Deloitte.

Canadian Association of Police Boards

A report on cybercrime in Canada

April 29, 2008

Audit.Tax.Consulting.Financial Advisory.

REPORT ON CYBER CRIME IN CANADA PRODUCED WITH SUPPORT FROM:

Public Safety Canada

Sécurité publique Canada

Alberta Government

Solicitor General and Public Security

THE CITY OF CALGARY

CALGARY POLICE COMMISSION

Table of contents

Executive Summary

Deloitte's engagement with the Canadian Association of Police Boards (CAPB) encompasses three distinct parts: a public survey, interviews with select stakeholders, and a review of open source research.

To gain their input on the issue of cybercrime with the objective of supporting future initiatives, Deloitte interviewed individuals from law enforcement; crown prosecutors, and other government personnel with experience in these issues. Respondents hold positions at the federal, provincial, regional or municipal level. In general terms, they were asked to comment on the following main subject areas:

1. The definition of cybercrime and the extent of the threat it poses
2. Challenges and opportunities in terms of cooperation and sharing of information among jurisdictions
3. The resources required to advance the battle against cybercrime
4. The status of Canadian anti-cybercrime legislation in the global context

To supplement the learning gained from these interviews and provide additional context, we included relevant findings from a review of open source research on the same topics. We also conducted a public opinion survey on the subject of cybercrime; a detailed report of this study is included as Appendix A.

Through the interviews, the research review on the subject of cybercrime, and our public survey, it was reinforced that an unclear definition of cybercrime in Canada is hindering efforts to detect, deter and prevent it – and that opportunities abound for more dedicated resources as well as for collaboration and coordination of efforts. Investigators and prosecutors stated they are simply scratching the surface, and are overwhelmed by the challenges.

It was suggested that many opportunities could be addressed through changes to legislation. These changes would enable efficient information-sharing among law enforcement agencies, assist in the prosecution of internet-based crimes, and significantly reduce investigation timelines.

Interviewees communicated the desire to have a government entity take the lead for coordination of cybercrime-related enforcement as well as for cyber security, and to set standards for other levels of government and the private sector to follow.

Suggestions put forward include:

- The establishment of a dedicated collaboration and coordination centre where law enforcement, government, the private sector, and academia would co-ordinate efforts in the fight against cyber crime.

- The evolution of Canadian legislation to address new crimes such as spam as well as evolving crimes such as child pornography and organized crime's use of technology and the internet. Specifically this includes:

  - implementation of the legislation as proposed in August of 2002 with respect to the lawful access provisions of the criminal code;
  - changes to existing legislation that would enable information sharing with law enforcement with lower judicial standards than those now applied to search and seizure warrants, and

- changes to the Canada Evidence Act that would improve on the existing Mutual Legal Assistance treaty's ability to enable the admission of documents held in the normal course of business in another country

- Increased resourcing and funding for law enforcement and Crown Prosecutors related to cybercrime investigations and prosecutions.

- The need for a central mechanism for the mandatory reporting of designated cyber security incidents to enable quantification of the potential damage to the Canadian economy

- Increased cybercrime awareness and prevention should be introduced into school curriculums as part of educating children on the issues of cybercrime.

- New legislation making spamming an offence.

- Mandatory reporting requirements for child pornography.

Restrictions

This report is not intended for general circulation or publication, and it is not to be reproduced or used for any purpose other than that outlined below without our written permission in each specific instance. We do not assume any responsibility or liability for losses incurred by CAPB or its employees or by any other parties as a result of the circulation, publication, reproduction or use of this report contrary to the provisions of this paragraph.

We understand and acknowledge that this report will be used by CAPB and will be given to individuals who have a vested interest in the contents of this report. In particular we are aware that the Ministry of Public Safety will be provided with a copy of this report. This report is based on information in our possession as of April 29, 2008. Deloitte cannot assume responsibility for the accuracy of the information obtained from open sources, nor can we guarantee that we located all relevant information that might exist regarding cybercrime. We reserve the right to review all findings and conclusions included or referred to in our report and, if we consider it necessary, to revise our report if any information is provided subsequent to the date of our report.

Interview Process

Deloitte developed questionnaires for the purpose of interviewing individuals from law enforcement and government; additional questions were asked based on their responses. In all cases we asked for and were given access to those individuals in each organization who had the most knowledge about cybercrime. The following specific questions were asked – in the report, responses have been grouped to avoid redundancy:

- What is your definition of cybercrime?
- What is the effect of cybercrime on the citizens of Canada?
- What do you see as the biggest threat in terms of cybercrime?
- In terms of combating cybercrime what do you believe is working/not working?
- How could the fight against cybercrime be improved?
- From an enforcement perspective, what do you see are the largest challenges in investigating cybercrime?
- How have jurisdictional issues affected your ability to investigate cybercrime?
- What role do you believe "Organized Crime" plays in cybercrime?
- What would you recommend in terms of investigative techniques or proactive procedures to address cybercrime detection/response/remediation?
- From your point of view, how much co-operation and sharing of information is there between agencies involved in the investigation of/response to cybercrime related matters?
- What exposure has your agency had with International cybercrime matters?
- What impact has cyber related crime affected the government in terms of resources required, policy, legislation, etc?
- How has the Crown's office had to change (if at all) in relation to training, infrastructure and personnel for cyber-related prosecutions?
- What does the Government see as a necessity for continuing to combat cyber-related threats/crimes?

To ensure the accuracy of their comments, interviews were recorded and later transcribed and reviewed with the consent and knowledge of the interviewee. We have included several direct quotations to illustrate many of the identified findings. These are indicated by the use of italics in the text.

The Deloitte team involved in this study would like to thank all those individuals interviewed and who provided valuable insight during the course of our work. The cooperation provided, the candour and frankness in answering our questions and providing us with information was greatly appreciated.

Subject Areas Explored

1. The definition of cybercrime and the extent of the threat it poses

In our interviews and review of information related to defining cybercrime with law enforcement and Crown prosecutors, a lack of a standard definition of cybercrime was widely referenced as a primary reason why few, if any, Canadian statistics exist with respect to cybercrime activities, investigations and prosecutions. Law enforcement agencies in Canada report criminal charges laid to Statistics Canada through an initiative called the Uniform Crime Reporting (UCR). Although the UCR presently does not have a standardized method of collecting data on cybercrime activity, it is encouraging to note that updates to the national UCR survey include abilities to report the use of computers in the commission of crimes.

Several law enforcement agencies referred to cybercrime as being substantively child pornography matters, while complaints such as threats via email or frauds involving electronic funds transactions were classified according to the traditional crime category of that nature.

A common definition cited by Canadian entities is from Statistics Canada which with the Canadian Police College defines cybercrime 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."[1]

The definition of cybercrime can be broken down into two components that deal with both the evolution of traditional crimes into a digital environment, and the emergence of new types of crime that substantively exist only in a digital environment. These two components are defined here as published by Statistics Canada, and have been echoed in many of the research sources we identified:

- Traditional crimes now being conducted through the use of computers or technology:

  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.[1]

- New crimes that involve acts against computers and technology directly:

