1 The Canadian Legal Framework

One of the challenges currently faced by legal authorities is the difficulty of applying existing legislation to criminal activities involving new technologies. Legislating in this area is faced with the complexity of protecting consumers and encouraging e-commerce growth without placing unnecessary restrictions on the trans-border flow of data (Davis 2003, 208). The Criminal Code

[15] Bot computers are computers that have been deliberately infected with a virus that allows the criminal to control

has long contained a provision targeting fraud at s.380. Prior to the enactment of the new identity theft legislation (discussed below), the Criminal Code did not contain any specific identity theft offence. With the exception of the offences dealing with computers (s.342.1), and devices to obtain computer service (342.2), the Code offences relating to property and theft predate computer technology and the Internet.[16] There is also an offence in the Code which deals with mischief in relation to data (s.430); however, this provision has not been used to prosecute anyone in Canada for committing fraud or identity theft.

Bill S-4, An Act to Amend the Criminal Code (Identity Theft and Related Misconduct) received Royal Assent October 22, 2009. It created several new Criminal Code offences targeting those aspects of identity theft not already covered. Note that there was no identity theft offence prior to this. More specifically, it focused on the preparatory stages of identity theft by making it an offence to obtain, possess, transfer or sell the identity documents of another person. The key provisions of this legislation are as follows:

- Clause 1 – Added section 56.1(1) to (4) of the Code - making, possessing, transferring, offering or selling "identity documents" of another person.
- Clauses 4 and 5 – Added section 342(3) and 342.01 (1) of the Code - fraudulent use or possession or trafficking of credit card data and knowingly possessing, importing or exporting devices that can be used to fraudulently copy credit card data.
- Clause 8 – Added section 368(1)(c) and (d) of the Code - using forged documents as if they were genuine, selling/making available forged documents, possessing forged documents with the intent to use it.
- Clause 9 – Added section 368.1 of the Code - illegal to obtain devices used to create forged documents.
- Clause 10 – Added to the existing offence the fact of pretending to be another person to avoid arrest or prosecution or to obstruct the administration of justice. Defined 'personating a person' to include pretending to be a person or using that person's identity information as if it pertained to the person using it. For someone to be found guilty of identity theft, the prosecution must prove that he or she knowingly obtained or possessed another person's "identity information." Identity information is defined as "any information – including biological or physiological information – of a type that is commonly used, alone or in combination with other information, to identify or purport to identify an individual." The new s.402.1 of the Code gives examples of identity information. Also added section 402.2(2) of the Code - transmitting, making available, distributing, selling, offering for sale or possessing another person's "identity information" and amended section 403 of the Code, replacing the offence of "personation with intent" with identity fraud.

There are also a number of provisions in the Personal Information Protection and Electronic Documents Act (PIPEDA) that can significantly reduce the risk of identity theft and fraud by

[16] Note, though, that under s.342.1 of the Code, fraudulent unauthorized interference with computer systems is an indictable offence punishable by ten years' imprisonment.

placing limits on the collection, use and disclosure of personal information. PIPEDA requires organizations engaged in commercial activities to adopt a number of safeguards with respect to the personal information they collect.[17] Both private and public sector organizations are also beginning to establish fraud control policies that address the risks associated with widespread Internet penetration in Canada. However, there needs to be further harmonization of these initiatives to deal with the problem of trans-border Internet fraud.

4.2 The Legal Framework in the United States

In the US, the regulation of electronic commerce, including the fraudulent activities discussed herein, generally fall the Federal Trade Commission (FTC), and to a lesser extent to the Department of Justice (DOJ), which can conduct criminal prosecutions and seek civil injunctive relief pursuant to 18 U.S.C. 1345 (Cukier and Levin 2009, 262). The US Constitution grants Congress the authority to supervise interstate commerce, of which electronic commerce, including spam, phishing, and other fraudulent activity committed over the Internet, is incorporated. There are a number of provisions within the Uniform Commercial Code which pertain to Internet fraud, including the following: Access Device Fraud (18 U.S.C. 1029) (i.e. fraud and related activity connected with access devices); Computer Fraud and Abuse Act (18 U.S.C. 1030) (i.e. fraud and related activity in connection with computers); CAN-SPAM Act (18 U.S.C. 1037) (i.e. fraud and related activity in connection with electronic mail; credit card fraud (15 U.S.C. 1644) and the Identity Theft Assumption Deterrence Act (i.e. 18 U.S.C. 1028) (i.e. fraud and related activity connected with identification documents, authentication features, and information).

