Catalogue no. 85-558-XIE

Cyber-Crime:
Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics

Canadian Centre for Justice Statistics

Statistics Canada Statistique Canada

Canada

How to obtain more information

Specific inquiries about this product and related statistics or services should be directed to: Canadian Centre for Justice Statistics, Toll free 1 800 387-2231 or (613) 951-9023, Statistics Canada, Ottawa, Ontario, K1A 0T6.

For information on the wide range of data available from Statistics Canada, you can contact us by calling one of our toll-free numbers. You can also contact us by e-mail or by visiting our Web site.

National inquiries line	**1 800 263-1136**
National telecommunications device for the hearing impaired	**1 800 363-7629**
Depository Services Program inquiries	**1 800 700-1033**
Fax line for Depository Services Program	**1 800 889-9734**
E-mail inquiries	**infostats@statcan.ca**
Web site	**www.statcan.ca**

Ordering and subscription information

This product, Catalogue no. 85-558-XIE, is available on Internet free. Users can obtain single issues at www.statcan.ca.

Standards of service to the public

Statistics Canada is committed to serving its clients in a prompt, reliable and courteous manner and in the official language of their choice. To this end, the Agency has developed standards of service which its employees observe in serving its clients. To obtain a copy of these service standards, please contact Statistics Canada toll free at 1 800 263-1136.

Statistics Canada
Canadian Centre for Justice Statistics

Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics

Prepared by: Melanie Kowalski

Published by authority of the Minister responsible for Statistics Canada

December 2002

Catalogue no. 85-558-XIE
ISBN 0-660-33200-8

Frequency: Occasional

Ottawa

La version française de cette publication est disponible sur demande (Catalogue nº 85-558-XIF).

Note of appreciation

Canada owes the success of its statistical system to a long-standing partnership between Statistics Canada, the citizens of Canada, its businesses, governments and other institutions. Accurate and timely statistical information could not be produced without their continued cooperation and goodwill.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cyber-crime is generally defined as a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence. This report provides a preliminary look into the issues, data sources, and feasibility of collecting police-reported cyber-crime statistics. Options for the development of ongoing data collection and the nature and extent of cyber-crime activity in Canada are explored through this study.

Countries around the world are currently looking at ways to ensure that these activities are properly investigated and reported. For example, the UCR National Incident Based Reporting System (NIBRS) in the United States includes a category that flags computer-related crimes. The NIBRS provides the capability to indicate whether a computer was the object of the crime and to indicate whether the offenders used computer equipment to perpetrate a crime.

Similar to research findings, consultations with Canadian police indicated that a uniform definition of cyber-crime has not been established among the police community. Of the 11 major police forces consulted, 8 have a specialized unit that is responsible for investigating cyber-crimes and have developed definitions, policies and procedures to assist in the investigation. Of these eight police forces, six have a system in place that collects data or information on cyber-crime activity. The police forces that did not currently collect this information stated that putting a data collection procedure in place would not result in significant respondent burden.

As a result of the consultations with police, two options have been identified for the future collection of data on cyber-crime from police services in Canada. The first option is to conduct a special study to collect detailed information from police agencies that currently collect cyber-crime statistics. The second option is to modify the Incident-based Crime Statistics (UCR2) Survey. This option would include adding a data element that identifies criminal offences involving a computer as the object or as the tool used to commit the crime. Both options are recommended to address the short-term and long-term data needs of law enforcement agencies, policymakers and legislators.

ACKNOWLEDGEMENTS

The Canadian Centre for Justice Statistics (CCJS) appreciates the assistance and support of the Police Information and Statistics (POLIS) Committee of the Canadian Association of Chiefs of Police and the co-operation of various Canadian police agencies that participated in the consultation process.

INTRODUCTION

Cyber-crime is a national and international concern that is having a serious impact on law enforcement at all levels. Cyber-crime has recently received increased attention from federal, provincial and territorial governments, as well as the police community. To date, there are no national data on this important issue. This study examines the feasibility of collecting police-reported cyber-crime statistics by examining different methods currently being used in the United States and the United Kingdom in addition to methods that selected police forces in Canada use to gather and store information on cyber-crime activity. The report examines definitions of cyber-crime, current legislation in Canada and other countries, existing data, results from consultations with selected police forces and, finally, options for collecting cyber-crime data from police agencies.

PART I – WHAT IS CYBER-CRIME?

To date, no single definition of cyber-crime has emerged that the majority of police departments use. The following working definition has increasingly been accepted by Canadian law enforcement agencies: "*a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence.*"[1]

Generally speaking, based on the definition created by the Canadian Police College and by other research sources (Carter: 1995; Davis and Hutchison: 1997), there are two broad categories of cyber-crime. The first category is defined where the computer is the tool of the crime. This category includes crimes that law enforcement has been fighting in the physical world but now is seeing with increasing frequency on the Internet. Some of these crimes include child pornography, criminal harassment, fraud, intellectual property violations and the sale of illegal substances and goods.

The second category is defined where the computer is the object of the crime. Cyber-crime consists of specific crimes dealing with computers and networks. These are new crimes that are specifically related to computer technology and the Internet. For example, hacking or unauthorized use of computer systems, defacing websites, creation and malicious dissemination of computer viruses.

In addition to cyber-crime, there is also “computer-supported crime” which covers the use of computers by criminals for communication and document or data storage. This type of crime is not included in the definition of cyber-crime used in this report.

The terms “computer crime”, “computer-related crime”, “high-tech crime”, “cyber-crime” and “Internet crime” are often used interchangeably when police and other information sources are discussed.

[1] *This definition is offered at the Canadian Police College, where Canadian police officers undergo training in computer crime investigative techniques.*

PART II – CANADIAN CYBER-CRIME LEGISLATION

One of the challenges currently faced by legal authorities is the difficulty of applying existing legislation to criminal activities involving new technologies. As a result of recent commitments made by the Council of Europe *Convention on Cyber-Crime*, efforts will be made to provide common international definitions of certain criminal offences relating to the use of new technologies (see Part III for more information on the *Convention on Cyber-Crime*).

Canada was one of the first countries to enact criminal laws in the area of computer crime (Convention on Cyber-Crime: 2001). According to a study by a United Nations-sponsored network of Internet policy officials, Canada is ahead of nearly two-thirds of the 52 countries surveyed in enacting laws to crack down on cyber-crimes (Chu: 2000). The 1985 amendments to the *Criminal Code* introduced into law what was at the time generally considered to be a comprehensive group of amendments directed at computer crime. These amendments included section 342.1 (unauthorized use of computer), section 430.(1.1) (mischief in relation to data), section 327 (possession of device to obtain telecommunication facility or service) and section 326 (theft of telecommunication service). In 1997, the *Criminal Law Improvement Act* made various amendments to the *Criminal Code,* including section 342.2 (possession of device to obtain computer service).

In some cases, traditional crimes have simply adapted to new technology and, the criminal justice system, in response, must make a similar adaptation. In addition, Canada has developed laws to successfully prosecute "other" computer-related crimes, such as computer fraud and computer forgery. In other cases, minor revisions to legislation have been required to ensure that offences are defined in a way that captures the new technological aspects of the crime and that the necessary law enforcement responses are permitted. For example, it is already illegal in Canada to possess child pornography, but revisions were made to legislation to make it illegal to download and view child pornography online.

Bill C-15A, which received Royal Assent on June 10, 2002, includes amendments to Canada's child pornography provisions that address the proliferation of that material on the Internet and similar advanced communications technologies. This Bill creates offences of transmitting, making available and accessing child pornography. It also creates an offence for the purpose of facilitating an offence against a child. The Bill also gives Canadian judges the power to ban Canada-based child pornography sites and to order the forfeiture of materials or computers used in the crime.

Bill C*15A*

Legislation to better protect children from sexual exploitation:

- Creates a new offence that targets criminals who use the Internet to lure and exploit children for sexual purposes;
- Makes it a crime to transmit, make available, export and intentionally access child pornography on the Internet;
- Allows judges to order the forfeiture of any materials or equipment used in the commission of a child pornography offence;
- Enhances the ability of judges to keep known sex offenders away from children by making prohibition orders, long-term offender designations and one-year peace bonds available for offences relating to child pornography and the Internet; and,
- Amends the child sex tourism law enacted in 1997 to simplify the process to prosecute Canadians who sexually assault children in other countries.

Source: *Department of Justice Canada: 2002*

PART III – ACTIVITIES TO ADDRESS CYBER-CRIME IN THE UNITIED STATES, THE UNITED KINGDOM AND CANADA

The Internet is now available in over 200 countries and because of its "borderless" nature, crimes may be committed through communications that are routed through a number of different countries (President's Working Group on Unlawful Conduct on the Internet: 2000). One of the biggest challenges of cyber-crime is that a criminal can commit a crime from any country in the world; can target victims all over the globe; hide his/her identify by transmitting communications through computer systems located in many foreign countries; and, store evidence in remote locations. The ability to trace communications through different computer networks in different jurisdictions is a critical element in preventing, investigating and prosecuting cyber-crime (Federal/Provincial/Territorial Working Group on Illegal and Offensive Content of the Internet: 2001). Thus, it is not surprising that initiatives for combating cyber-crime largely rely on international cooperation.

The first comprehensive international effort to deal with computer crime problems was initiated by the Organization for Economic Co-operation and Development during the 1970's. Considerable effort went into determining what was meant by "computer crime" and towards developing guidelines to promote harmonization of international computer crime laws. It was recognized that international harmonization was necessary in order to have effective enforcement of what is largely an international crime.