  The second category is defined where the computer is the object of the crime. Cybercrime 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.[1]
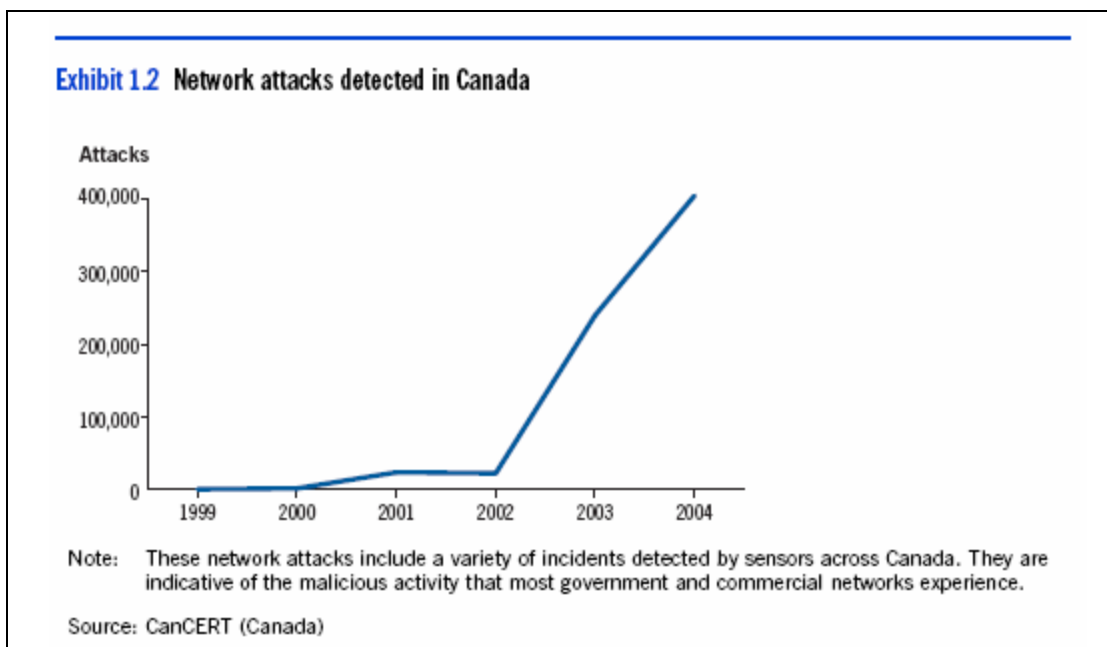
---

[1] Catalogue no. 85-558-XIE Cybercrime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics. Canadian Centre for Justice Statistics

Comments from law enforcement professionals and Crown Prosecutors underline their appreciation for both the extensive use of computers and information technology by criminals in perpetrating both traditional and new criminal activities in Canada. For example, consider the advancement of cell phones, which have been transformed from pure voice communication devices with limited capabilities to a full mobile computing device offering online and global connectivity. Such devices often include complex security features for privacy protection that often pose challenges to law enforcement even when they may be legally entitled to review the information on those devices. Traditional crimes such as drug trafficking now almost always include an analysis of cell phones when individuals are arrested.

> "...a lot of the investigators have come to realize just how much information is available in PDA's and cell phones, and in the last year we have seen a dramatic increase in the number of PDA's and cell phones that are being sent in for examination, just to download the data for intelligence purposes. It's far outstripping our predictions and probably will quickly outstrip our capability to deal with it." - Municipal Policing Senior Manager

Cybercrime, by any definition, potentially affects all Canadians and organizations within Canada. Our personal and corporate information, whether it is with our financial institutions, retail outlets where we shop or with our Government, is digitally stored and accessed.

Much of the critical infrastructure within Canada is also digitally controlled or accessed making the exposure to malicious cyber attacks an increasingly real threat. In 2005, the last year that Canada's Auditor General reported on the state of IT security for the Government of Canada, the trend of Network Attacks had risen dramatically as shown below:

Exhibit 1.2 Network attacks detected in Canada

Note: These network attacks include a variety of incidents detected by sensors across Canada. They are indicative of the malicious activity that most government and commercial networks experience.

Source: CanCERT (Canada)

Cyber incidents have risen significantly since 2001, and the increase and the patterns are similar in Canada and in the U.S. However, only a small percentage of incidents are actually reported. Network attacks are a good indicator of the real risks. Since our last 2002 Report, these attacks have increased dramatically, which shows how easily and quickly they can be launched.[2]

---

[2] Report of the Auditor General of Canada – February 2005

2. Challenges and opportunities in terms of cooperation and sharing of information

With an estimated 85% of Canada's critical infrastructure being owned and operated by the private sector, the coordination and collaboration between the private sector and government for the protection of the cyber elements in Canada's critical infrastructure is a key concern. Public Safety Canada outlined specific cybercrime elements related to critical infrastructure in its 2003 "Threat Analysis Report TA03-001." Public Safety Canada outlines the following[3]:

> Malicious computer-based threats to Canadian Critical Infrastructure are characterized by a number of elements which make them both difficult to predict and detect:
>
> - The problem of hacker identification is particularly difficult in a domain where maintaining anonymity is easy and where there are sometimes time lapses between the intruder action, the intrusion itself, and the actual effects. In addition, the continuing proliferation of sophisticated computer technologies into the mainstream population makes assigning attribution increasingly difficult.
>
> - The threat is not restricted by political or geographical boundaries. Attacks can originate from anywhere in the world and from multiple locations simultaneously. Investigations and back tracking through a web of false leads and unwittingly slaved systems can be time consuming and resource intensive to pursue.
>
> - The threat environment is extremely fluid. The window of time between the discovery of vulnerabilities and the creation of a new tool or technique to exploit the vulnerability is rapidly decreasing.
>
> - The technology employed for attacks is simple to use, inexpensive, and widely available. Computer intruder tools and techniques are widely available on computer bulletin boards and various web sites as are encryption and anonymity tools.
>
> - These methods of attack have become increasingly automated and more sophisticated resulting in more damage from a single attack.
>
> - The tools used in attacks are often similar or identical to, those technologies which are employed to ensure network reliability.
>
> - The cost required to develop a significant attack capability continues to decrease.
>
> - Publicly and privately controlled infrastructures are becoming increasingly networked/interconnected/interdependent and, as a result are becoming more vulnerable to a diverse number of threats. The phenomena make it harder to differentiate between the author or authors of electronic attacks as well as other system-related malfunctions. While lead federal agencies have had some notable successes in ascertaining the identity of malicious code authors, tracking down and apprehending them has proven more difficult, costly and resource intensive. Ironically, the very innovations that are spurring economic development and driving globalization are rendering users vulnerable to more diverse threats.

---

[3] Public Safety Canada: Threats to Canada's Infrastructure. http://ww3.ps-sp.gc.ca/opsprods/other/TA03-001_e.asp

The costs associated with the events as outlined by Public Safety Canada were described by interviewees as being substantial.

Through our interviews with law enforcement agencies across Canada, a consistent theme was the need for increased coordination and collaboration both across Canada and internationally in combating cybercrime. Investigators dedicated to technological crime units and law enforcement management told us that many of their successes in investigating and apprehending cybercrime offenders were made possible by the informal networking relationships they have with other agencies.

> *"We're not leveraging the intellectual abilities of the universities. We're not leveraging the capacity of industry with their ability to operate internationally, their expertise, their equipment, infrastructure and we're not leveraging ability of police to operate their investigative abilities and their international contact networks. We're simply not connecting everybody in a way that we should. We have all the ability in the world to really seriously kick butt on internet crime. Nobody has ever just been given the incentive to. "* - Policing Technology Expert

> *"When we get our act together and cooperate we can be very effective. We are not anywhere near coordinated enough and what we are also not doing is leveraging the power of all the good guys. We tend to operate in silos. Once again we have law enforcement, we have private security, we have different segments and we're not working with each other enough. Police know how to investigate things. Industry has the technical expertise. Universities have research expertise. We have all kinds, we have all the pieces to the puzzle but we're not putting the pieces together and making the puzzle."* - Technology Expert

> *"If there's a way we can find a mechanism for funding some research labs across the country, that would prove of real benefit to cyber security in Canada, protecting critical infrastructure."* - Federal Policing Technology Expert

Input from law enforcement suggests that that there is considerable duplication of effort, and no formal process to share advances being made or to stay on top of the latest technology. Centralizing the collaboration and coordination between law enforcement, government and private sectors in efforts to fight against cybercrime have been established in the U.S. and U.K. These examples such as the National Cyber Forensics & Training Alliance (NCFTA) in the U.S. and the Child Exploitation and Online Protection Centre (CEOPS) in the U.K. are examples of the coordination of responses to cybercrime matters through centers developed for specific purposes. NCFTA was developed several years ago in the U.S. and has established key partnerships and hosts resources between industry, law enforcement & academia in a facility that allows subject matter experts from these sectors to share expertise and intelligence in the development of solutions towards cybercrime issues. Specifically the FBI, National White Collar Crime Center, Carnegie Mellon University, and West Virginia University form the key partnerships within NCFTA that represent the stakeholder groups. CEOPS was established with a similar model but with specific focus towards eradicating child exploitation through partnerships with law enforcement, government and corporations. Specifically, through partnerships with entities such as Microsoft, Visa, SERCO and government agencies and corporations.