In addition, the Fair Credit Reporting Act (15 U.S.C. 1681) was amended in 2003 by the Fair and Accurate Credit Transactions Act, with specific sections designed to combat identity theft. For example, the law requires credit agencies to correct erroneous charges within four days of receiving a police report and, in addition, credit agencies must take extra steps to verify an applicant's identity when a fraud alert has been placed on a consumer's file (White and Fisher 2008, 5). The Gramm-Leach-Bliley Act (1999) contains a section dealing with fraudulent access to financial information, requiring financial institutions, such as banks and investment companies, to have policies procedures and controls in place to prevent the unauthorized disclosure of customer financial information (White and Fisher 2008, 5). Lastly, the FTC was created by Congress, through the Federal Trade Commission Act. The Act, and subsequent legislation,

- dealing with differing privacy regimes;
- achieving mutual assistance and strategic intelligence in a timely manner;
- the need to secure the cooperation and assistance of internet service providers (ISPs);
- the need for the trans-national search of computer data banks and the interception of

In recent years, there have been a number of milestones that address the challenges of combating trans-national cybercrime. One of the most significant of these was the Council of Europe's Convention on Cybercrime, whose efforts to harmonize substantive and procedural law serves as a model for nations around the world. This was the first multilateral treaty aimed at facilitating international cooperation in the prosecution of computer crimes. It was signed in Budapest on November 23, 2001, by member states of the Council of Europe and by several non-member states, including Canada, Japan, South Africa and the US, that participated in its development (Huey and Rosenberg 2004, 597). The Convention entered into force on July 1, 2004. As of March 16, 2011, there were 47 signatory states.[19]

Of the 47 countries that signed the Convention, 30 countries have ratified it and entered it into force, including the US. Canada has not ratified the Convention. The Convention requires each signatory state to make it an offence to commit certain crimes using computer systems (including computer-related fraud and forgery, offences related to child pornography and the infringement of copyright) and to grant new powers of search and seizure to its law enforcement officials, including the expedited preservation of stored computer data, search and seizure of stored computer data and the real-time collection of computer data. Article 25 requires law enforcement officials in each signatory state to assist those of other participating states by cooperating with "mutual assistance requests" from police "to the widest extent possible."

Elsewhere in the world, regional organizations have begun to address the important unresolved issues relating to trans-national cybercrime. Beginning in the late 1990s, the G8 subgroup on high tech crime established a 24/7 network of experts to assist in high-tech crime investigation to ensure that no criminal receives a safe haven anywhere in the world (Schjolberg 2008, 13). The G8 also negotiated principles and an action plan to combat high tech crime, as well as better practices documents, including guides for security of computer networks, international requests for assistance, legislative drafting, and tracing networked communications across borders (Urbas and Choo 2008, 12). In addition, the G8 has worked with training conferences for cybercrime agencies from every continent (except Antarctica) and conferences for law enforcement and industry on improved cooperation and tracing online criminal communications.

Similar steps have also been taken by the Organization for Economic Cooperation and Development (OECD). In 2002, the OECD published Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, which were developed with the following aims: promote a culture of security among all participants in the use of information systems and networks; raise awareness of the risks to information systems and networks, as well as the policies, practices, measures and procedures available for their implementation; foster greater confidence among all participants in information systems and networks and the way in which they are provided and used; create a general framework of reference that will help TT4 and NGOs understand security issues and respect ethical norms when developing and implementing policies and procedures for the security of information systems and networks. (Urbas and Choo 2008, 12).

[19] Council of Europe Treaty Office, available online at: http://conventions.coe.int.

The European Union (EU) adopted a Framework Decision and entered it into force in 2005, which provides that states will criminalize illegal system interference and illegal data interference, and illegal access to information systems (Urbas and Choo 2008, 15). Similarly, the Asia Pacific Economic Cooperation (APEC) has committed to encouraging its member states to enact a comprehensive set of laws relating to cybercrime, as well as a policy framework that addresses substantive, procedural and mutual legal assistance measures, consistent with international legal instruments (Urbas and Choo 2008, 16). APEC has conducted a capacity-building project on cybercrime for its members in relation to legislation and investigative capabilities, whereby the advanced APEC economies support the less advanced in training law enforcement personnel (Li 2007). Similar commitments were also made by the Association of Southeast Asian Nations (ASEAN) in 2006, and the League of Arab States, as well as some members of the African Union. As well, in 2008, NATO opened a centre for excellence on cyber defense in Estonia, in order to conduct research on cyber warfare. The Organization of American States (OAS) has also taken steps to combat threats to cybersecurity, including urging member states to adopt cybercrime laws and to facilitate international cooperation.