Most recently in 2001, Canada and 29 other countries signed the Council of Europe *Convention on Cyber-Crime*, but most, including Canada, still have not ratified this first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks (Convention on Cyber-Crime: 2001). The *Convention on Cyber-Crime* will require parties to establish laws against cyber-crime, to ensure that their law enforcement officials have the necessary procedural authorities to investigate and prosecute cyber-crime offences effectively, and to provide international cooperation to other parties in the fight against computer-related crime.

The *Convention on Cyber-Crime* is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Furthermore, the efforts of the G7 and G8 since 1996 illustrate the commitment of the international community to address multi-jurisdictional issues related to cyber-crime. For example, the High-Tech Crime Subgroup within the Lyon Group (formerly the Experts Group on Transnational Organized Crime) examines international technological issues. The Group is working together to build cooperation in combating computer crime across national borders.

At the G8 Justice and Interior Ministers' meeting held at Mont Tremblant in May 2002, the Ministers endorsed revised G8 Recommendations on Transnational Crime; Recommendations on Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations; as well as a number of other documents that would help governments to combat high-tech crime.

United States

The United States began to respond to the cyber-crime problem in 1984 when it enacted its first law, the *Computer Fraud and Abuse Act* (18 U.S.C. 1030), directly targeting attacks on computer systems. In 1991, the Department of Justice created a specialized unit to address computer issues. The Computer Crime and Intellectual Property Section evaluates

computer crime problems, offers legislative and policy proposals to address these problems and prosecutes those who violate the law.

In 2001, the U.S. Department of Justice proposed creating nine specialized prosecutorial units that would be dedicated to fighting cyber-crime. The new teams will be called Computer Hacking and Intellectual Property Units and will focus on high-technology crimes including computer intrusions and hackings; theft of computers and high-tech components; fraud, copyright and trademark violations; and, theft of trade secrets and economic espionage. To date, five units are currently operating in the U.S.

The Federal Bureau of Investigation (FBI) has also taken a number of steps to address cyber-crime. The National Infrastructure Protection Center was created in February 1998 by the FBI and was given a mission to detect, assess, and investigate significant threats and incidents concerning intrusion of critical infrastructures. During the course of such investigations, it was increasingly found that the intrusion was merely the first step in a more traditional criminal scheme involving fraud or other financial gain (Kubic: 2001). This has been the case in numerous incidents involving computer intrusions into the databases of credit card companies, financial institutions, online businesses, etc. to obtain credit card or other identification information for individuals. This information is then used in schemes to defraud individuals and/or businesses. In addition, the FBI continues to develop and operate cyber-crime task forces consisting of investigators and resources from other federal agencies as well as state and local agencies. The United States has also actively participated in the area of cyber-crime at the G8 Justice and Interior Ministers' meetings and at the Council of Europe *Convention on Cyber-Crime* meeting.

United Kingdom

In June 1999, an Internet Crime Forum was formed in the United Kingdom (UK), bringing together representatives from government, law enforcement and the Internet industry. Its overall aim is "to develop and maintain a working relationship between the Internet Service Providers Industry and Law Enforcement Agencies in the UK, such that criminal investigations are carried out lawfully, quickly and efficiently while protecting the confidentiality of legitimate communications and with minimum impact on the business of the industry." (The Internet Crime Forum: March 2001).

In addition to issues identified by the Forum, a national hi-tech strategy was drawn up which included a strategic threat assessment (Project Trawler) published in 1999 by the National Criminal Intelligence Service. Project Trawler identified significant gaps in investigative capability at both local and national levels and informed policymakers of the potential threat of high-tech crime. In response to the gaps, the first National Hi-Tech Crime Unit became operational in April 2001.

Internet content hotlines, such as the Internet Watch Foundation in the UK, have been established as an effective mechanism for dealing with complaints about the content of the World Wide Web and in Usenet newsgroups. These hotlines will also establish a contact system with overseas police forces in accordance with the UK's commitments at the G8 Justice and Interior Ministers' meeting at Mont Tremblant in May 2002, and as a result of the UK's work at the Council of Europe *Convention on Cyber-Crime* meeting in November 2001.

Canada

Canada is an active participant in a number of international organizations such as the G8 Group of Senior Experts on Transnational Organized Crime, the Committee of Experts on Crime in Cyberspace of the Council of Europe and the Organization of American States Group of Government Experts on Cyber-Crime.

The Government of Canada hosts global summits, conducts international studies and has helped draft the Council of Europe *Convention on Cyber-Crime*. The Canadian Association of Internet Providers is sharing information with European Internet service providers and working with other countries to develop international solutions.

Similar to the US's Infrastructure protection program, the Office of the Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) was created by the federal government in 2001. OCIPEP provides national leadership to help ensure the protection of Canada's critical infrastructure – in both its physical and cyber dimensions – regardless of the

source of threats and vulnerabilities. OCIPEP works with various departments, especially Solicitor General Canada, to develop a comprehensive approach to protecting our critical infrastructure and responding to incidents.

There are a number of other major national initiatives in place that address concerns regarding offensive and illegal content on the Internet. In 1997, a Federal-Provincial-Territorial Working Group on Offensive Content on the Internet was established to examine issues relating to the unlawful use of new communications technologies, particularly the Internet and its role in the distribution of offensive content such as child pornography, obscenity and hate propaganda. As part of this initiative, the Working Group in Cyber-Crime has given its attention to Internet luring which, in some forms, could be considered a criminal activity and to communication with children for purposes of sexual exploitation. This Working Group's primary focus is on the criminal law issues associated with new technologies, such as providing law enforcement with the proper tools and legislative framework to combat cyber-crime – especially online child pornography.

A federal interdepartmental strategy, entitled *"Canadian Strategy to Promote Safe, Wise and Responsible Internet Use"* presents an end-user model to address illegal activities on the Internet. Its goal is to educate Canadians about illegal and offensive content on the Internet, and empower them to take action in their homes. In addition, this strategy has led the Government of Canada and the private sector to examine the costs and benefits of establishing a Canadian hotline to report illegal Internet content.

The Federal-Provincial-Territorial Consumer Measures Committee has established an Electronic Commerce Working Group with a mandate to examine consumer issues related to e-commerce and to develop options with respect to consumer education, industry self-regulation and consumer-protection legislation.

PART IV – DATA COLLECTION EFFORTS IN THE UNITED STATES, THE UNITED KINGDOM AND CANADA

United States

Some national data collection methods on computer-related crime in the United States include:

(1) Uniform Crime Reporting (UCR) National Incident Based Reporting System;
(2) National Victimization Survey;
(3) Computer Crime and Security Survey;
(4) Internet Fraud Complaint Center; and,
(5) Other Planned Programs.

1. UCR National Incident Based Reporting System:

The UCR National Incident Based Reporting System (NIBRS) collects incident and arrest-level crime data maintained in law enforcement records (similar to Canada's UCR2 survey). The NIBRS includes a category that captures data on computer crime incidents.

It is the national UCR Program's position that computer crime actually involves historical offences such as larceny, embezzlement, and trespassing, which are being perpetrated through the use of a new tool, the computer. If larcenies, embezzlements, and trespasses relating to computers were to be reported under a new classification called 'Computer Crime', the national UCR Program's traditional time series relating to such crimes would be distorted.

To avoid such a result, NIBRS provides the capability to indicate whether a computer was the object of the crime and to indicate whether the offender(s) used computer equipment to perpetrate a crime (see text box "NIBRS and computer crime"). This data element should be used to indicate whether any of the offenders in the incident were suspected of using a computer, computer terminal, or other computer equipment to perpetrate the crime (see Appendix A for the Incident Reporting Form).

NIBRS and computer crime:

The NIBRS provides the capability to indicate whether a computer was the object of the crime and whether the offenders used computer equipment to perpetrate a crime.

1. Where the computer was the object of the crime:

Data Element 15 –**PROPERTY DESCRIPTION**- enter 07= Computer Hardware/Software- defined as computers, computer peripherals, eg., tape and disk drivers, printers; and storage media i.e., magnetic tapes, magnetic and optical disks, etc.

2. Where the offender used computer equipment to perpetrate the crime:

Data Element 8 –**OFFENDERS SUSPECTED OF USING**- enter C= Computer Equipment

For example (1) A computer hacker used his personal computer and a telephone modem to gain access to a company's computer and steal proprietary data. C = Computer Equipment should be entered. (2) A private residence was burglarized and a personal computer was stolen, along with other items. C = Computer Equipment should not be entered because, even though the computer was one of the fruits of the crime, it was not used to commit the crime.

Source: *Federal Bureau of Investigation: 2000.*

In 2000, of the 45,950 computer crimes reported by the NIBRS[2], 5,744 were crimes where the computer was the tool and 40,211 were crimes where the computer was the object. The most common type of computer crime for both definitions was larceny/theft. Table 1 provides a breakdown of offences reported through the NIBRS in which the offender was suspected of using a computer to commit the offence and where the computer was the object of the crime.