> *"What we need is to have a centre of excellence where everybody is brought together, you've got to have some Crown representatives there to work and some government representatives to make sure that we're on top of the rules, are keeping up with the new crimes that are coming on board."* - Tech Crime Police Supervisor

"...traditional methods of fighting and prosecuting crime no longer apply. Sharing of tools and expertise within law enforcement is essential in achieving this as well as partnerships with other government agencies and the private sector." – Tech Crimes Supervisor

"National level partnerships need to be forged and bring all those people to the table in order to share investigative techniques so that we're not reinventing the wheel for instance. And that's where at a national level if partnerships are occurring they're able to share ongoing investigations, new investigative techniques that have been successful or failed or otherwise. And then we think on a proactive basis at the national level I think that's where it should occur." - Police Organized Crime Supervisor

Due to the global nature of cybercrime matters and the increased need to obtain evidence from foreign jurisdictions, a desire for a centralized and coordinated approach to assist with international liaisons and facilitation of investigations was identified.

"So at the highest levels of government this has to be considered a priority and at least start the discussion in terms of modernizing the ability of transmitting evidence across borders because it's not slowing down the bad guys. They're not stopping because it's in a different country. They're taking advantage of that. I mean, if I was a criminal online I'd want to be looking for victims in some other country just because I'm sure that's it got to be more difficult to get me from one country to the next." - Provincial Crown Prosecutor

"...In some cases it's frustrated our ability completely because all the evidence that we need is found in foreign countries and the time and effort required to try to gather the evidence is it worth it, given the dollar value of the fraud or whatever the case may be." - Provincial Crown Prosecutor

Interviewees also commented that opportunities for sharing and collaboration with the Canadian public through prevention education were limited by resource constraints:

"I think really from a law enforcement perspective, that's one of our gap areas to be addressed. Because the people with specialized expertise in this area are in such demand, and we have service shortfalls and backlogs, and we are trying to clear the cases, we're not out there being as pro-active as we should be. In any mission you read for police service units, To Protect, Detect and Investigate, and to be honest, in our program, the prevention is one of our Achilles heels. It's one of the weak links that we have, in my view." - Federal Technology Crimes Supervisor

"I think there's another fabulous opportunity for Canada to take the lead and that's to actually implement a cyber safety program in our academic curriculum starting at preschool because these kids are already using computers at home and so that if it's part of the curriculum for every year of every school from preschool through to university" - Post Secondary Research Coordinator

3. The resources required to advance the battle against cybercrime

The topic of detection and enforcement resources dedicated to cybercrime matters was identified as an area of discussion by those stakeholders interviewed. Law enforcement and Crown Prosecutors told us they would like to have dedicated cybercrime trained resources to effectively investigate and prosecute cyber criminals. Technical training for law enforcement through the national Canadian Police College was regarded as one of the highest caliber curriculums available to law enforcement, albeit limited numbers can be trained. We were informed of situations where designated technological crime investigators had to wait over a year to attend their first foundational Canadian Police College training course in the investigation of technological crime.

> *"I believe by and large most law enforcement agencies are under resourced for their tech crime requirements and therefore being under resourced, they're under capacity and if a child exploitation thing is going on then they take their limited resources and put it there, therefore leaving any other cyber facilitated crime available so if I'm out there in the real world and I know that all your resources are on the ICE unit chances are you're attracting another client in towards another, into your financial fields or other fields." - Federal Police Senior Manager*

> *"I'm astonished at how few resources there are to online fraud." - Provincial Crown Prosecutor*

The "2007 Internet Crime Report" released by the Internet Crime Complaint Center (IC3) shows that the financial losses of referred cases to law enforcement is increasing. For 2007, IC3 referred a total of $US239.09 million in claimed financial losses from various forms of cybercrime. This amount is an increase from the $US198.44 million claimed in 2006 as also reported by IC3. From a global perspective, of the 206,884 complaints received in 2007 by IC3 of cybercrime matters, Canada was the second highest country from which complainants filed reports of having being victimized by cybercrime, with approximately 4,344 complaints.[4]

Similar trends of increased reporting to law enforcement of cybercrime matters is outlined in the 2007 "CSI Computer Crime and Security Survey" by the Computer Security Institute where 29% of responding organizations reported computer intrusions to law enforcement from 25% the previous year. In a similar trend, the average annual financial loss reported by responding organizations rose to $350, 424 per organization from $168,000 the previous year.[5]

- ### Cybercrime training for Crown Prosecutors

The ability of Provincial Crown prosecutors to thoroughly understand the technical issues of cybercrime activities is proving to be a challenge facing Provincial Attorneys General. In terms of resource allocation, while the police are now coming up to speed both at the municipal and federal level by training investigators and setting up dedicated sections; the Prosecution Services across Canada have not been as quick to respond to cybercrime matters.

The benefits of having Crown Prosecutors knowledgeable in various cybercrime issues provides for an increased degree of understanding of the technical aspects of the matters being presented before the Court, which is a positive contribution in prosecuting such cases.

---

[4] 2007 Internet Crime Report: Internet Crime Complaint Center IC3
[5] CSI Survey 2007: Computer Security Institute

"The idea of this unit is that the prosecutors in it are specially trained in computers, the technology, the forensics, that kind of thing so that when we get a file we can be more or less on the same page as the investigators." - Provincial Crown Attorney

- **Dedicated child exploitation initiatives**

Among the most successful initiatives are the various Integrated Child Exploitation (ICE) Units established across Canada. As a partnership between federal and municipal law enforcement agencies, the ICE units use dedicated investigators and coordinated efforts focused towards a single objective of investigating child pornography and exploitation matters. Their collaboration and dedicated efforts are leading to higher levels of detection and conviction:

"The RCMP's National Child Exploitation Coordination Centre (NCECC), provides investigational support, expertise, training standards and tools to police services across Canada to combat child sexual exploitation on the Internet. Public Safety works closely with the Centre to develop policy that will address this problem. The NCECC also works with Cybertip.ca, Canada's hotline and reporting site for cybercrime activity" - Public Safety Canada

"We are seeing a lot more convictions and a lot more investigations because we have finally applied resources in most provinces." – Senior Child Exploitation Officer

We conducted an interview with Cybertip.ca, and were provided with the following statistics. Since the National Tip line went National in January 2005:

- over 24,000 reports have been received to date
- 40% of the reports are forwarded to law enforcement. 90% of the forwarded reports are in one of four areas; child pornography, online luring, child sex tourism and children exploited through prostitution
- 30 arrests have resulted based on reports filed with law enforcement
- almost 3000 websites have been shut down

Our interviews with law enforcement and Crown Prosecutors generated frequent requests to increase the resources dedicated to investigative and enforcement bodies. They outlined the following needs:

- an increase in the number of Crown Prosecutors trained in cybercrime matters across Canada
- an increase in training available to law enforcement either through the Canadian Police College or private industry
- additional funding for training in cybercrime matters, from private or public sector venues – wherever the expertise resides
- the rate of law enforcement agencies adopting a form of specialized cybercrime investigative capability to be mirrored by the respective Crown Prosecutors' offices

On a related note, concerns were also shared that the ability to share prevention education with the public was limited by resource constraints.

- **Retention of trained resources**

There is a perception that corporations are seeking many of the skill sets that are being developed within the law enforcement community. Therefore, there is an increased risk that law enforcement will have difficulties in retaining cybercrime investigative talent.

"Retention will always be an issue. Our specialized civilians here have all kinds of opportunities to go out and make more money than they make here. They are the guys that are developing the forensic utilities that we use, developing the specialized tools and things like that. Our regular members have tremendous opportunities to go out and work for organizations like yours and the banks and all the consulting companies, and the corporations are looking for people like that, so retention is always an issue." – Federal Tech Crime Supervisor

- **Increased focus on emerging cybercrime issues**

During the course of our interviews, two emerging issues - cyberbullying and organized crime - provided examples of how cybercrime continues to evolve.