The connection between organized crime and cybercrime was one of the focuses of the 11th UN Crime Congress in 2005. The United Nations General Assembly has also adopted a number of resolutions on combating the misuse of information technologies. A UN Working Group on Internet Governance was established to contribute to the World Summit on the Information Society which was held in Tunisia in November 2005 (Schjolberg 2008, 10). A Global Cybersecurity Agenda was also launched in May 2007 by the Secretary-General as a global framework for dialogue and international cooperation in the development of strategies and solutions to enhance information security. Additionally, the International Telecommunications Union (ITU) in Geneva has become the most active UN organization aimed at reaching harmonization on global cybercrime legislation and it has been looking at how to promote international cooperation and build on existing international agreements in this area, particularly the Council of Europe's Convention on Cybercrime (Schjolberg 2008, 20).

The private sector has also been active in trying to enhance the ability of law enforcement officials around the world to deal with the problem of cybercrime. For example, Microsoft has invested millions of dollars in developing an international training program and technological resource for law enforcement agencies around the world to be able to investigate computer-facilitated crimes against children (Microsoft 2005). This project was initially developed with the help of several international police agencies in conjunction with the RCMP and the Toronto Police Service (RCMP 2005). While it has primarily been used to combat online child pornography, it can also be used to facilitate the investigation and prosecution of other kinds of offenders, such as those committing fraud and identity theft. Successes such as these indicate that the global fight against transnational cybercrime is capable of being won.

6.0 Additional Issues for Law Enforcement and Prosecutors

In Canada, the Royal Canadian Mounted Police (RCMP) is responsible for the investigation of all computer crime offences within its jurisdiction, as well as those in which the Government of Canada is victimized, regardless of the source of the offender, as well as offences involving organized crime or affecting the interests of Canada. Commercial crime sections of the RCMP

(van der Heijden et al. 2003), and drug dealers (Bouchard and Tremblay 2005). Due to the inherent nature of criminal offending, capture-recapture methodologies require expansion in order to satisfy two key assumptions: population homogeneity and independence.

The problem is that the two-method sample requires that no outside variables influence the actor's inclusion (or lack thereof) in the second sample. The cases must be independent of one another across samples (Weaver and Collins 2007). This might be problematic for current efforts in the case where, for example, an offender who was

arrested twice in a given time period (Bouchard 2007). Accordingly, if data on known arrests and re-arrests "follow the Poisson distribution specified by Z's model, the missing cell in the distribution should be estimated correctly, that is, the number of offenders with zero arrests" (Bouchard 2007). This approach allows for an assessment of hidden populations.

The advantages of Zelterman's Poisson estimator for the purpose of estimating criminal populations are evident. First, it can minimize the impact of population heterogeneity in arrest risks by eliminating the minority of high-rate offenders with multiple arrests. Specifically, the formula provided by Zelterman includes only those offenders arrested once (n1) or twice (n2) for the purpose of establishing the arrest parameter. As Bouchard comments:

> Zelterman (1988) and other researchers who derived similar models (Chao 1989), base their approach on the rationale that estimation models should be complex enough to be meaningful, but simple enough to contain only the parameters that are necessary, and close to the quantity to be estimated: Observations that are close to the object of interest should, intuitively, have more bearing on it. (Bouchard 2007).

Although this characteristic will result in more conservative estimations, there is some logic in the notion that information about offenders who are not arrested might be best estimated from information about offenders who are rarely arrested. It should be noted that more information is provided by using more complex models that consider the full range of arrestees and their different arrest rates (Bouchard 2007),[21] or models that consider a series of covariates in fitting an estimation curve (Bouchard 2007).[22]

A second advantage of Zelterman's truncated Poisson model is it can be used on only one sample (as with arrest data), which is in contrast to other capture-recapture approaches that require three or more samples to develop estimates. While this might be seen as a disadvantage in that there are instances in which triangulation would be advantageous for identifying a sample, the preferred method of estimating a hidden population of cyber-fraud offenders requires focus on those who are currently unaccounted for within the general population. Stated differently, using only arrest data confines the interpretation to prevalence estimates of offenders "at risk of being arrested," which specifies the scope to those who are considered hidden (Bouchard and Tremblay 2005).

A possible concern associated with the use of Zelterman's truncated Poisson model is that the population of unknown cyber-fraud offenders cannot be assumed to be a closed population because there is a distinct possibility that offenders will enter and exit criminal activity. Despite this reality, the model assumes that "the hidden population of interest is a "closed" population" (Bouchard 2007). To overcome this problem, other researchers who have employed the Zelterman's truncated Poisson model have compensated through the use of data at an aggregate level. For example, in the identification of hidden populations of marijuana growers, Bouchard

---

[21] "Compared to the 30,298 index offenders estimated by Greene and Stollmack's (1981) heterogenous Poisson model for D.C. in 1975, the Zmodel derives an estimate of 29,842 offenders (a 2% underestimate)."