Table 1
Computer Crime Offences by Type, 2000, United States[1]

	Computer was:	
	Tool	Object
Assault Offences	878	282
Sex offences, forcible	73	15
Kidnapping/Abduction	12	32
Sex offences, non-forcible	5	0
Murder & Non-negligent Manslaughter	0	1
Crimes Against the Person	**968**	**330**
Drug/Narcotic Offences	605	606
Weapon Law violations	36	52
Pornography/Obscene Material	108	1
Gambling offences	6	4
Prostitution Offences	9	0
Crimes Against Society	**764**	**663**
Larceny/Theft Offences	1,589	19,950
Destruction/Damage/Vandalism of Property	485	2,990
Burglary/Breaking and Entering	373	14,174
Fraud Offences	756	595
Counterfeiting/Forgery	525	293
Motor Vehicle Theft	110	386
Embezzlement	84	277
Robbery	37	220
Stolen Property Offences	31	283
Arson	10	39
Extortion/Blackmail	7	10
Bribery	5	1
Crimes Against Property	**4,012**	**39,218**
Total	**5,744**	**40,211**

[1] *69 agencies submitted data where an offender was suspected of using computer equipment to commit a crime. 102 agencies submitted data where computer hardware/software was the object of the crime in 2000. The NIBRS represents 13% of police agencies in the United States accounting for 16% of the US population.*

Source: *National Incident Based Reported System, Federal Bureau of Investigation, U.S. Department of Justice.*

2. National Victimization Survey:

Victimization surveys are another method used to capture information on criminal offences and incidents. Through the Bureau of Justice Statistics, the U.S. Department of Justices' National Crime Victimization Survey (NCVS) captures information on crimes experienced by individuals and households and whether or not these crimes were reported to the police. In its 2001 incident report, the NCVS for the first time asked questions on computer crime. These included questions on computer use and experience with computer-related incidents (see Appendix B for details). Once available, these results will provide more information about the nature of crime being committed via the Internet.

[2] *In 2000, NIBRS represented 13% of police agencies in the United States, accounting for 16% of the US population.*

3. Computer Crime and Security Survey:

The annual "Computer Crime and Security Survey" is conducted as a public service by the Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation Computer Intrusion Squad. The aim of this effort is to help raise the level of security awareness as well as to assist in determining the scope of computer crime in the U.S. The work focuses on the extent and types of computer crime and summarizes the financial estimates of loss from respondents willing to do so. Results from the 2001 survey indicate that 91% of large U.S. corporations and government agencies (based on responses from 538 computer security practitioners) detected computer security breaches within the past year (Power: 2001)

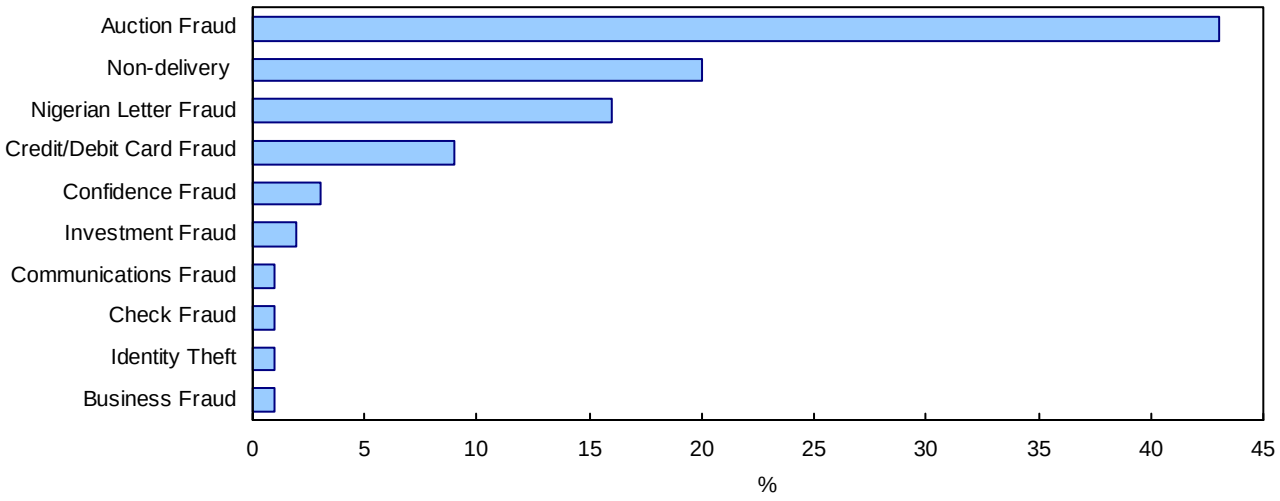
4. Internet Fraud Complaint Center:

In May 2000, the Internet Fraud Complaint Center (IFCC), created by the FBI, and the national White Collar Crime Center (a non-profit organization funded by Congress) went online. The IFCC offers a central repository for complaints related to Internet fraud and uses the information to quantify fraud patterns and provide timely statistical data of current fraud trends (see text box for a description of major types of Internet fraud being reported).

In 2001, the IFCC website received 49,711 complaints, including computer intrusions, unsolicited e-mail and child pornography. Internet auction fraud was the most common reported offence, comprising 43% of referred complaints (see Figure 1).

Figure 1

Most Common Internet Fraud Complaints Reported, USA, 2000



Source: *Internet Fraud Complaint Center, 2001.*

Major Types of Internet Fraud Reported to IFCC

Auction and Retail Schemes Online – These schemes induce their victims to send money for promised items, but then deliver nothing or only an item far less valuable than what was promised (e.g., counterfeit or altered goods).

Business Opportunity/'work-at-home' Schemes Online – These schemes typically require an individual to pay but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business.

Confidence Fraud – The reliance on another's discretion and/or breach in a relationship of trust resulting in financial loss.

Identity Theft and Fraud – the wrongful obtaining and using of someone else's personal data in some way that involves fraud or deception, typically for economic gain.

Investment Schemes Online – deceptive practices involving the use of capital either through income-producing vehicles or through more risk-oriented ventures designed to result in capital gains.

Credit Card Schemes – unlawfully obtained credit card numbers to order goods or services online.

Source: *Internet Fraud Complaint Center: 2001*

5. Other Planned Programs:

In addition to the data sources described above, in 2000, the Bureau of Justice Statistics (BJS) began strategizing the development of a statistical program to measure changes in the incidence, magnitude, and consequences of electronic or cyber-crime. It has been proposed that these statistics will include data on both personal and property crimes, ranging from e-mail threats and harassment to illegal use of or access to networks to commit fraud or theft (Bureau of Justice Statistics: 2002). The BJS and the Census Bureau, as well as representatives from businesses and universities, will explore issues and design an agenda for the collection of cyber-crime statistics.

Currently, the Census Bureau is conducting a pilot survey of businesses with respect to computer-related crime. If successful, the actual survey of about 36,000 businesses will commence in the Fall 2003 to measure the nature and extent of computer-related crime against businesses. The survey will obtain information on the frequency and types of computer crime, the cost of computer security, and the economic losses sustained (U.S. Census Bureau: 2002).

United Kingdom

The primary method used to collect data on crime committed on the Internet is the British Crime (victimization) Survey (BCS). The BCS measures the amount of crime in England and Wales by asking people about crimes they have experienced in the last year. In its 2001 survey the BCS added the following questions addressing:

- Credit card use; where do people use credit cards? (including Internet)
- How worried are people about each of the places where they use credit cards?
- Credit/ bank card fraud
- Use of Internet to purchase goods
- Precautions when buying goods on the Internet
- Worry about virus attacks, someone accessing files without permission (home/work)
- Experience of virus attacks
- Worry about being sent offensive pornographic material over the Internet without consent
- Receipt of offensive pornographic material

Once available, this information will provide further insight into cyber-crime activity in the UK.

Another method the UK uses to report illegal Internet material is through the Internet Watch Foundation (IWF). The IWF assesses the material reported by the public and then notifies the service provider and the police. The IWF has a specific mandate to deal with child pornography, adult material that would break the Obscene Publication Act, and criminal racist

material. The most recent statistics show that in 1999, 19,710 items were reported through the IWF, almost all being child pornography (99%).

Canada

Canada presently does not have a uniform method of collecting data on cyber-crime activity. Although limited, the Incident-based Uniform Crime Reporting (UCR2.1 version) Survey and the Adult Criminal Court Survey, provide data on the few *Criminal Code* offences related to cyber-crime. Statistics Canada's household surveys and a federally-funded study conducted by the Media Awareness Network – 'Canada's Children in a Wired World Survey' – and prepared by Environics Research Group examine Internet use patterns among Canadian families.

1. 2000 General Social Survey:

The 2000 General Social Survey (GSS)[3] collected detailed information on individual use of technology. Although not designed to specifically capture information on cyber-crime activity, the 2000 GSS collected information on offensive content and security issues relating to the Internet (see Appendix C 'Measuring Cyber-Crime through the GSS').

In 2000, 53% of Canadians 15 years of age and over said they used the Internet at home, work or somewhere else in the last 12 months, a dramatic increase since 1994 (18%) (Statistics Canada: March 2001).