Cyber Bullying: The ability to be connected to the Internet has introduced unique and challenging issues to groups such as schools, parents and students as it relates to cyber bullying. The traditional safe havens of a student's home and school classrooms are now disappearing as the Internet is not limited by these physical boundaries, but only limited by connectivity to the Internet. Children are now using the Internet to communicate with their peers, during school and at home:

"They don't even have a safe haven if they're being cyber bullied, there's nowhere that they can get away from it because they know who's doing it to them and they see them at school and then they come home and they turn on their computer and it's right there in their face and that's where some kids get desperate because they don't even have the safe haven of their home because they're being cyber bullied at home and when kids start turning off their computers that needs to be a wake up call to parents that they're afraid of something on there." – Crime Prevention Officer

The issues around cyber bullying and its associated affects have been researched by Tanya Beran of the University of Calgary:

> More than two thirds of students (69%) have heard of incidents of cyber-harassment, about one quarter (21%) have been harassed several times, and a few students (3%) admitted engaging in this form of harassment. These preliminary studies suggest that cyber-harassment is becoming a significant problem. Attempts to reduce this behaviour are complicated as "cyber-bullies" may be anonymous, and, therefore, difficult for school administrators and parents to identify. Considering that many illegal activities occur over the Internet (for instance, money laundering and theft of intellectual property), responsible behaviours must be promoted at an early age. As we learn more about cyber-harassment and develop strategies to manage it, administrators will likely experience difficulties with surveillance and other control mechanisms. However, just as smoking, littering, and driving after consuming alcohol have become socially unacceptable, attitudes about bullying in school and cyberspace need to change so that more support is provided to protect students from fear and intimidation from harassment that ultimately interferes with their learning. [Cyber-Harassment: A Study of a New Method for an Old Behaviour - Tanya Beran - Qing Li University of Calgary 2006]

Organized crime: This was described in two fashions – what would typically be known as "traditional organized crime," and criminals who used the Internet to become organized. This second description was particularly evident in the area of child pornography and the ability for individuals with that predilection to communicate in Internet venues.

Organized crime groups are often and increasingly involved in Internet-based crimes (e.g., identity theft, fraud, and online child exploitation). Using the Internet and related services to further their criminal activities, criminal organizations are able to recruit, plan, communicate, and raise and move funds for their endeavours. The borderless nature of the Internet, the relatively low risk of detection and high rewards, helps organized crime groups undertake international crimes. – Public Safety Canada

"I think organized crime has seen the advantages of using Internet based services, with regards to planning their activities, communicating, using the secure, anonymous aspect of it, actually doing some of their criminal acts through the Internet, or using the Internet services to facilitate it, the same way a business would. Business uses it because it is quick, cheap and secure communications around the world. The criminals are definitely going to exploit that, the same way the terrorists would. They recruit people through it, they find people of like minds and like interests, and I think organized crime, national security threats, are using it extensively." – Federal Technology Crime Supervisor

"Ready access to others with the same predilections that you can now rationalize with each other and exchange strategies on hiding evidence and of meeting children and all that so the cybercrimes that we're seeing, we're seeing them increasing exponentially because more and more people are drawn to it." – Child Exploitation Investigator

Our research into the effects of "Organized Crime" and the implications for businesses outlined findings in a 2002 CERT® report that stated that "Organized Crime" has indeed availed themselves of individuals with technical competencies to assist in their illegal activity.

> Criminal organizations have increasingly hired financial specialists to conduct their money laundering transactions. This adds an extra layer of insulation while utilizing legal and financial experts knowledgeable about the layering of financial transactions and the availability of safe havens in offshore financial jurisdictions. Similarly, organized crime does not need to develop technical expertise about the Internet; it can hire those in the intruder community who do have the expertise, ensuring through a mixture of rewards and threats that they carry out their assigned tasks effectively and efficiently.[Organized Crime and Cybercrime: Implications for Business- Phil Williams, CERT® Coordination Center 2002]

4. The status of Canadian anti-cybercrime legislation and the global context

During the course of our interviews, we were told by a variety of stakeholders that there is a desire to review and where necessary update Canadian legislation in response to current cybercrime activities. We were reminded that Canada is a signatory to the Council of Europe's 2001 Convention on cybercrime; however, as yet, there has been no ratification to this agreement.

"We're not there in terms of the Canadian legislation, we have signed onto this Treaty, but we can't ratify as a Nation, until such time as we have the legislation in place in the Criminal Code that will allow us to respect every aspect of that Cybercrime Convention." – Federal Technology Crime Supervisor

In a document on this Convention, the Department of Justice for Canada points out that changes to current legislation which would have to be adopted in order to comply with the Convention's requirements[6]:

> The Convention will help Canada and its partners fight crimes committed against the integrity, availability and confidentiality of computer systems and tele-communications networks and those criminal activities such as on-line fraud or the distribution of child pornography over the Internet that use such networks to commit traditional offences. Most of the required offences and procedures already exist in Canada. However, before Canada can ratify the Convention and give it effect, the Criminal Code would need to be amended to include an offence in relation to computer viruses that are not yet deployed. Complementary or further amendments could be made to other existing laws, such as the Competition Act, in order to modernize them in accord with the Convention, notably in the areas of real-time tracing of traffic data and interception of e-mail.

Interviews indicated a level of confusion surrounding the various privacy laws and what can and cannot be released without the need of a court order. The Australia Cybercrime Act of 2001, the U.S. Homeland Security Act, and the USA Patriot Act of 2001 all provide provisions for mandatory compliance for law enforcement information requests. Canada has tabled the Lawful Access/Modernization of Investigative Techniques legislation which would address some of the privacy access concerns; however, as of 2008 it has not been ratified.

> *"Their legal advice is, if law enforcement comes and asks you for this piece of information on one of their users or subscribers, you should ask for a warrant. Well, our interpretation of the privacy law is that it's permissive and would allow us to get that without warrant if they want to voluntarily provide it to us. It would be nice if we had legislation that made it clearer to them that that was the spirit and intent of the legislation."* - Federal Tech Crimes Supervisor

Mutual Legal Assistance Treaties (MLAT)

MLATs were seen by law enforcement and Crown Prosecutors as being ineffective as a legislative tool in combating cybercrime, primarily due to the issue that digital evidence is moved, altered, or deleted with such great ease. The need for legislation and methodologies to secure digital evidence from our international MLAT partners in a timely fashion was mentioned frequently as an issue. These issues may be addressed if legislative changes permitting the ratification of the Council of Europe Convention are passed.

> *"The MLAT process was never intended for evidence that is literally volatile. I mean digital evidence when it goes away there's no microfiche; it's not sitting in some box in a banker's basement. It is truly gone and the MLAT process was never intended for that. Hotmail, Gmail, they're hosted in the United States they have no Canadian presence. If we need evidence from them we have to go through the MLAT process which is six to nine months down the road and sometimes at that stage of the investigation we don't even know who the suspect is. We're doing that to identify the suspect and so if it's gonna take nine months to even get to the point where you can write a search warrant to get into the guy's house, the odds of the evidence still being on his computer are really slim. And so what we try to do is we try to encourage the investigators to contact the other end, contact the police in the other*

---

[6] Department of Justice http://www.canada.justice.gc.ca/en/cons/la_al/a.html

> *jurisdiction and open up a joint investigation so that they can use their legal processes to get the evidence much quicker."* - Provincial Crown Prosecutor

Canada Evidence Act

Crown prosecutors pointed out that in their view legislative changes to the Canada Evidence Act to permit affidavit or video evidence would assist in the prosecution of multi jurisdictional cybercrime cases:

> *"They need to broaden the ability to have evidence given in court by other than, what lawyers call viva voce, means in person, live means. We need to be able to utilize paper documents like affidavits and use the technology."* - Provincial Crown Prosecutor

> *"… one solution is to amend the Criminal law and the Law of Evidence, Canada Evidence Act in this country to permit people to give evidence by other means other than physically having to come to Canada to do that."* - Provincial Crown Prosecutor

On August 25, 2002, the Canadian Department of Justice, Solicitor-General and Industry Canada released a consultation document[7] which proposes to amend several Canadian statutes, including the *Criminal Code* and the *Competition Act*, in preparation for ratifying the Council of Europe's *Convention on Cybercrime*. The proposal discusses new investigatory powers for law enforcement, which would be exercised under lower judicial standards than those now applied to search and seizure warrants and intercepts under the *Criminal Code*; a requirement that telecommunications and Internet service providers make their networks "wiretap" compliant; mechanisms for providing subscriber and service provider information to law enforcement, and the creation of new criminal offences for virus production and dissemination.