[22] "Compared to the 62,722 illegal gun possession offenders estimated by van der Heijden et al.'s (2003) Poisson-based regression model, the Z model derives a 50,866 offender estimate (a 23% underestimate)."

demonstrates that the "likelihood of severe departures from this assumption is minimized [with]… analysis of re-arrest distributions at an aggregate level (arrests and re-arrests at the provincial level) rather than at a city or neighborhood level" (Bouchard 2007). Although this does not eliminate the risk of desistance from criminal activity, aggregate level measurement does mitigate the chances of offenders "being excluded from a sample simply because they moved to another city or neighborhood" (Bouchard 2007).

There is also some evidence (Kendall 1999) that using closed models for open populations is not necessarily as problematic as might be first assumed. As is suggested by Bouchard, "if the period under study is short enough, criminal population movements are unlikely to be swift and massive enough to have an impact on the prevalence rates" (Bouchard 2007) derived from closed population models such as Zelterman's. Given that Zelterman's truncated Poisson model has yet to be tested with a cyber-fraud population, and that the inherent 'non-spatial/non-geographic' component of cybercrime requires more investigation, it would be prudent to supplement the model with the use of hidden Markov models or others crafted for open populations. The selection of either or any data capture method is highly tied to the identification of specific population characteristics so that the most appropriate method is employed.

8.0 Establishing the Characteristics of Cyber-Fraud Offenders, Investigation and Networks

In academic discourse, a number of theories have been put forward to explain why people commit fraud. Some of the essential factors identified by researchers include the following:

- a perceived opportunity, such as the absence or bypassing of controls that enable fraud to be identified or prevented;
- an offender with a motivation to steal assets, whether through the existence of a financial crisis, the presence of debts, or living beyond one's means;
- a rationalization for acting illegally, such as the belief that the victim can bear the loss, or that the stolen funds will be repaid; and
- the absence of capable guardians, such as through inefficient business security practices, the absence of an effective regulatory framework, or a lack of effective fraud prevention resources and tactics.

The motivations and justifications for cyber-fraud are much the same. However, the Internet has created new opportunities for fraud, and offenders can relocate to jurisdictions where Internet Service Providers (ISPs) have trouble monitoring and filtering the increasing amount of traffic across their networks (Symantec 2010, 8). The Internet is a highly vulnerable domain, with few protections in the way of guardianship (White and Fisher 2008, 17). In addition, social networking sites continue to provide new opportunities for crime and some industry analysts have predicted that these venues will face new threats as the number of users continues to grow (McAfee 2010(b), 2). Users have proven to be highly trusting in these social environments and readily click on hyperlinks or other kinds of invitations to view content sent by their 'friends' (McAfee 2010(b), 4).

A number of other recent trends have increased the number and frequency of cyber-fraud incidents:

- an underground economy has evolved around stealing, packaging, and reselling information (Deloitte 2010(a), 5);
- individuals and organizations are increasingly dependent upon computer-based technologies for the storage and processing of information and communications;
- online banking, investing, retail and trade, as well as widespread intellectual property distribution, have created new opportunities for fraud and theft; and
- economic hardships resulting from the 2008-2010 global financial recession created new opportunities to exploit peoples' fears and economic vulnerabilities (Urbas and Choo 2008, 6).

For example, Symantec reports that while the level of financially-oriented spam and phishing remained relatively constant from 2008 to 2009, there was a marked increase in messages advertising the refinancing of debts and mortgages, along with offers of loans and opportunities to earn money while working from home (Symantec 2010, 13). New job opportunities have also emerged within the ever more robust underground economy, such as the role of 'money mule' or 'wire mule,' discussed in subsection 3.0 (Deloitte 2010(a), 6). This demonstrates that cybercrime offenders have readily been able to adapt their techniques to take advantage of current events and significant economic trends.

As David Wall has discussed (Wall 2009), and as previously noted, the emergence of identified patterns and connections between those committing cyber-fraud has raised a number of questions about the relationship between network actors. In particular, cyberspace provides many kinds of criminal actors with a safe haven that also enhances their organizational and operational capabilities. Although a traditional network of organized offending has been considered, there is evidence to indicate that the hierarchical structure does not apply to online networks of cyber-fraud offenders. In other words, it would be hasty to assume such a simplistic understanding of the network structure without an identification of the prevailing structure itself (Morselli 2009).