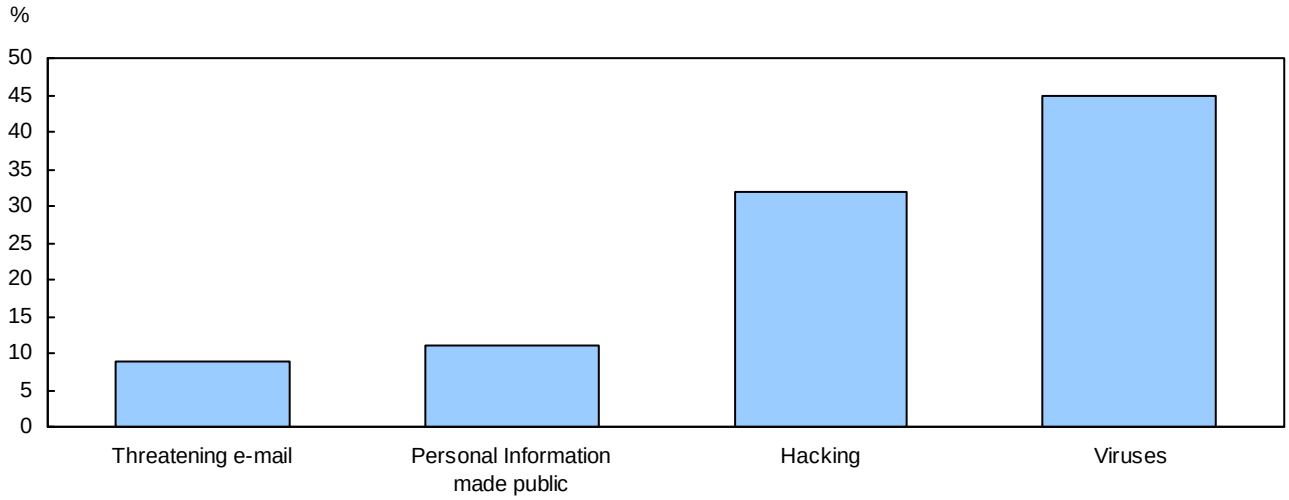
Offensive content, including the collection and distribution of obscene, hate material and pornography continues to pose a concern for criminal justice officials in addition to parents of young children. Highlights from results of the 2000 GSS indicate that:

- 6% of parents reported that their child came across offensive content on the Internet.
- Half (49%) of Canadians have come across websites that contain pornography. Of those that have come across pornographic websites, 83% came across it unexpectedly and 46% found it offensive.
- 13% of Internet users came across content that promotes hate or violence to a particular group.
- 8% of Canadians who used the Internet had received threatening or harassing e-mail.

[3] *The GSS is an annual telephone sample survey covering the non-institutionalized population aged 15 and over in all provinces. The GSS related to technology is conducted every five years. Data were collected over a 12-month period from January to December 2000. The representative sample had 25,090 respondents, representing an 81% response rate.*

Figure 2

Problems Associated with Security on the Internet, Canada, 2000



Source: *General Social Survey, Cycle 14, 2000.*

According to results from the GSS, 5% of Canadians that used the Internet in the past year experienced problems associated with security. Forty-five percent of respondents indicated problems with a virus, 32% reported someone hacking into their e-mail accounts or computer files, 11% said their personal information was made public and 9% indicated receiving threatening e-mail (see Figure 2) (refer to question 4 in Appendix C 'Measuring Cyber-crime through the GSS).

2. Household Internet Use Survey:

This Statistics Canada survey asks about Internet use by Canadian households and is administered to a sub-sample of households included in the Labour Force Survey. The most recent data from this survey showed that Internet use by a household member from one location or another (e.g. home, work, school, etc.) increased from 51% in 2000 to 60% in 2001. These persons are accessing the Internet more frequently and they are staying on-line longer even though privacy is still a concern for the majority of respondents. Close to 60% of Internet users expressed concern about privacy on the Internet. Respondents indicating regular use from home reported that they were concerned about content that may be viewed by children in the household, particularly pornography (80%) (Statistics Canada: July 2002).

3. Canada's Children in a Wired World: The Parents' View

The national survey - Canada's Children in a Wired World - conducted in 2000 by the Media Awareness Network, and funded by Industry Canada in partnership with Health Canada and Human Resources Development Canada, found that 51% of online parents indicated that the biggest concern in terms of their child's Internet use was exposure to inappropriate material (including pornography, violence and hate sites). A further 18% of the parents reported they were most concerned about interactive communications, such as Internet chat, and 23% of parents reported no concerns at all (Media Awareness Network and Environics Research Group: 2000).

4. Adult Criminal Courts Survey (ACCS):

The ACCS collects data on disposed federal statute charges in provincial and territorial adult criminal and superior courts. The data represent seven provinces and one territory and account for 80% of the national adult court caseload. To date, the technology-specific offences that are presently in the *Criminal Code* include (see legislation for more detail):

– unauthorized use of computer - section 342.1
– possession of device to obtain computer service - section 342.2
– possession of device to obtain telecommunication facility or service - section 327
– mischief in relation to data - section 430.(1.1)
– theft of telecommunication service - section 326

Table 2 reveals that there is no consistent trend among any of these five offences between 1995 and 2001. Possession of a device to obtain a telecommunication facility or service and theft of telecommunication service are more predominant than the other technology-specific offences.

Table 2
Technology-Specific Offences[1], Number of Charges, Canada, 1995/96 to 2000/01

Criminal Code Offence	1995/96	1996/97	1997/98	1998/99	1999/00	2000/01
Mischief in relation to data - C.C.430.(1.1)	64	19	61	20	15	16
Theft of telecommunication service - C.C.326	433	443	520	396	301	270
Possession of device to obtain telecommunication facility or service - C.C.327	357	220	262	238	599	133
Unauthorized use of computer - C.C.342.1	25	26	57	113	43	58

[1] *There were no charges reported for possession of a device to obtain computer services (C.C.342.2) for 1995/96 through to 2000/01.*

Note: *Adult Criminal Court Survey data are from 7 provinces and one territory representing 80% of the national adult court caseload.*

Source: *Adult Criminal Court Survey, Canadian Centre for Justice Statistics Canada.*

5. Incident-based Uniform Crime Reporting (UCR2) Survey:

There are currently two versions of the incident-based UCR2 survey. Only the most recent version (UCR2.1) includes a data element "type of fraud" for recording any fraud that involves the unauthorized use of a computer or use of a computer for illegal means. In 2001, 32 forces were providing data to the UCR 2.1 survey representing 27% of the national volume of crime. These 32 police forces reported 100 incidents of computer-related fraud in 2001. Some examples include hacking, illegal use of user ID or personal password.

As in the case of NIBRS, the specific sections of the *Criminal Code* related to technology-specific offences (see ACCS section above) are grouped with traditional offences such as fraud and theft. The NIBRS provides a good basis for a similar method to be adopted by the UCR2 survey to collect cyber-crime statistics.

6. PhoneBusters National Call Centre

PhoneBusters was established in January 1993 by the Ontario Provincial Police (OPP) Rackets Branch to collect telemarketing fraud complaints, share evidence with other enforcement agencies and educate the public about telemarketing scams. In June 2001, PhoneBusters became national in scope with the participation of the Royal Canadian Mounted Police (RCMP). This joint venture enables the collection and analysis of data to identify national trends and provide assistance in investigating telemarketing crime both nationally and internationally (Royal Canadian Mounted Police: June 2001).

7. Cybertip.ca

In September 2002, the Government of Canada funded Child Find Manitoba to support Cybertip.ca, a hotline and website to help prevent online sexual exploitation of children. The website allows the public to report potentially illegal content and activities on the Internet, such as child pornography and luring, through an online reporting form. The information is analyzed and then referred to the appropriate law enforcement agencies as required (Canada Newswire: 2002).

PART V – RESULTS FROM CONSULTATIONS WITH POLICE

Police Definitions, Policies and Procedures Regarding Cyber-Crime

In Canada, there is no national mandate requiring police departments to keep track of the number of offences that have been committed with the aid of the Internet/computer. However, some police departments voluntarily do so.

In order to identify information needs as well as the feasibility of collecting cyber-crime statistics from police, the CCJS contacted 11 major police agencies in Canada during 2002:

1. Halifax Police
2. Montreal Urban Community (MUC) Police
3. Sûreté du Quebec (SQ)
4. Ottawa Police
5. Royal Canadian Mounted Police (RCMP)
6. Ontario Provincial Police (OPP)
7. Toronto Police
8. Winnipeg Police
9. Edmonton Police
10. Calgary Police
11. Vancouver Police

Overall findings:

One issue in gathering data on cyber-crime from police is that there is no consistent definition of cyber-crime: five police forces have implemented a formal definition, three had an informal definition and three did not have any definition.

The lack of a standard definition among police makes it difficult to ensure that cyber-crime statistics are collected in a consistent fashion. The core problem is that many police forces make no distinction of whether the crime committed was via the Internet or simply computer-related.

Table 3
Summary of Police Responses

Police Department	Specialized Unit	Policy/Procedures	Definition	Data
Halifax	√	√ Informal	√ Formal	√
MUC	√	√ Informal	√ Informal	√
SQ	√	√ Formal	√ Formal	√
Ottawa	√	√ Informal	√ Informal	√
RCMP	√	√ Formal	√ Formal	√
OPP	√	√ Informal	√ Informal	√
Toronto	√	√ Informal	No	No
Winnipeg	No	No	No	No
Edmonton	No	No	No	No
Calgary	No	No	√ Formal	No
Vancouver	√	√ Informal	√ Formal	No

Most specialized high-tech units investigate only cyber-crimes where the computer is the target of the crime. Where cyber-crime is classified as the computer being the tool, other units will take charge. For example, if an Internet fraud is committed, the Fraud Unit will be responsible for the case. The High-Tech Unit's responsibility would be to provide assistance if needed.

Although some respondents have policies and procedures concerning cyber-crime, most used informal procedures with no specific guidelines. Of the 11 police forces, the RCMP and the SQ were the only police forces that had implemented formal policies and procedures.

Of the eight police forces having units that investigate cyber-crime, six collect, store and compile this information. This information is stored in electronic format within their information systems specifically designed for intelligence gathering and analysis. Most of these forces indicated that a separate element was added to their records management system to indicate whether or not an offence involved the aid of a computer/Internet. Among the police forces that were able to provide data, the most common offences being committed with the use of a computer were fraud, child pornography, threats and harassment.

Many of the forces currently not reporting this information stated that it would be feasible to add a component to their records management system to capture this information and that the procedure would not produce significant respondent burden. Therefore, it appears that there is potential for future data collection.

Findings from individual forces:

Note: Edmonton and Winnipeg police force do not have a unit that specifically investigates cyber-crime.