Unsolicited E-mail Legislation (SPAM)

A number of stakeholders described spam as a significant problem and believe that legislation enabling Canadian entities to defend and support stronger enforcement should be put in place.

> *"There are significant legal gaps in Canada to defend against spam and related online threats like spy ware and phishing and therefore its recommended that we upgrade our legislation to deal with it and support stronger enforcement."* - Federal Agency Analyst

We reviewed numerous sources that outlined evidence to support the conclusion that spam has increased significantly in the last number of years. MessageLabs Intelligence provides these statistics from January 2008:

- Spam – 73.4% overall (an increase of 0.3% since December); the level was 69.5% in the U.S., 72.5% in Canada, and 63.8% in the UK.
- Viruses – One in 131.4 emails in January contained malware (an increase of 0.1% since December)
- Phishing – One in 147.5 emails comprised a phishing attack (an increase of 0.13% since December)

---

[7] Cybercrime and lawful access Lex Informatica. http://www.lexinformatica.org/Cybercrime/ Aug 2004

In a publication provided to us by Industry Canada, six recommendations were made with respect to legislation, regulation and enforcement by the Spam Task Force in May 2005. The recommendations for creation of new legislation have not been implemented. The recommendations on international cooperation have, however, resulted in participation in such groups such as Organization for Economic Co-operation and Development, which involves over 30 countries cooperating to develop policy on SPAM issues.[8]

Child pornography legislation

During our review, the issue of mandatory reporting requirements with respect to child pornography was discussed.

> *The Federal Provincial Territorial (FPT) Cybercrime Working Group, which is co-chaired by Justice Canada and British Columbia and includes provincial Justice and Public Safety Department representatives and a number of federal departments (e.g. Public Safety, Industry and Statistics). The work of this group has led to important reforms in the Criminal Code of Canada, including the creation of a child-luring provision within the Code. The working group is currently examining the mandatory reporting of child sexual exploitation by ISPs. - Public Safety Canada*

The Government of Manitoba has taken the lead in Canada and proposed a bill in November 2007 under Provincial legislation that would provide for mandatory reporting of child pornography to Cybertip.ca in the same way that it is currently mandatory to report child abuse to authorities.

In 2002 the U.S., Criminal Code 13032 (Reporting of child pornography by electronic communication service providers) included the duty to report as outlined here:

> Whoever, while engaged in providing an electronic communication service or a remote computing service to the public, through a facility or means of interstate or foreign commerce, obtains knowledge of facts or circumstances from which a violation of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 of title 18, involving child pornography (as defined in section 2256 of that title), or a violation of section 1466A of that title, is apparent, shall, as soon as reasonably possible, make a report of such facts or circumstances to the Cyber Tip Line at the National Center for Missing and Exploited Children, which shall forward that report to a law enforcement agency or agencies designated by the Attorney General.

Australia passed legislation that came into effect in 2005 that requires ISPs and Internet Content Hosts to report child pornography to law enforcement. Specifically, Australian Criminal Code 474.25 (Obligations of Internet service providers and Internet content hosts) states that:

A person commits an offence if the person:

a) is an Internet service provider or an Internet content host;
b) is aware that the service provided by the person can be used to access particular material that the person has reasonable grounds to believe is:
   i. child pornography material; or
   ii. child abuse material; and

does not refer details of the material to the Australian Federal Police within a reasonable time after becoming aware of the existence of the material.

---

[8] Stopping Spam – Creating a Stronger, Safer Internet – Task Force on Spam – 2005

Summary

In summary, through the interviews of select stakeholders and open research, it was reinforced that:

- The unclear definition of cybercrime in Canada is hindering the efforts to detect, deter and prevent it.
- Opportunity exists for more dedicated resources to increase the collaboration and coordination of stakeholders in the response to increasing the effectiveness of cybercrime prevention, detection, enforcement and prosecution.
- The need to ensure timely and relevant changes to legislation to address cybercrime issues.

Appendix A

A Public Survey on Cybercrime Matters in Canada

In conjunction with Ipsos Canada, an online survey of residents of Canada was performed. The final survey sample includes responses from 587 respondents.

- 53% of the respondents were Female.

- 76% of the respondents were English speaking.

Geographic Regions

Geographically, our largest number of participants resided in Ontario and Quebec. The number of respondents was consistent with the population bases of each province.

- Ontario 38%
- Quebec 24%
- British Columbia 14%
- Alberta 9%
- Saskatchewan 4%
- Manitoba 3%
- New Brunswick 3%
- Nova Scotia 3%
- Prince Edward Island 1 %
- Newfoundland and Labrador 1%