Methodologically, the most suitable place to begin gathering data is through those who are currently engaged in combating cyber-fraud: law enforcement investigators and IT security professionals. Through the use of telephone interviews, data were collected relating to: the identification of criminal organizations; their membership; how leaders emerge; recruitment techniques; criminal activ

criminal networks rather than single individuals were discussed. The interviews were conducted by telephone for approximately 45 to 60 minutes each.

The process of coding the interview notes was open-ended, whereby the notes were re-read with the understanding that themes corresponding with the interview guide would immediately be apparent (Esterberg 2002). The analysis also revealed additional patterns within the data that might also be considered thematic codes. The interview transcripts were then re-evaluated

Additionally, some organized crime groups reportedly keep the target amount low to ensure that victims will not be inclined to complain and police will not be willing to investigate. Even for larger scams, such as romance scams through online dating sites which often get personal, and sometimes moves off-line, the typical price asked by scammers tends to be in the range of $3,000 to $5,000 (although this depends on the net worth of the victim). Generally speaking, this research shows that the amounts stolen tend to be under $5,000.

Yet, one of the IT personnel stated that for a secondary victim, such as a bank, these losses can add up to as much as $100,000 monthly, or $1.2 million per year. The participants also reported that there are a number of non-monetary harms that result from the cyber-fraud incidents they encountered. When the IT personnel sub-sample commented on the harms it was primarily in terms of administrative expenditures, both for preventing and responding to cyber-fraud occurrences after the fact. For example, one participant noted that there is an expense associated with the activities beyond any initial loss, citing:

> If it's an employee, we call it insider fraud – a different classification. We have systems that forensically track this when it occurs – while it doesn't happen as often...[we] have experienced this in past 12 months. The traditional way is when an insider is approached by an external crime group (i.e. the employee works at the help desk and has access to customers' data).

Given the finding from the IT sample that inside and outside cyber-fraud offenders were commonly dealt with internally whereas reported to the police, it was not particularly surprising that a number of the law enforcement participants reported that, in the case of corporate victims, offenders tend to be outside of the organization. For example, when asked about the location of offenders, one law enforcement participant commented that to the best of his or her knowledge, the offenders were "all outsiders". However, this was also the response given by other IT participants who identified the primary source of cyber-fraud as originating outside the company.

9.2.4 Network Structure and Function

Many of the law enforcement and IT security personnel believed that cyber-fraud incidents in

– individuals and organizations – from the Russian mafia” . Reportedly, the primary means of detecting whether or not the individuals were located outside Canada was the fact that the IP addresses were traced to locations outside Canada. However, other participants indicated that they were under the impression that a criminal

> fake Websites or the purchase/sale of fraudulent goods and services – but it changes from one site to another. The credit card scamming groups are focused on credit cards but when it comes to making counterfeit credit cards, they are not focused on one commodity…they move on whatever the demand is. Also deal in counterfeit currency, fake passports and identification documents – it depends on the commodity. Do participants change? Some groups do, depending on the fraud type. They can have connections with other criminal organizations – but I don't know how they find these groups and make these connections.

Reportedly, when it comes to high-profile hacking and phishing Websites, offenders are often working as part of a team of specialists, each of whom has a defined role within the network. The structure of the network is reportedly goal-oriented. As one interviewee noted, the structure is comprised of "[s]pecialists – one guy does phishing, tries to steal information, then the other guy takes the information to get money – it's a world of specialists. Some are good at creating credit cards, others are good at trying to get money from ATMs". The same participant also noted that the emphasis is on knowledge rather than other resources, commenting that "[s]ometimes they work together to maintain bots, but that doesn't mean they're doing business together – they share knowledge but not necessarily money or criminal activities".

One individual might commit the phishing attack itself, for instance, while another 'specialist' takes the stolen information and creates fraudulent credit cards, which a third 'specialist' then uses at an ATM to steal money from the victims' accounts. This research further shows that, in some cases, these individuals locate each other in chat rooms and Web forums; then, they come together to carry out individual criminal transactions. Furthermore, according to one law enforcement participant:

> [p]eople know each other. Not just online. When online, [they] exchange information on how to better themselves. These folks know each other in real space. We never get to the key player. Most are male between the ages of 20 and 35. A lot are bilingual and some are tri-lingual.