1. Halifax Police

The Halifax police department defines cyber-crime as: "any communication which attempts or completes a criminal offence, sent or received by means of a computer." The department investigates cyber-crime through the General Investigation Section, with the exception of child pornography cases. Within the General Investigation Section four persons are trained to deal with Internet-related crime issues. In addition, the Computer Forensics Unit within the Technical Support Section work on a number of files including computer hacking, Internet prostitution and pornography, frauds, threats and child pornography.

Although no formal policy is in place, Halifax police determine whether an incident is a computer-related crime if communications were sent, posted or received by way of a computer system.

The Halifax police department has a system in place that captures statistics on cyber-crime. In 2001, 41 cyber-crimes were reported, most commonly child pornography (8) and fraud (5). 'Other' *Criminal Code* offences accounted for the remaining reported offences.

2. Montreal Urban Community (MUC) Police

There is no formal definition in place within the MUC that defines cyber-crime. The Division of Special Tactics contains a Crime Technology sub-unit that investigates cyber-crime. The mandate of this sub-unit is to support other divisions with incidents involving a computer. The number of crimes that this unit has provided assistance on declined 23% between 2000 and 2001, from 275 incidents to 213 incidents.

The Montreal Police Service is currently preparing formal policies and procedures relating to computer and Internet crime investigations.

3. Sûreté du Québec (SQ)

The SQ defines cyber-crime as "all crimes that are committed through the Internet". The Division of Cyber Surveillance and Monitoring, operational since December 2001, is the SQ's specialized unit that investigates and monitors cyber-crime. The Division analyzes and evaluates each crime to determine whether or not the crime is related to the Internet, and carries out preliminary assessments of criminal information banks, suspicious Internet activities, Internet infiltration,

child pornography, etc. The staff prepares and executes warrants and then forwards the file to the appropriate unit of the police force concerned. In addition, the highly qualified and experienced staff supports and trains members of the Sûreté du Québec and personnel from other assisting organizations. Between January 2002 and September 2002, the Division provided assistance in 309 incidents involving 185 morality incidents, 99 economic crime incidents and 99 incidents against the person.

4. Ottawa Police

Ottawa Police do not have a formal definition of cyber-crime or formal policy for computer crime investigation. However, there is a formal policy for certain investigation types that are Internet-related such as child pornography and fraud. In 1999, the Ottawa Police Service's High-Tech Crime Unit was created to deal with cyber-crime activity.

The responsibilities of the High-Tech Crime Unit (HTCU) include:

- Crimes where the computer is the target of the offence (i.e. network intrusion or 'hacking'). Crimes where the computer is used as a tool (i.e. fraud, threats and harassment) are handled by the appropriate investigative sections.
- Crimes related to child pornography on the Internet. Crimes related to child sexual abuse are referred to the Sexual Assault Child Abuse Section.
- Forensic analysis of computer systems. Overall responsibility for the investigations remain with the assigned sections (as above) while the HTCU provides technical assistance to these investigators. This can range from recovered stolen property to death investigations.
- Technical assistance to other investigative sections regarding Internet issues. This can range from online suicide complaint investigation to e-mail tracing.

In-house codes are used with their records management system to flag crime that has been committed with the aid of the computer.

Ottawa Police Statistics on Internet-related Crime, 2000 and 2001

	2000	2001
Threats	63	76
Threats to Partner	1	2
Child Pornography	31	26
Fraud> $5,000	7	6
Fraud≤ $5,000	31	28
Mischief with Data	10	17
TOTAL	**143**	**155**

Source: *Ottawa Police Service*

5. Royal Canadian Mounted Police (RCMP)

The Computer Crime Program at the RCMP defines cyber-crime within two broad categories: computer crime and computer-assisted crime.

Computer crime is any criminal act where a computer and/or its contents are the object of a crime. Computer crimes involve the *Criminal Code* offences relating to the unauthorized use of computers or mischief in relation to data. These also include hackers who gain unauthorized access to computer systems and tamper with data.

Computer-assisted crime involves traditional criminal offences that are facilitated by the computer (i.e. drug trafficking, fraud, the distribution of child pornography, etc.). In computer-assisted crimes the computer is used as a tool that aids in the commission of the offence.

To maximize its efficiency, the RCMP aligned its technological crime resources under a new Technological Crime Branch. This Branch is responsible for research and development, policy and standards and investigational support in the technological crime area. One of the specialized duties of this Branch is to investigate crimes where computer systems and/or their contents are the objects of crime. This includes investigating abused telecommunication systems, particularly in an inter-provincial and international context. Another specialized duty of the Technological Crime Branch is to provide computer investigative support including the search, seizure and analysis of electronic evidence in support of computer-assisted criminal investigations, such as organized crime, national security, proceeds of crime and economic crimes.

The RCMP has a system in place within their Operational Statistics Reporting (OSR) System that captures data on cyber-crime. In 1997 the RCMP implemented an Internet survey code providing the capability to determine whether the Internet played a significant or integral role in the crime. The number of cyber-crimes has increased from 54 incidents in 1997 to 768 incidents in 2001. In 2001, the most common cyber-crimes reported were mischief to data (376), child pornography (110) and unauthorized use of a computer (58).

6. Ontario Provincial Police (OPP)

The OPP does not have a formal definition of cyber-crime for statistical reporting purposes. The OPP classifies a crime as a computer crime when the substantive offence falls within Section 342.1 'Unauthorized use of computer' or Section 430. (1.1) 'Mischief in relation to data' of the *Criminal Code*.

The OPP investigates cyber-crimes and supports the electronic search and seizure for the Anti-Rackets Health Fraud Investigative Team through the Electronic Crime Section, developed in 1999.

The OPP does not have a specific written policy on how cyber-crime investigations are conducted; however, the OPP does have a specific written policy and procedure on the search and seizure of digital evidence. The investigation of a traditional crime that involves a computer element such as the Internet or electronic evidence is conducted in the same fashion as any other criminal occurrence, where the lead investigator could be from the field or headquarters but assistance is readily available from the Electronic Crime Section. The Electronic Crime Section provides expertise upon request to OPP detachments, OPP Bureaus, Government agencies, and other municipal agencies.

The mandate of the e-Crime Team is to provide technology investigative expertise in the areas of conducting forensic computer searches, assist in traditional investigations in which computers are being used as a tool, investigate computer crime as defined in the *Criminal Code* and act as consultants in investigations where technology is being used to further a crime.

The OPP e-Crime Section has a system in place within their records management system that captures Internet-related crime statistics. In 2001, the e-Crime Section received a total of 191 requests for service, of which 70% were Internet-related. The most common Internet-related offences were fraud (19), uttering threats (16), mischief to data (10), child pornography (9), sexual assault (9) and criminal harassment (6).

The OPP also has the Child Pornography Unit, which is dedicated to the investigation of Child Pornography that includes the use of the Internet and computers. The Child Pornography Unit has a system in place within their records management system that captures Internet investigation statistics. In the year 2001, the Child Pornography Unit responded to 410 investigations, executed 91 search warrants, and laid 75 charges against 37 persons.

7. Toronto Police

Although there is no operating definition of cyber-crime with this police force, Toronto Police investigate cyber-crime through the Sexual Exploitation Section and the Technical Support Section.

Part of the mandate of the Sexual Exploitation Section within the Sexual Assault Squad is to investigate exploitation on the Internet. Currently, the Toronto Police Service has six individuals dedicated to Internet child pornography investigations. The Toronto Police are proposing a 2-year project which will address the growing demand for Child Pornography investigation, and would bring the total staff in the Child Exploitation Section to ten members.

In addition, the Technical Support Section also provides assistance to other units when a crime is committed with the aid of a computer. This section currently has two individuals dedicated to forensic examination of computers and retrieval of evidence. The result of the 2-year project proposal would see the dedication of six additional officers.

To date, the Toronto Police Service has nothing in place within their records management system that traces cyber-crime.

8. Calgary Police

The Calgary Police Service defines technical/computer crime as "any action, which contravenes any law, and involves a computer system or other technological device. It may be that the device or computer system is an object of a crime, an instrument used to commit a crime or a repository of evidence related to a crime."

The Calgary Police Service's Technical Crime-Unit is a sub-unit within the Commercial Crimes Unit. To date, the Calgary Police do not have a formal method of identifying and gathering statistics on cyber-crime. The Technical Crime sub-unit is in the early stages of building a database which will contain cyber-crimes in addition to statistics regarding crimes involving the use of computers.

9. Vancouver Police

The Vancouver Police use the Canadian Police College's definition of cyber-crime. They classify cyber-crime as per the two sections in the *Criminal Code* that refer to criminal interference with a computer and/or the data therein. Other than that, a crime is computer-related when a computer is used as an instrument of the crime i.e.: importing, exporting, transporting or storing of data. The Vancouver Police Financial Crimes section is responsible for investigating any Internet-related crime according to the *Criminal Code.*

To date, Vancouver Police do not have a system in place that captures cyber-crime statistics. However, identifying the crime as Internet/computer related should not be a problem for future data capturing.

PART VI – DATA COLLECTION OPTIONS FROM POLICE

Based on the findings from the CCJS's consultations with police and the review of other data collection methods from the United States and the United Kingdom, two options have been identified for the future collection of data on cyber-crime from police forces: conducting a special study and modifying the Incident-based Crime Statistics Survey. Examples from Household surveys described in Part IV illustrate other sources of additional information that are available. This section however talks about information related to the collection of police-reported statistics on cyber-crime.

Option 1: Special Study

One option would be a special study to collect detailed information from police agencies that collect cyber-crime statistics. As specialized units become more equipped to investigate cyber-crime, data collection methods may improve among police forces in Canada. Currently, at least six forces collect statistics on cyber-crime. Until such time that the UCR2 survey can be modified, a special study would permit police to provide the information they currently collect on cyber-crime.