Participation by region
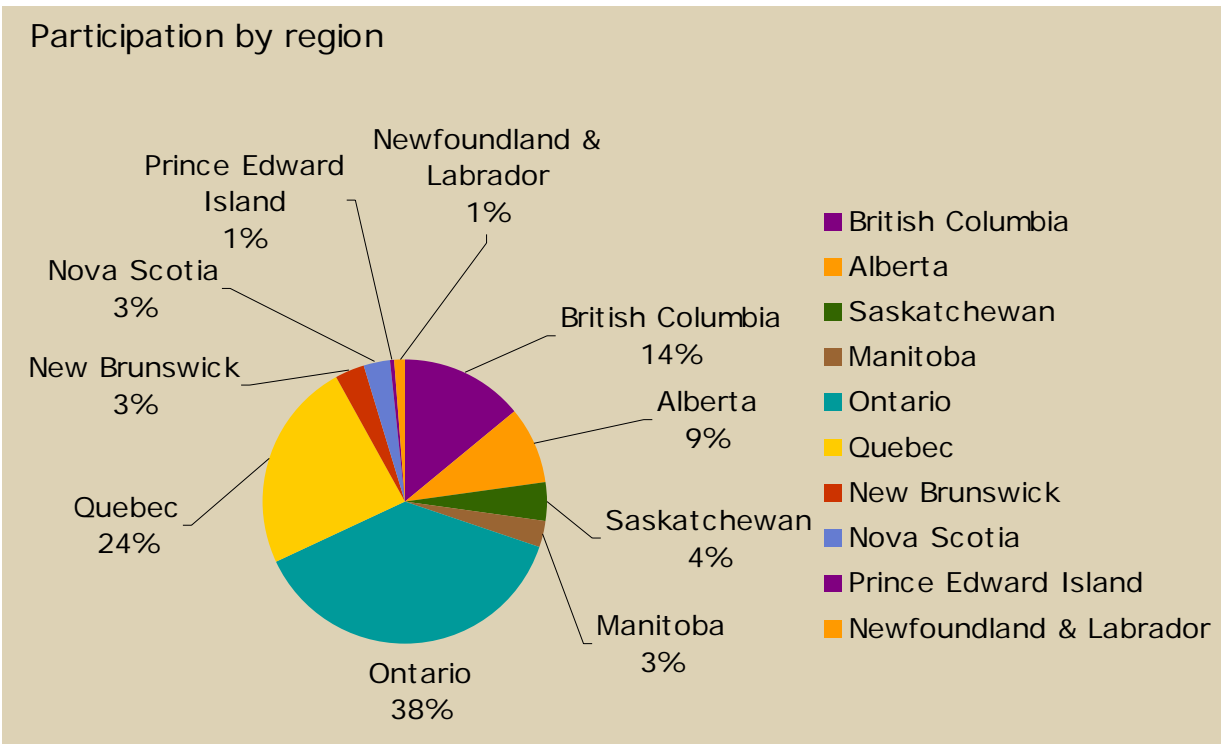
Survey Results

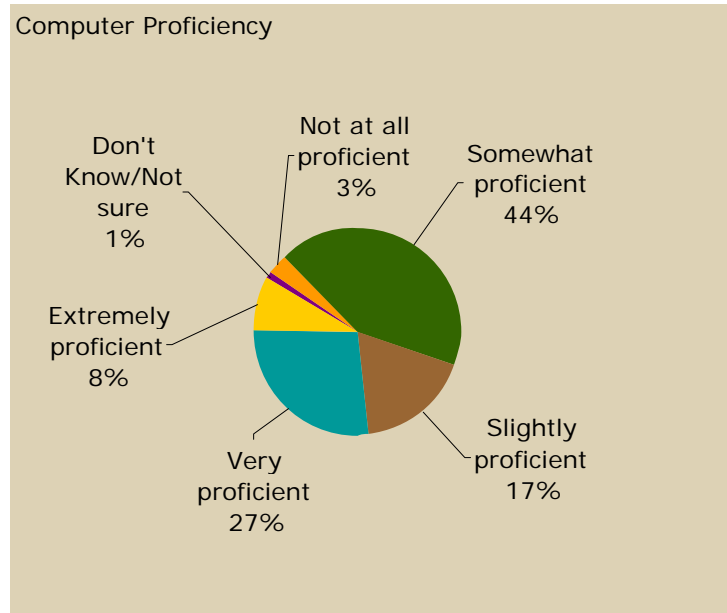The survey was developed by Deloitte and administered online by Ipsos Reid. A total of 587 individuals responded to the survey. The survey ran during the period January 23 through January 31, 2008. For certain questions not all respondents answered the question or gave multiple responses. The number of respondents to those questions is noted under the appropriate chart.

Q1. How would you rate your proficiency with a computer?

Computer Proficiency

- Not at all proficient 3%
- Somewhat proficient 44%
- Don't Know/Not sure 1%
- Extremely proficient 8%
- Very proficient 27%
- Slightly proficient 17%

Q2. How often do you use the internet?

Average Internet Usage

- Weekly 6%
- Daily 94%
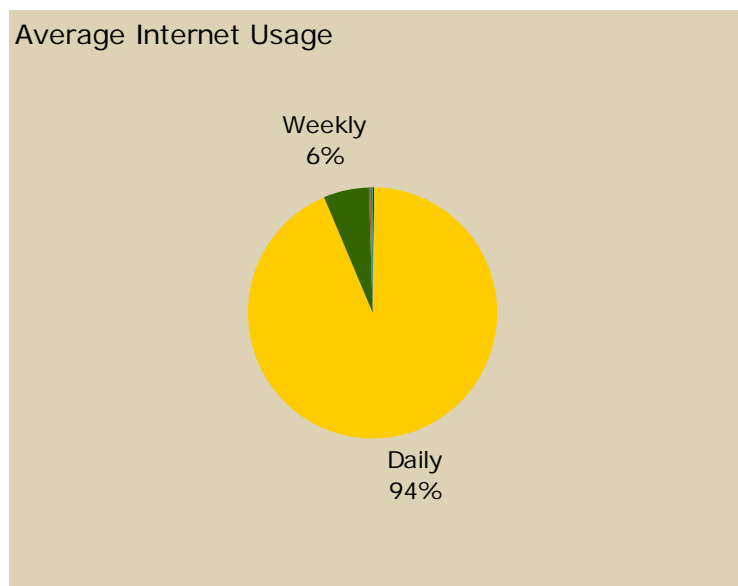
Q3. Select the activity you spend the majority of your time when on the Internet?

Primary Internet Use

Social Networking: Email, Instant Messenger, social network — 50%

Entertainment : Music, Movies, Games, etc. — 19%

E-Commerce: (Banking, Shopping) — 9%

Educational — 5%

Business Related Activities — 11%

Legend:
- Entertainment : Music, Movies, Games, etc.
- Social Networking: Email, Instant Messenger, social network
- Business Related Activities
- Educational
- E-Commerce: (Banking, Shopping)
- News/ information/ research
- Travel information/ booking
- E-mail

Q4. How often do you make purchases online?

Online Purchase Frequency

Did not know/ Not sure — 2%
Daily — 1%
Weekly — 4%
Monthly — 28%
Yearly — 25%
Less Often — 19%
Never — 21%
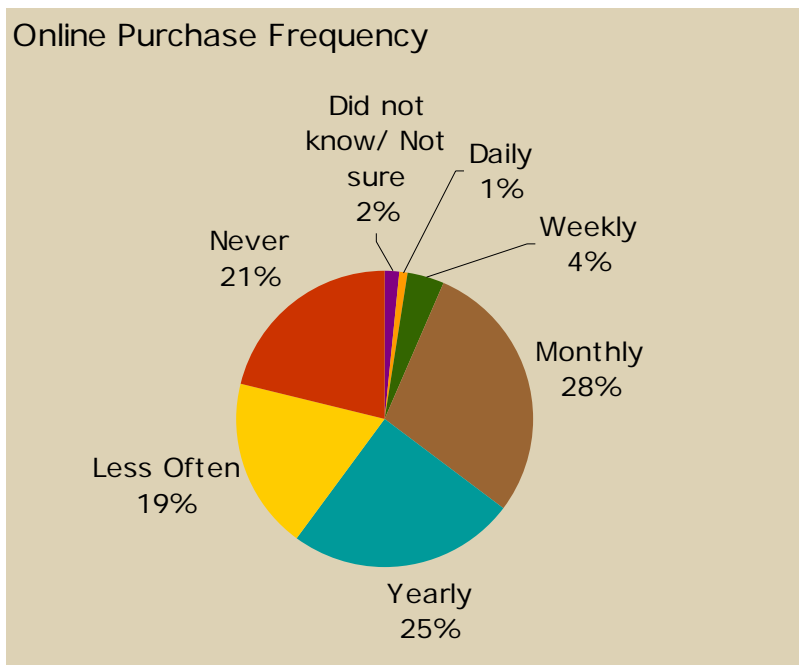
Q4b. When making purchases online, how confident are you that your information is kept secure and private?

Online transaction security confidence

- Don't Know / Not Sure 1%
- Not at all confident 5%
- Slightly confident 10%
- Somewhat confident 46%
- Very confident 33%
- Extremely confident 5%
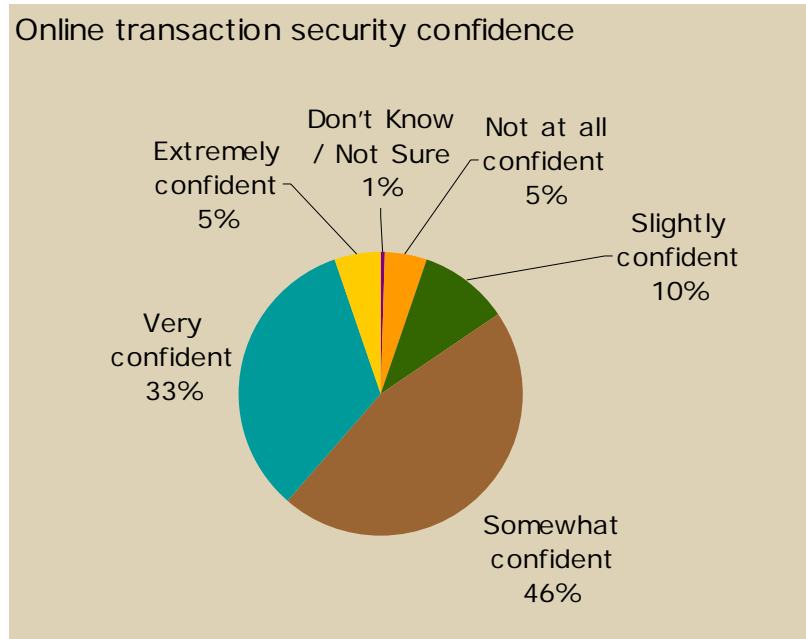
Q5. How often do you conduct financial transactions online? (e.g. Internet banking, checking your balance)