9.2.4 Enforcement Activities

In terms of addressing cyber-fraud, the IT sub-sample reported a trend towards promoting prevention rather than repairing harms after the event. In particular, prevention appeared to be a function of awareness of what is taking place within the business community along with an understanding of the nature and characteristics of cyber-fraud. There appeared to be an acknowledgement that cyber-fraud is very industry-specific and technology is being used to address the problem in a proactive manner. As one participant commented:

> We spend a lot of time on general behavior profiling so you can look at something and see that the customer is expected to behave in a particular way…if it's out of the norm, it becomes something we need to take a look at. We want to make sure people are working within systems and rules…they can

– unless it’s a life or death issue– this is good for protecting people’s privacy but it doesn’t help investigations. Would lawful access help? I don’t know if it would have teeth.

sample; indeed, others fully endorsed a system of mandatory reporting. As one participant commented, the “[the] private sector is blaming law enforcement and law enforcement is saying no reports are being made”.

Like the IT sub-sample, when asked what are the key challenges related to reliably measuring the scope of cyber fraud and the number of associated offenders in Canada, the law enforcement participants reported that lack of education and information sharing are critical. In terms of reporting, there appeared to be awareness among the law enforcement sub-sample that minimal loss is a reason for the under-reporting of cyber-fraud. As one participant noted in relation to the data:

> I think there is…I don’t know…I have no proof of this but I think people tend to file a complaint when there’s a big loss. The number will be higher than expected because people with small losses don’t report to police, just the bank. Mostly the banks refund money, so they don’t need to report to police.

Further, the economic motivations for industry to not report cyber-fraud were identified by one of the law enforcement sub-sample members who noted that, “Perhaps banks are not [reporting cyber-fraud] because they don’t suffer, it doesn’t affect their bottom line” . The same participant also commented on the onus for companies to provide knowledge to the public, commenting that:

> Larger organizations – like ISPs or banks – or even agencies like INTERAC – they could be doing a better job of educating people. I think there could be more public safety alerts (like public service announcements) to remind people that banks don’t send you emails…but so many people fall for phishing or pharming scams and don’t realize big companies don’t do business that way” .

Ultimately, there is a large gap in the data on cyber-fraud and the reason for this was identified by one law enforcement participant who stated that, “About 90% of all fraud data in Canada doesn’t fit in police databases…the banks get reports, some are forwarded to police and some are just handled internally or dropped altogether. Pension and disability fraud is the same; it sits with organizations and doesn’t get reported to police”.

Individual victims are typically either too embarrassed or ashamed, or believe that the loss is not significant enough to justify making a report. As was noted:

> Not everyone files complaints, especially about identity theft – people don’t call or notify police. A lot of the cyber-crime is not reported or is only reported to banks then is not reported to police by banks. They are afraid and want to keep it quiet – they want to ry b85 0 Tw v70 TD .0003 Tc -.0003 Tw (td wavod)negry v public ty

front. There should be more public safety alerts (i.e. public service announcements) to educate people on how not to fall victim to phishing scams.

One of the central frustrations was that cyber-fraud incidents are being reported to many different police organizations in Canada. The RCMP, municipal police forces and provincial police across the country all receive tips relating to cyber-fraud incidents. However, there seems to be little effort to coordinate these tips. Many seem to be kept internally and not reported to an external body. Many municipal police agencies do not report cyber-fraud incidents to the Canadian Anti-Fraud Centre, or any other entity. And, while reports are being made about violent and high-risk offenders through the RCMP, mandatory reporting does not apply in the case of cyber-fraud. Moreover, many law enforcement officials expressed frustration by the way that the statistical information is being recorded in the Uniform Crime Reporting Survey. According to the respondents, there is not enough specificity in the UCR reporting system when it comes to cyber-fraud, and cybercrime, more generally. The figures on cyber-fraud are lumped together under the heading of fraud, and there is no way to determine what type of fraudulent schemes the incidents are linked to. This means that information that could be valuable to better understanding cyber-fraud is being lost.

9.2.6 Suggestions for Data Sources and Solutions to Current Issues

One of the significant trends that emerged from the IT sub-sample supported mandatory reporting of incidents of cyber-fraud and called for a standardized method of data collection. As was noted by one participant, "I think the way government is moving is in the right direction, creating RCMP offices, asking people to report to the RCMP; but more of these efforts are needed. When industry involved in an attack, we have to share information about it and having a federal framework to support this is very useful".

Further, the IT participants reported a need for information sharing within the IT security industry and a desire for government involvement in cyber-crime fighting attempts. This was elaborated upon by the same IT sub-sample participant who suggested that:

> There needs to be a mechanism for the reporting and sharing of information to other members of industry…this would be very useful. There are good models for this elsewhere, like in the nuclear industry and air-traffic control…we need policy and regulations to enforce compliance. It's always easier with a public entity…it's easy to enforce compliance, sharing information, mitigating risks, but banks and telecoms are not in the same position. They are worried about losing customers [in the electrical industry] we have a monopoly on customers. We don't see the same partnerships in the private sector, like banking.