Advantages:

- Data availability - some data are currently available from police;
- Progress step towards defining the framework for the development of a new data element in the UCR2 survey; and,
- Possibility/ability to have data before revisions to the UCR2 survey could be made.

Disadvantages:

- Absence of a formal definition of cyber-crime. Data from different police forces may not be measuring the same concept; and,
- Cost to develop a survey and data collection system, and analyze and disseminate data.

Depending on the number of police services participating, the focus of the study, questions asked, system costs and deliverables, the costs of a special study would be a minimum of $100,000 over a 1 to 2-year period.

Option 2: Modifying the Incident-based Crime Statistics (UCR2) Survey

Another option would be adding a data element to the UCR survey similar to the United States NIBRS to identify whether or not a *Criminal Code* offence is related to the Internet/computer. For example, the officer would still code the violation code that presently exists for the *Criminal Code* offence committed (e.g. fraud), but would use the new data element to flag whether or not the crime was Internet/computer-related.

Below is an example of a possible new UCR2 data element:

DATA ELEMENT 1a

Name: Cyber-Crime
Record: Incident Level

General Definition: *A criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence (Canadian Police College).*

Coding Options:

(i) No, incident is not related to the Internet or computer equipment
(ii) Yes, incident involved a computer/Internet- if yes go to Data Element 1b
(iii) Unknown
(iv) Not applicable

DATA ELEMENT 1b

Name: Cyber-Crime Type
Record: Incident Level

General Definition: *This data element defines different methods to commit a criminal offence with the aid of the Internet/ computer. These methods include the computer being used as a tool and the computer being used as the object of the crime. Child pornography, criminal harassment, intellectual property violation and the sale of illegal substances and goods are some examples where the computer is the tool of the crime. Hacking, defacing websites, creation and malicious dissemination of computer viruses are examples where the computer is the object of the crime.*

Coding Options:

(i) Object of the crime (i.e. hacking)
(ii) Instrument/ tool for the crime (i.e. fraud, child pornography)
(iii) Unknown
(iv) Not applicable

Advantages:

- Possibility/ability to collect detailed information, not only on the Incident but also on the Accused and the Victim (for offences against the person only);
- The UCR2 survey already exists - once the data element is added, there are no significant additional costs to incur;
- Possibility/ability to produce annual statistics on the incidence of cyber-crime;
- Some police services are currently collecting cyber-crime statistics in their records management system; and,
- Many forces currently not reporting cyber-crime statistics indicated that adding a new component to their records management system for this would not produce significant respondent burden.

Disadvantages:

- Implementation time - it will be a few years before another version of the survey with these and other changes can be considered; and,
- Not all police forces provide data to the UCR2 - currently the coverage is 60% of the national volume of crime.

Modifying the UCR2 Survey is an expensive and lengthy exercise. However, once in place, the total costs would be far lower than conducting future Special Studies to capture and analyze cyber-crime data.

RECOMMENDATIONS:

It is recommended that both options be used as tools for facilitating the future data collection of cyber-crime statistics. Ideally, for the short-term, the special study (option 1) can be used to survey all of the major police forces in Canada to examine their current methods of data collection. Through this option, data quality can be examined and assistance provided to jointly establish common definitions, policies, procedures and data collection methods among police forces. The results from this option can be used to assist in the redevelopment of the UCR2 survey (option 2) which can be viewed as a long-term goal.

PART VII – CONCLUSION

Recent attention from federal, provincial and territorial governments, as well as the police community on cyber-crime has led the CCJS to examine the feasibility of collecting police-reported data on Internet crime. This report provides a preliminary look into the feasibility of collecting police-reported cyber-crime statistics and offers possible options for the collection of cyber-crime statistics.

Collecting police-reported statistics on Internet criminal activity presents a great challenge as it poses many questions about data availability and reliability. A range of factors including the absence of an uniform definition among police departments, the lack of formal policies and procedures within specialized units, and the lack of resources provided to specialized units investigating Internet/ computer crime contribute to the challenges faced in collecting accurate statistics on cyber-crime activity.

New challenges, specific to cyber-crime, contribute to the amount of cyber-crime activity not being reported and investigated by the police. In addition, cyber-crime may be one of the most under-reported form of criminal behavior because the victim often remains unaware that an offence has even taken place, and in the case of businesses, are reluctant to report for fear of loss of consumer confidence. Sophisticated technologies, storage capacities of computer networks and global distribution of information increase the difficulty of detecting cyber-crime. The literature suggests that most cyber-crime occurrences may not be reported to police.

These challenges include:

1. Technical challenges that hinder law enforcement's ability to find and prosecute criminals operating online;
2. Legal challenges resulting from out of date laws, and legal tools needed to investigate cyber-crime are lagging behind technological structural and social changes;
3. Operational challenges to ensure that law enforcement officers are well-trained and well-equipped to work together, including across national borders;
4. Difficulty in identifying the perpetrators of these crimes as they frequently use false identities online and make use of anonymous re-mailer services; and,
5. Difficulty in identifying the exact location of the crime. These crimes can be perpetrated from any location that has telephone service. Some examples include public Internet stations in airports, bus depots, libraries, cyber-cafés and convenience stores.

However, collecting cyber-crime statistics at a national level is important in order to assess the impact that this type of crime has on society. Governments and the police community rely on this information to help them enforce policies and procedures as well as allocating resources to investigate and prevent the incidence of cyber-crime activity in Canada.

This report has presented two options for the possible collection of data on cyber-crime activity in Canada. The short-term option would be a Special Study to collect detailed information from police agencies that collect cyber-crime statistics. The long-term option would involve adding a data element to the UCR2 Survey to identify *Criminal Code* offences involving the Internet/computer as the object or as the tool used to commit the crime.

REFERENCES

Bureau of Justice Statistics. 2002 *Office of Justice Prosecutions.* U.S. Department of Justice. <http://www.ojp.usdoj.gov >. (Accessed November 4, 2002).

Canada Newswire. 2002. *Child Online Safety Gets a Boost with Launch of Cybertip.ca.* http://www.newswire.ca/releases/September2002/26/c5173.html. (Accessed November 4, 2002).

Carter, D. 1995. "Computer crime categories: How techno-criminals operate." *FBI Law Enforcement Bulletin*. 64(7), 21.

Chu, S. 2000, December 14. *Canada lags in cyber-crime laws.* <http://globetechnology.com/servlet/GAMArticleHTML>. (Accessed November 4, 2002).

Convention on Cyber-Crime. 2001. *The Convention on Cyber- Crime, a unique instrument for international co-operation.* Budapest: Council of Europe. <http://conventions.coe.int/treaty/EN/projets/projets.htm:2001> . (Accessed November 4, 2002).

Davis, R and Hutchison, S. 1997. *Computer Crime in Canada.* Toronto: Thomson Canada Limited.

Department of Justice Canada. 2002. *Stronger Child Pornography Laws Receive Royal Assent.* Ottawa: Department of Justice Canada. <http://canada.justice.gc.ca/ennews/nr/2002/doc_30529.html>. (Accessed November 4, 2002).

Federal Bureau of Investigation. 2000. *National Incident-Based Reporting System, Volume 1: Data Collection Guidelines.* West Virginia: FBI, US Department of Justice.

Federal/Provincial/Territorial Working Group on Illegal and Offensive Content on the Internet. 2001. *Report to the coordinating committee of senior officials*. Ottawa: Department of Justice.

Finkelhor, D., K.J. Mitchell and J. Wolak. 2000. *Online Victimization: A Report of the Nation's Youth.* Washington, D.C.: National Center for Missing and Exploited Children.

General Social Survey, Cycle 14. 2000. *Access to and Use of Information Communication Technology.* Ottawa: Statistics Canada.

Internet Crime Forum. 2001, March. *Internet Crime Forum.* <http://www.internetcrimeforum.org.uk>. (Accessed November 4, 2002).

Internet Fraud Complaint Center. 2001. *IFCC 2001 Internet fraud report*.<http://www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf>.
(Accessed November 4, 2002).

Kubic, T. 2001, June. *The FBI's Perspective on the Cyber Crime Problem*. <http://www.FBI.GOV//CONGRESS/Congress01/kubic06/201.htm>. (Accessed November 4, 2002).

Media Awareness Network and Environics Research Group. 2000, March. *Canada's Children in a wired world – The parents' view.* Ottawa: Government of Canada. <http://strategis.ic.gc.ca/pics/sf/finalreporteng.pdf> . (Accessed November 4, 2002).

Media Awareness Network and Environics Research Group. 2001, October. *Young Canadians in a wired world – The students' view.* Ottawa: Government of Canada. <http://www.connect.gc.ca/cyberwise/pdf/wired_e.pdf> . (Accessed November 4, 2002).

Power, R. 2001. "2001 CSI/FBI computer crime and security survey." *Computer Security Issues & Trends.* San Francisco: Computer Security Institute, 7(1).

President's Working Group on Unlawful Conduct on the Internet. 2000, March *The electronic frontier: The challenge of unlawful conduct involving the use of the Internet.* Washington, D.C: U.S. Department of Justice. <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>. (Accessed November 4, 2002).

Royal Canadian Mounted Police. 2001, June. *PhoneBusters National Call Centre.* <http://www.rcmp-grc.gc.ca/news/nr-01-09.htm> . (Accessed November 4, 2002).

Statistics Canada. 2001, March. *Overview: Access to and Use of Information Communication on Technology.* Housing, Family and Social Statistics Division. <http://www.statcan.ca/english/IPS/Data/56-505-XIE/free.htm> . (Accessed November 4, 2002).