Online Financial Transaction Frequency

- Did not know/ Not sure 1%
- Daily 15%
- Weekly 44%
- Monthly 15%
- Yearly 1%
- Less Often 3%
- Never 21%
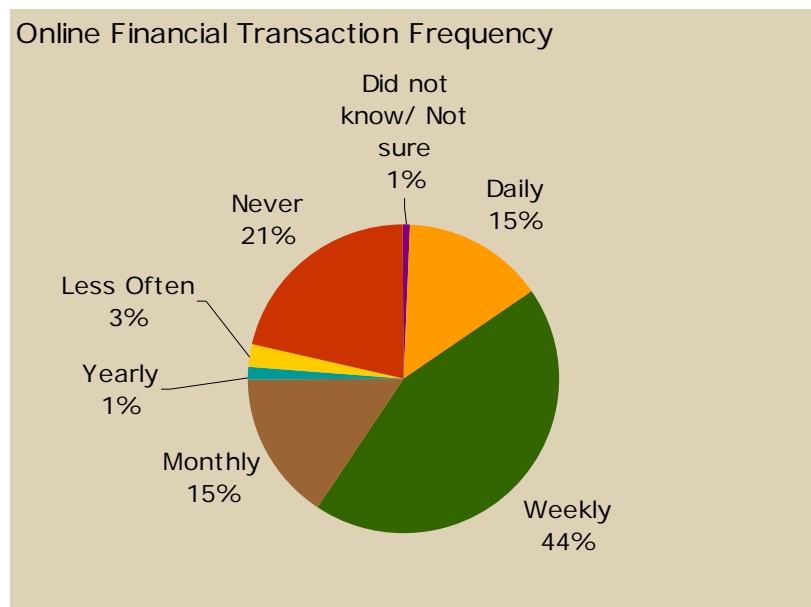
Q6. What, if any, type or types of Cybercrime have you been a victim of?

Types of Cyber Crimes

Child pornography 1%

Computer viruses 32%

I have not been a victim of cyber-crime 51%

Financial fraud 4%

On-line harassment 6%

Other 3%

Legend:
- Child pornography
- Computer viruses
- Financial fraud
- Identify theft
- On-line harassment
- Sale of illegal goods or substances
- Other
- I have not been a victim of cyber-crime
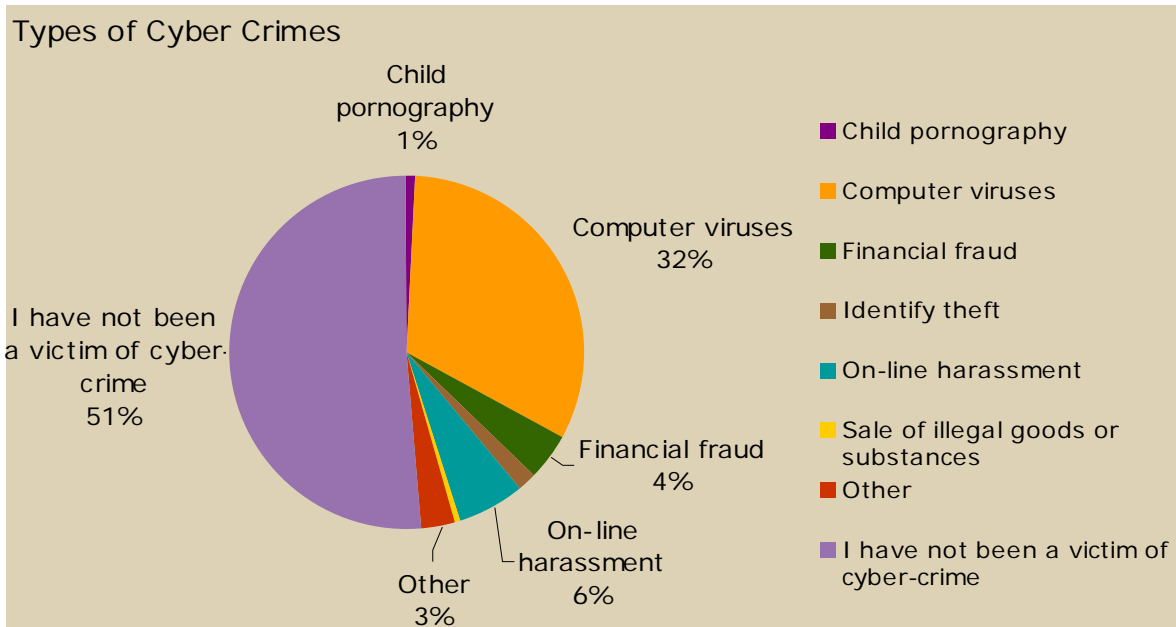
There were 658 responses to this question.

Q7. How many times have you been impacted by Cybercrime within the past 12 months?

Frequency of Victimization - Past 12 Months

Category	Respondents
No impact in the past 12 month	60
1 time	63
2-3 times	73
4-6 times	13
More than 6 times	21
Don't Know /Not Sure	21
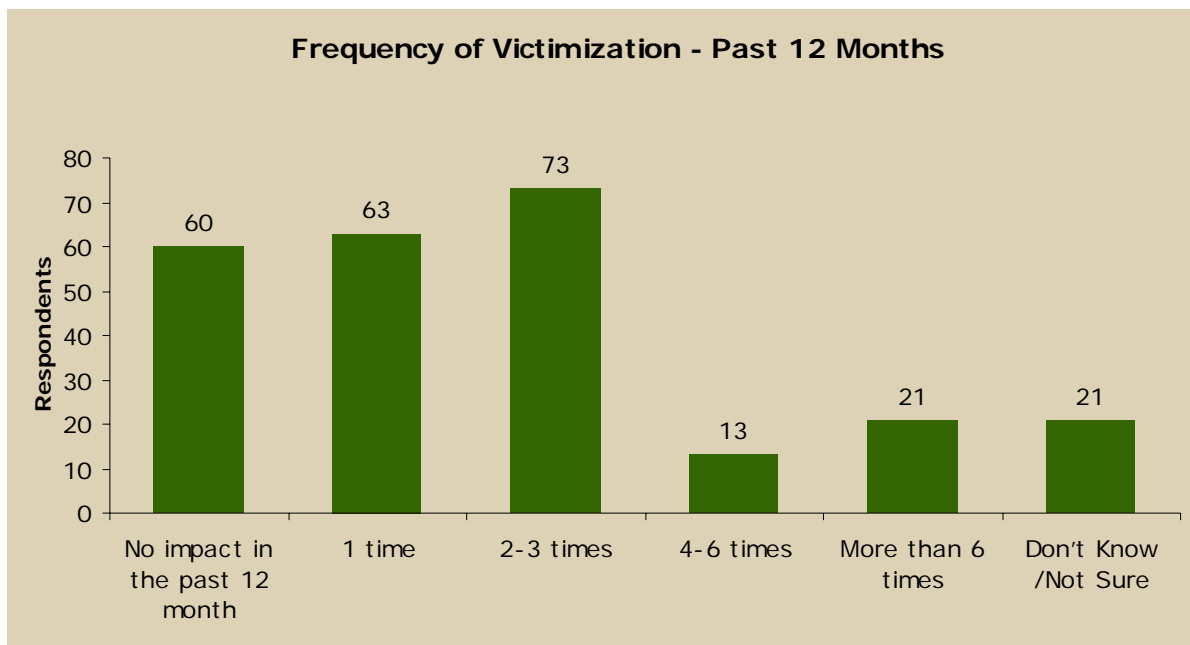
There were 251 responses to this question.