Other participants reported a desire for IT accreditation, standardized reporting models, and government leadership to adopt models used in the United States. As was noted by one of the IT sub-sample members, "We need the Canadian government to step up…we see cybercrime units are being developed in the United States and this would be ideal here. I would be in favour of mandatory reporting legislation…the United States is the one to follow".

with each other and persuading industry to report on what their actual losses are. According to the respondents, there is a great deal of support for mandatory reporting. As one respondent noted:

> I think if companies were mandated to report attacks, that might help - there have been cases of entire servers brought down and nobody knew anything. I think the spam laws that came into force recently (Bill C-28) should help Canadians, but the majority of spam originates from overseas.

According to the law enforcement sub-group, there needs to be a new way that Statistics Canada measures the police data relating to cyber-fraud in the Uniform Crime Reporting Survey (UCR) because the categories do not adequately reflect changes in society and in crime that have occurred over the course of the last decade or so. Currently, within the UCR scoring, there is no way to break down information about fraud by type, such as mass marketing fraud, or 419 scams, so it is not as useful to the police as it could otherwise be.

There was discussion about the creation of a central data hub to record and measure data relating to cyber-fraud across Canada. This entity could also conduct online surveys or polls of Canadians to gather information about cyber-fraud. Currently, the various police agencies across Canada have their own ways of collecting data and keeping track of files, and many do not record complaints alone, preferring only to keep a record if the incident leads to a formal investigation. It would be more effective and efficient to create a centralized agency to collect and compile the data. Police agencies would be assured better communication about police cases. The

identify key players within the group. With the collection of preliminary data into cyber-fraud, the hidden population could be estimated through one of the standardized data estimation techniques discussed above. Of the options available for hidden populations, a truncated Poisson model is a good place to start. This would help mitigate many of the issues confronted by law enforcement that lead to the lack of reporting and the inherent challenges that come with investigating and preventing cyber-fraud offending.

In summary, the following recommendations could be extremely effective toward addressing cyber-fraud in Canada:

- There needs to be more emphasis placed on educating Canadians about how to avoid the scams themselves. The Canadian government, banks and ISPs must take greater responsibility on this front. There should be more public safety alerts (i.e. public service announcements) to educate people on how to not fall victim to phishing scams.
- New initiatives, such as creating an online database of best practices which IT security professional members can add to and view, and/or developing an online community (e.g. to send out advice and tips) and holding best practice information sessions/conferences within specific industry sectors, could be instrumental to proactively responding to cyber-fraud threats, as well as gathering information about current threats and vulnerabilities.
- The Canadian government would benefit from a national strategy for gathering data anonymously from police officers, banks, and private and public entities with respect to cyber-fraud. It is a matter of encouraging police agencies to communicate with each other and persuading industry to report on what thei

- the harmonization of procedural provisions relating to the investigation and prosecution of computer crimes;
- and the establishment of cooperative measures facilitating the exchange of evidence, information and the extradition of suspects (Schjolberg 2008, 1).

x Resources are also needed to ensure that they are equipped to deal with complex inter-jurisdictional fraud cases.

REFERENCES

Albanese, J. S. (2005). "Fraud: The Characteristic Crime of the Twenty-First Century." Trends in Organized Crime 8(4), pp.6-14.

An Act to Amend the Criminal Code (Identity Theft and Related Misconduct) and the Personal Information Protection and Electronic Documents Act. S.C. 2000, c.5.

Begin, N. Dezhkam, N., Etges, R. and Hejazi, W. (2010a) "Managing the risk of social networking: Additional findings and analysis from the 2010 Rotman-TELUS Joint Study on Canadian IT Security Practices." Toronto: Telus Security Solutions.

– – – ., Dezhkam, N., Etges, R. and Hejazi, W. (2010b). "2010 Executive Briefing - Rotman-Telus Joint Study on Canadian IT Security." Toronto: Telus Security Solutions.

Berg, S. (2009). "Identity Theft Causes, Correlates and Factors: A Content An

Crime." Ottawa: CISC.

– – – . (2005). Canadian Centre for Justice Statistics. "A Feasibility Report on Improving the Measurement of Fraud in Canada." Ottawa: Minister of Industry.

Canadian Anti-Fraud Centre. (2010). "Annual Statistical Report 2010 - Mass Marketing Fraud and ID Theft Activities." Available online at: http://www.antifraudcentre-centreantifraude.ca [accessed April 19, 2011].

Canadian Bankers Association (CBA). (2011). "Statistics." Available at: http://www.cba.ca/en/component/ content/publication/69-statistics [accessed April 9, 2011].