Statistics Canada. 2002, July. *Household Internet Use Survey.* The Daily. <http://www.statcan.ca/Daily/English/020725/d020725a.htm> . (Accessed November 4, 2002).

U.S. Census Bureau. 2002. *Computer Security Survey*. <http://www.census.gov/eos/www/css/css.html>. (Accessed November 4, 2002).

APPENDIX A: Incident Report: NIBRS Survey (USA)

ORI #:

INCIDENT #:

REPORT TYPE: ❑ INITIAL REPORT ❑ SUPPLEMENT

INCIDENT REPORT
(EXAMPLE)

INCIDENT STATUS: ❑ UNFOUNDED ❑ CLEARED BY ARREST ❑ CLEARED EXCEPTIONALLY
EXCEPTIONAL CLEARANCE DATE:

A ❑ DEATH OF OFFENDER
B ❑ PROSECUTION DECLINED
C ❑ EXTRADITION DECLINED
D ❑ REFUSED TO COOPERATE
E ❑ JUVENILE, NO CUSTODY
N ❑ NOT APPLICABLE

COMPLAINANT: (Last, First, Middle)

PHONE: (Home) ( ) (Business) ( )

ADDRESS: (Street, City, State, Zip)

LOCATION OF INCIDENT: (Address Or Block No.)

UCR OFFENSE CODE:	DATE(S) OF INCIDENT:	TIME(S) OF INCIDENT:
1.		
2.		
3.		

OFFENSE:	(Check If Bias Motivated)	OFFENDER:
1.	1. ❑	1.
2.	2. ❑	2.
3.	3. ❑	3.

BIAS MOTIVATION: (Check one for Offense #1)

RACIAL
11 ❑ ANTI - WHITE
12 ❑ ANTI - BLACK
13 ❑ ANTI - AMERICAN INDIAN / ALASKAN NATIVE
14 ❑ ANTI - ASIAN / PACIFIC ISLANDER
15 ❑ ANTI - MULTI - RACIAL GROUP

ETHNICITY / NATIONAL ORIGIN
31 ❑ ANTI - ARAB
32 ❑ ANTI - HISPANIC
33 ❑ ANTI - OTHER ETHNICITY / NATIONAL ORIGIN

RELIGIOUS
21 ❑ ANTI - JEWISH
22 ❑ ANTI - CATHOLIC
23 ❑ ANTI - PROTESTANT
24 ❑ ANTI - ISLAMIC (MOSLEM)
25 ❑ ANTI - OTHER RELIGION
26 ❑ ANTI - MULTI - RELIGIOUS GROUP
27 ❑ ANTI - ATHEISM / AGNOSTICISM

SEXUAL
41 ❑ ANTI - MALE HOMOSEXUAL (GAY)
42 ❑ ANTI - FEMALE HOMOSEXUAL (LESBIAN)
43 ❑ ANTI - HOMOSEXUAL (GAYS AND LESBIANS)
44 ❑ ANTI - HETEROSEXUAL
45 ❑ ANTI - BISEXUAL

ENTER BIAS MOTIVATION CODE IF DIFFERENT FROM OFFENSE #1
#2 [ ][ ]
#3 [ ][ ]

OFFENSE STATUS: (Check Only One Per Offense)

1.	2.	3.
A ❑ ATTEMPTED	A ❑ ATTEMPTED	A ❑ ATTEMPTED
C ❑ COMPLETED	C ❑ COMPLETED	C ❑ COMPLETED

OFFENDER(S) USED: (Check As Many As Apply)
A ❑ ALCOHOL
C ❑ COMPUTER EQUIP.
D ❑ DRUGS
N ❑ NOT APPLICABLE

(For Burglary Only)
NUMBER OF PREMISES ENTERED: _____
METHOD OF ENTRY: F ❑ FORCIBLE N ❑ NO FORCE

LOCATION OF OFFENSE: (Check Only One) (Enter Code Number for Offense #2 _____ #3 _____)
01 ❑ AIR / BUS / TRAIN TERMINAL
02 ❑ BANK / SAVINGS & LOAN
03 ❑ BAR / NIGHT CLUB
04 ❑ CHURCH / SYNAGOGUE / TEMPLE
05 ❑ COMMERCIAL / OFFICE BUILDING
06 ❑ CONSTRUCTION SITE
07 ❑ CONVENIENCE STORE
08 ❑ DEPARTMENT / DISCOUNT STORE
09 ❑ DRUG STORE / DR'S OFFICE / HOSPITAL
10 ❑ FIELD / WOODS
11 ❑ GOVERNMENT / PUBLIC BUILDINGS
12 ❑ GROCERY / SUPERMARKET
13 ❑ HIGHWAY / ROAD / ALLEY
14 ❑ HOTEL / MOTEL / ETC.
15 ❑ JAIL / PRISON
16 ❑ LAKE / WATERWAY
17 ❑ LIQUOR STORE
18 ❑ PARKING LOT / GARAGE
19 ❑ RENTAL / STORAGE FACILITY
20 ❑ RESIDENCE / HOME
21 ❑ RESTAURANT
22 ❑ SCHOOL / COLLEGE
23 ❑ SERVICE / GAS STATION
24 ❑ SPECIALTY STORE (TV, FUR, ETC.)
25 ❑ OTHER / UNKNOWN

TYPE CRIMINAL ACTIVITY: (Check Up To Three)
B ❑ BUYING / RECEIVING
C ❑ CULTIVATING / MANUFACTURING / PUBLISHING
D ❑ DISTRIBUTING / SELLING
E ❑ EXPLOITING CHILDREN
O ❑ OPERATING / PROMOTING / ASSISTING
P ❑ POSSESSING / CONCEALING
T ❑ TRANSPORTING / TRANSMITTING / IMPORTING
U ❑ USING / CONSUMING

TYPE WEAPON / FORCE INVOLVED: (Check Up To Three) (Enter A In Box If Automatic)
11 ❑ FIREARM (type not stated)
12 ❑ HANDGUN
13 ❑ RIFLE
14 ❑ SHOTGUN
15 ❑ OTHER FIREARM
20 ❑ KNIFE / CUTTING INSTRUMENT
30 ❑ BLUNT OBJECT
35 ❑ MOTOR VEHICLE
40 ❑ PERSONAL WEAPONS
50 ❑ POISON
60 ❑ EXPLOSIVES
65 ❑ FIRE / INCENDIARY
70 ❑ NARCOTICS / DRUGS
85 ❑ ASPHYXIATION
90 ❑ OTHER
95 ❑ UNKNOWN
99 ❑ NONE

VICTIM # 1: (Last, First, Middle)

PHONE: (Home)

ADDRESS: (Street, City, State, Zip)

TYPE OF VICTIM: (Check Only One)
I ❑ INDIVIDUAL
B ❑ BUSINESS
F ❑ FINANCIAL
G ❑ GOVERNMENT
R ❑ RELIGIOUS
S ❑ SOCIETY / PUBLIC
O ❑ OTHER
U ❑ UNKNOWN

RACE: W ❑ WHITE B ❑ BLACK I ❑ INDIAN A ❑ ASIAN U ❑ UNKNOWN

SEX: M ❑ MALE F ❑ FEMALE U ❑ UNKNOWN

AGE:
DOB:
NO. OF VICTIMS:

RESIDENT STATUS: R ❑ RESIDENT N ❑ NONRESIDENT U ❑ UNKNOWN

ETHNICITY: H ❑ HISPANIC N ❑ NON - HISPANIC U ❑ UNKNOWN

AGGRAVATED ASSAULT / HOMICIDE CIRCUMSTANCES: (Check Up to Two)
01 ❑ ARGUMENT
02 ❑ ASSAULT ON LAW OFFICER
03 ❑ DRUG DEALING
04 ❑ GANGLAND
05 ❑ JUVENILE GANG
06 ❑ LOVERS' QUARREL
07 ❑ MERCY KILLING
08 ❑ OTHER FELONY INVOLVED
09 ❑ OTHER CIRCUMSTANCES
10 ❑ UNKNOWN CIRCUMSTANCES

INJURY TYPE: (Check Up to Five)
N ❑ NONE
B ❑ BROKEN BONES
I ❑ POSS. INT. INJURIES
L ❑ SEVERE LACERATION
M ❑ MINOR INJURY
O ❑ MAJOR INJURY
T ❑ LOSS OF TEETH
U ❑ UNCONSCIOUSNESS

VICTIM CONNECTED TO OFFENSE NUMBER ABOVE:
1. ❑
2. ❑
3. ❑

RELATIONSHIP OF VICTIM TO OFFENDER: (For multiple offender relationships enter offender number[s] in space)
SE ____ SPOUSE
CS ____ COMMON - LAW SPOUSE
PA ____ PARENT
SB ____ SIBLING
CH ____ CHILD
GP ____ GRANDPARENT
GC ____ GRANDCHILD
IL ____ IN-LAW
SP ____ STEPPARENT
SC ____ STEPCHILD
SS ____ STEPSIBLING
OF ____ OTHER FAMILY
AQ ____ ACQUAINTANCE
FR ____ FRIEND
NE ____ NEIGHBOR
BE ____ BABYSITTEE (baby)
BG ____ BOY / GIRL FRIEND
CF ____ CHILD OF "BG" ABOVE
HH ____ HOMOSEXUAL REL.
XS ____ EX-SPOUSE
EE ____ EMPLOYEE
ER ____ EMPLOYER
OK ____ OTHERWISE KNOWN
ST ____ STRANGER
VO ____ VICTIM WAS OFFENDER
RU ____ RELATIONSHIP UNKNOWN