Chawki, M. (2009). "Nigeria Tackles Advance Fee Fraud." Journal of Information, Law and Technology 1. Available at: http://go.w

Auerbach Publications.

Hser Y (1993). "Population Estimation of Illicit Drug Users in Los Angeles County." Drug Issues 23:323–334.

Huey, L. and Rosenberg, R.S. (2004). "Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention." Canadian Journal of Criminology and Criminal Justice 46: 597-631.

Identity Theft and Assumption Deterrence Act, Pub. L. No. 105-318, 112 Stat. 3007 (Oct. 30, 1998).

Ipsos Reid, (2009). "CSA Investor Index 2009." Prepared for Canadian Securities Administrators Investor Education Committee. Ottawa: Ipsos Reid.

Kendall, L.W. (1999). "Robustness of Closed Capture-Recapture Methods to Violations of the Closure Assumption." Ecology, 80: 2517–2525

King, A. and Thomas, J. (2009). "You Can't Cheat an Honest Man: Making ($$$ and) Sense of the Nigerian Email Scams" in Crimes of the Internet. Edited by Frank Schmalleger and Michael Pittaro. Upper Saddle River, NJ: Pearson Education Inc.

Kowalski, M. (2002). "Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics." Ottawa: Minister of Industry.

Lee, B., Cho, H., Chae, M., and Shim, S. (2010). "Empirical Analysis of Auction Fraud: Credit Card Phantom Transactions." Expert Systems with Applications, 37: 2991-2999.

Levi, M. and Burrows, J. (2008). "Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey." British Journal of Criminology, 48: 293-318.

– – – . and Fleming, M. H. and Hopkins, M. with the assistance of Matthews, K. (2007). "The Nature, Extent and Economic Impact of Fraud in the UK." Report for the Association of Chief Police Officers' Economic Crime Portfolio. Available at: http://citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.108.8217&rep=rep1&type=pdf. [accessed April 19, 2011].

Li, X. (2007). "International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene." Webology, 4(3):1-45.

McAfee. (2010a). “A Good Decade for Cybercri: McAfee’s Look Back at Ten Years of Cybercrime.” Santa Clara: McAfee Inc.

– – – . (2010b). “2010 Threat Predicti.” Santa Clara: McAfee Inc.

Menn, J. (2010). Fatal System Error – The Hunt for the New Crime Lords Who are Bringing Down the Internet. New York: PublicAffairs.

Microsoft, (2005). “Tool Thwarts Online Predators.” Available at: http://www.microsoft.com /presspass/features/2005/apr05/04-14CETS.mspx [accessed April 7, 2011].

Morselli, C., Gabor, T., and Kiedrowski, J. (2010). “Factors That Shape Organized Crime,” prepared for Research and National Coordination Organized Crime Division, Law Enforcement and Policy Branch, Public Safety Canada.

Morselli, C. (2009). Inside Criminal Networks. New York: Springer.

OECD Guidelines for the Security of Informati

Geneva". Available at: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf. [accessed April 19, 2011].

Schwarz, C. J., and Seber, G. A. F. (1999). A Review of Estimating Animal Abundance. III. Statistical Science, 14:427-456.

Sheehan, K.B. and M.G. Hoy, (2000). "Dimensions of Privacy Concern Among Online Consumers." Journal of Public Policy and Marketing, 19(1):63-73.

Smit, F., Toet, J., and van der Heijden, P. (1997). "Testing the Number of Opiate Users in Rotterdam Using Statistical Models for Incomplete Count Data." European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), 1997 Methodological Pilot Study of Local Prevalence Estimates. EMCDDA, Lisbon.

Smith, R. G. (2008). "Coordinating Individual and Organizational Responses to Fraud." Crime, Law and Social Change, 49:379-396.

– – – . and Gregor Urbas. (2001). "Controlling Fraud on the Internet: A CAPA Perspective: Report for the Confederation of Asian and Pacific Accountants." Research and Public Policy Series No. 39." Canberra: Australian Institute of Criminology.

Spam Act 2003. Act No. 129 of 2003, as amended.

Spiekermann, S., Grossklags, J., and Berendt, B. (2002). "E-privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior," Proceedings of the Third AMC Conference on Electronic Commerce, 38-47.

Stroik, A. and Huang, W., (2009). "Nature and Distribution of Phishing," in Crimes of the Internet. Edited by Frank Schmalleger and Michael Pittaro. Upper Saddle River, NJ: Pearson Education Inc.

Zambo, S. (2007). “Digital La Costa Nostra: The