Page _____ of _____

PROPERTY

TYPE PROPERTY LOSS / ETC.	CODE	QUANTITY	PROPERTY DESCRIPTION INCLUDE MAKE, MODEL, SIZE, TYPE, SERIAL #, COLOR, ETC.	VALUE	DATE RECOVERED Month / Day / Year
1 ❑ NONE					
2 ❑ BURNED					
3 ❑ COUNTERFEITED / FORGED					
4 ❑ DAMAGED / DESTROYED					
5 ❑ RECOVERED					
6 ❑ SEIZED					
7 ❑ STOLEN					
8 ❑ UNKNOWN					

PROPERTY DESCRIPTION CODE TABLE:

(Enter Number In Code Column Above)

01 AIRCRAFT
02 ALCOHOL
03 AUTOMOBILES
04 BICYCLES
05 BUSES
06 CLOTHES / FURS
07 COMPUTER HARDWARE / SOFTWARE
08 CONSUMABLE GOODS
09 CREDIT / DEBIT CARDS
10 DRUGS / NARCOTICS
11 DRUG / NARCOTIC EQUIPMENT
12 FARM EQUIPMENT
13 FIREARMS
14 GAMBLING EQUIPMENT
15 HEAVY CONSTRUCTION / INDUSTRIAL EQUIPMENT
16 HOUSEHOLD GOODS
17 JEWELRY / PRECIOUS METALS
18 LIVESTOCK
19 MERCHANDISE
20 MONEY
21 NEGOTIABLE INSTRUMENTS
22 NONNEGOTIABLE INSTRUMENTS
23 OFFICE-TYPE EQUIPMENT
24 OTHER MOTOR VEHICLES
25 PURSES / HANDBAGS / WALLETS
26 RADIOS / TVs / VCRs
27 RECORDINGS - AUDIO / VISUAL
28 RECREATIONAL VEHICLES
29 STRUCTURES - SINGLE OCCUPANCY DWELLINGS
30 STRUCTURES - OTHER DWELLINGS
31 STRUCTURES - OTHER COMMERCIAL / BUSINESS
32 STRUCTURES - INDUSTRIAL / MANUFACTURING
33 STRUCTURES - PUBLIC / COMMUNITY
34 STRUCTURES - STORAGE
35 STRUCTURES - OTHER
36 TOOLS - POWER / HAND
37 TRUCKS
38 VEHICLE PARTS / ACCESSORIES
39 WATERCRAFT
77 OTHER
88 PENDING INVENTORY
99 (_____)

OFFENDER

NUMBER OF OFFENDERS: _____

1. **ADDRESS:** (Street, City, State, Zip)

AGE: **SEX:** M ❑ MALE F ❑ FEMALE U ❑ UNKNOWN **RACE:** W ❑ WHITE B ❑ BLACK I ❑ INDIAN A ❑ ASIAN U ❑ UNKNOWN **HEIGHT:** _____ feet _____ inches **WEIGHT:** **EYES:** **HAIR:** **CLOTHING:**

2. **ADDRESS:**

AGE: **SEX:** M ❑ MALE F ❑ FEMALE U ❑ UNKNOWN **RACE:** W ❑ WHITE B ❑ BLACK I ❑ INDIAN A ❑ ASIAN U ❑ UNKNOWN **HEIGHT:** _____ feet _____ inches **WEIGHT:** **EYES:** **HAIR:** **CLOTHING:**

3. **ADDRESS:**

AGE: **SEX:** M ❑ MALE F ❑ FEMALE U ❑ UNKNOWN **RACE:** W ❑ WHITE B ❑ BLACK I ❑ INDIAN A ❑ ASIAN U ❑ UNKNOWN **HEIGHT:** _____ feet _____ inches **WEIGHT:** **EYES:** **HAIR:** **CLOTHING:**

ARRESTEE

NUMBER OF ARRESTEES: _____ **MULTIPLE CLEARANCE INDICATOR:** M ❑ MULTIPLE C ❑ COUNT ARRESTEE N ❑ NOT APPLICABLE

ARRESTEE #1: (Last, First, Middle) **ADDRESS:** (Street, City, State, Zip)

AGE: **SEX:** M ❑ MALE F ❑ FEMALE **RACE:** W ❑ WHITE B ❑ BLACK I ❑ INDIAN A ❑ ASIAN U ❑ UNKNOWN **DOB:** **ARRESTEE ETHNICITY:** H ❑ HISPANIC N ❑ NON-HISPANIC U ❑ UNKNOWN **RESIDENT STATUS:** R ❑ RESIDENT N ❑ NONRESIDENT U ❑ UNKNOWN

ARRESTEE WAS ARMED WITH: (Check Up To Two) (Enter A In Box If Automatic)
01 ❑ UNARMED
11 ❑ FIREARM (type not stated)
12 ❑ HANDGUN
13 ❑ RIFLE
14 ❑ SHOTGUN
15 ❑ OTHER FIREARM
16 ❑ LETHAL CUTTING INSTRUMENT (e.g. Switchblade Knife, etc.)
17 ❑ CLUB / BLACKJACK / BRASS KNUCKLES

TYPE OF ARREST:
O ❑ ON-VIEW
S ❑ SUMMONED / CITED
T ❑ TAKEN INTO CUSTODY

DISPOSITION OF ARRESTEE UNDER 18:
H ❑ HANDLED WITHIN DEPARTMENT
R ❑ REFERRED TO OTHER AUTHORITY

HEIGHT: feet / inches	WEIGHT:	EYES:	HAIR:	ARREST NUMBER:	ARREST DATE:	UCR ARREST OFFENSE CODE:

WITNESS

NAME: (Last, First, Middle)	ADDRESS: (Street, City, State, Zip)	RESIDENTIAL PHONE:	BUSINESS PHONE:
#1			
#2			

NARRATIVE

❑ continued on supplement

APPENDIX B: National Victimization Survey (USA)

FORM **NCVS-1**
(5-10-2001)

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU

ACTING AS COLLECTING AGENT FOR THE
BUREAU OF JUSTICE STATISTICS
U.S. DEPARTMENT OF JUSTICE

NATIONAL CRIME VICTIMIZATION SURVEY

NCVS-1 BASIC SCREEN QUESTIONNAIRE

HOUSEHOLD RESPONDENT'S COMPUTER CRIME SCREEN QUESTIONS

FIELD REPRESENTATIVE – *Read introduction.*

INTRO: **The next series of questions are about YOUR use of a computer. Please include ALL computers, laptops, or access to WebTV used at home, work, or school for PERSONAL USE *or* for operating a home business.**

45c. **During the last 6 months, have YOU used a computer, laptop, or WebTV for the following purposes** *(Read answer categories 1–4)* –

Mark (X) all that apply.

100 *
1 ☐ **For personal use at home?**
2 ☐ **For personal use at work?**
3 ☐ **For personal use at school, libraries, etc.?**
4 ☐ **To operate a home business?**
5 ☐ None of the above – ***SKIP*** *to Check Item D*

45d. **How many computers do you have access to for personal use or for operating a home business?**

101
0 ☐ None
1 ☐ 1
2 ☐ 2
3 ☐ 3
4 ☐ 4 or more

45e. **Do YOU use the Internet for personal use or for operating a home business?**

102
1 ☐ Personal use
2 ☐ Operating a home business
3 ☐ Both
4 ☐ None of the above

45f. **Have you experienced any of the following COMPUTER-RELATED incidents in the last 6 months** *(Read answer categories 1–6)* –

Mark (X) all that apply.

103 *
1 ☐ **Fraud in purchasing something over the Internet?**
2 ☐ **Computer virus attack?**
3 ☐ **Threats of harm or physical attack made while online or through E-mail?**
4 ☐ **Unrequested lewd or obscene messages, communications, or images while online or through E-mail?**
5 ☐ *(Only ask if box 4 is marked in Item 45c)* **Software copyright violation in connection with a home business?**
6 ☐ **Something else that you consider a computer-related crime?**–*Specify* ✍
_____
_____
7 ☐ No computer-related incidents –***SKIP*** *to Check Item D*

45g. **Did you suffer any monetary loss as a result of the incident(s) you just mentioned?**

104
1 ☐ Yes
2 ☐ No – ***SKIP*** *to 45i*

45h. **How much money did you lose as a result of the incident(s)?**

105
$_____ .00 Amount of loss
x ☐ Don't know

45i. **Did you report the incident(s) you just mentioned to** *(Read answer categories 1–5)* –

Mark (X) all that apply.

106 *
1 ☐ **A law enforcement agency?**
2 ☐ **An Internet Service provider?**
3 ☐ **A Website administrator?**
4 ☐ **A Systems Administrator?**
5 ☐ **Someone else? –** *Specify* ✍
_____
_____
6 ☐ None of the above

APPENDIX C: Measuring Cyber-Crime through the GSS

The 2000 GSS (cycle 14) is the first cycle to collect detailed information on access to and the use of technology in Canada (the 1994 cycle provided limited information). The questions used to provide some measure of Internet crime activity include:

1. To the best of your knowledge, while on the Internet have your children come across content that promotes hate or violence against a particular group?

2. Have you ever received e-mail that you considered personally threatening or harassing?

3. While on the Internet, have you come across content that promotes hate or violence against a particular group?

4. While on the Internet, have you come across websites that contain pornography?
   Were you looking for this content or did you come across it unexpectedly?
   Did you find it offensive?

5. *Have you experienced any problems* associated with security on the Internet?
   What was (were) the problem(s) associated with security on the Internet?

   (1) Viruses
   (2) Threatening e-mail messages
   (3) People hacking into e-mail accounts or computer files
   (4) Personal information was made public
   (5) Other

Source: *General Social Survey, Cycle 14: 2000.*