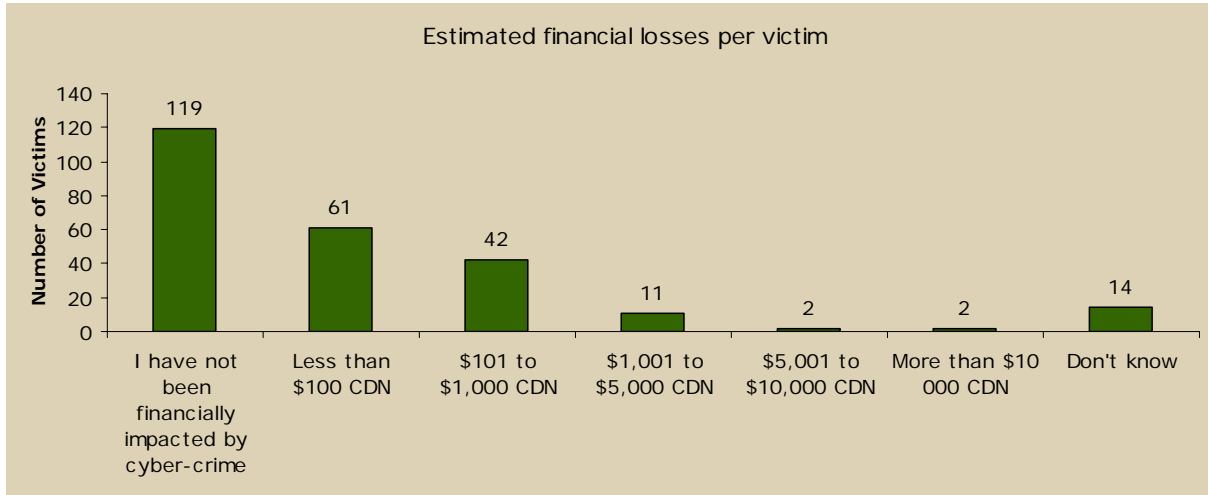## Q8. What has been the total estimated financial impact of cybercrime on you?

Estimated financial losses per victim

Category	Number of Victims
I have not been financially impacted by cyber-crime	119
Less than $100 CDN	61
$101 to $1,000 CDN	42
$1,001 to $5,000 CDN	11
$5,001 to $10,000 CDN	2
More than $10 000 CDN	2
Don't know	14

There were 251 responses to this question.

Q9. Is Cybercrime a concern for you?

Is Cyber Crime a Concern?

Yes 86%

No 14%
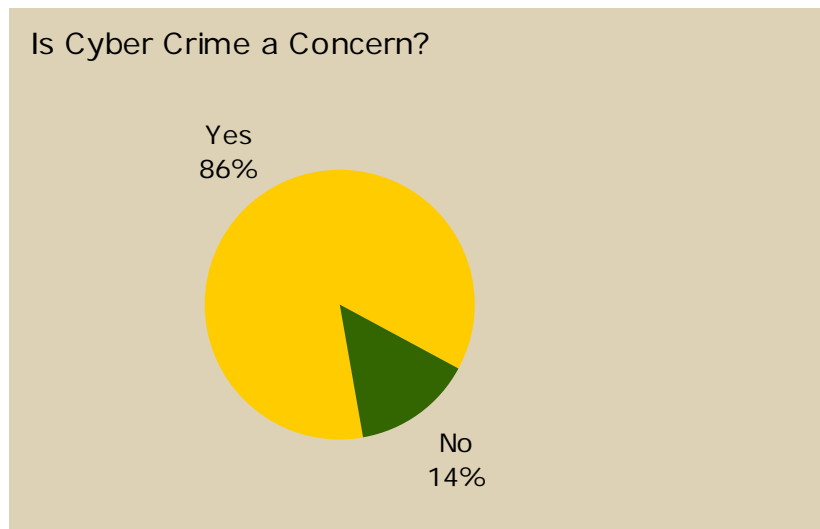
Q10. How likely do you believe that people are targeted for a Cybercrime?

Are People Targeted for Cyber Crime?

- 3%
- 2%
- 11%
- 16%
- 31%
- 37%

Legend:
- Not at all likely
- Slightly likely
- Somewhat likely
- Very likely
- Extremely likely
- Don't Care / Not Sure
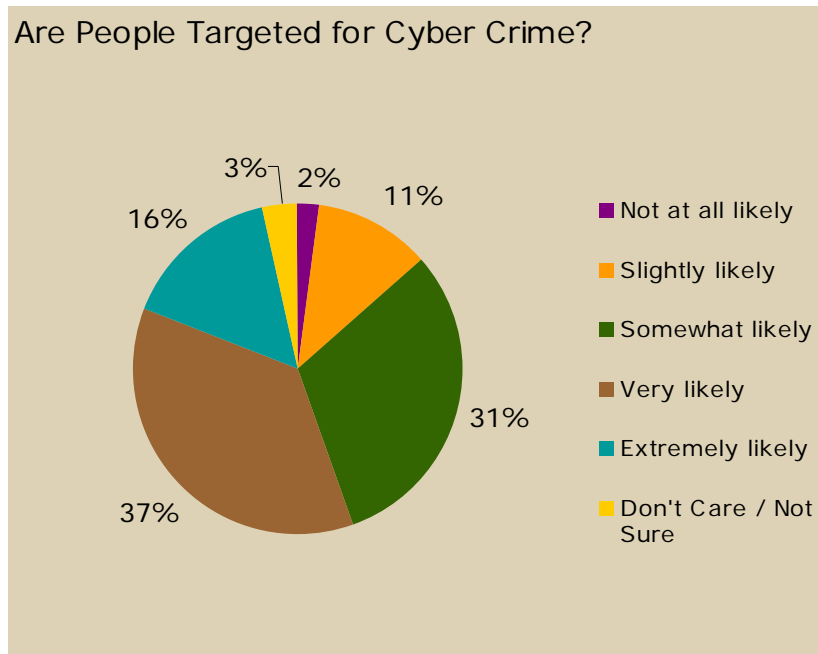
Q11. How likely do you believe you are to be targeted or exploited by Cybercrime?

Are You Targeted for Cyber Crime?

- Extremely likely 3%
- Don't Care / Not Sure 7%
- Not at all likely 12%
- Very likely 13%
- Somewhat likely 30%
- Slightly likely 35%

Q12. What do you see as the biggest threat to you in terms of Cybercrime?

Greatest Threat

Identity Theft 34%

Financial Fraud 25%

Don't Know / Not sure 5%

On-line harassment 2%

Computer viruses 32%

- Don't Know / Not sure
- Financial Fraud
- Identity Theft
- Computer viruses
- Other
- Sale of illegal goods or substances
- Child pornography
- On-line harassment
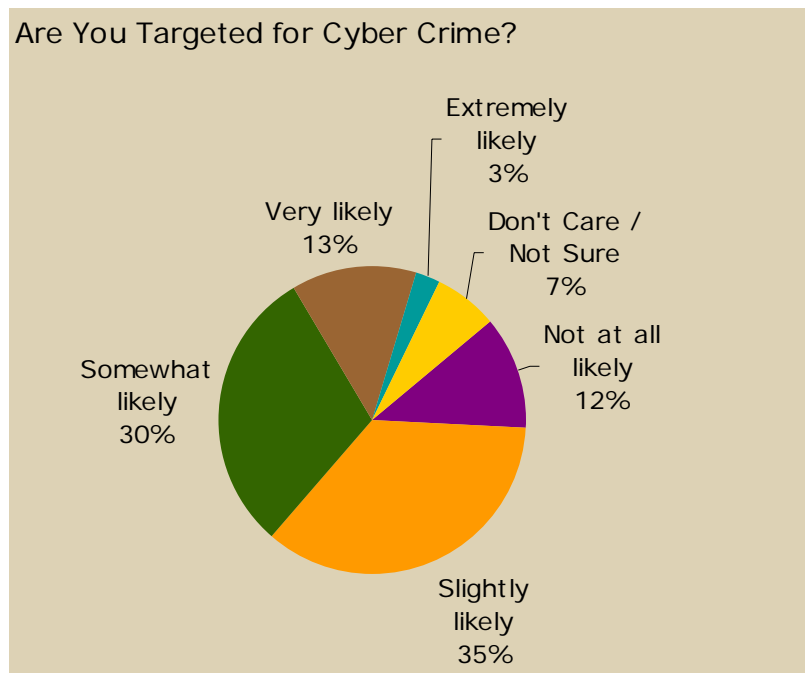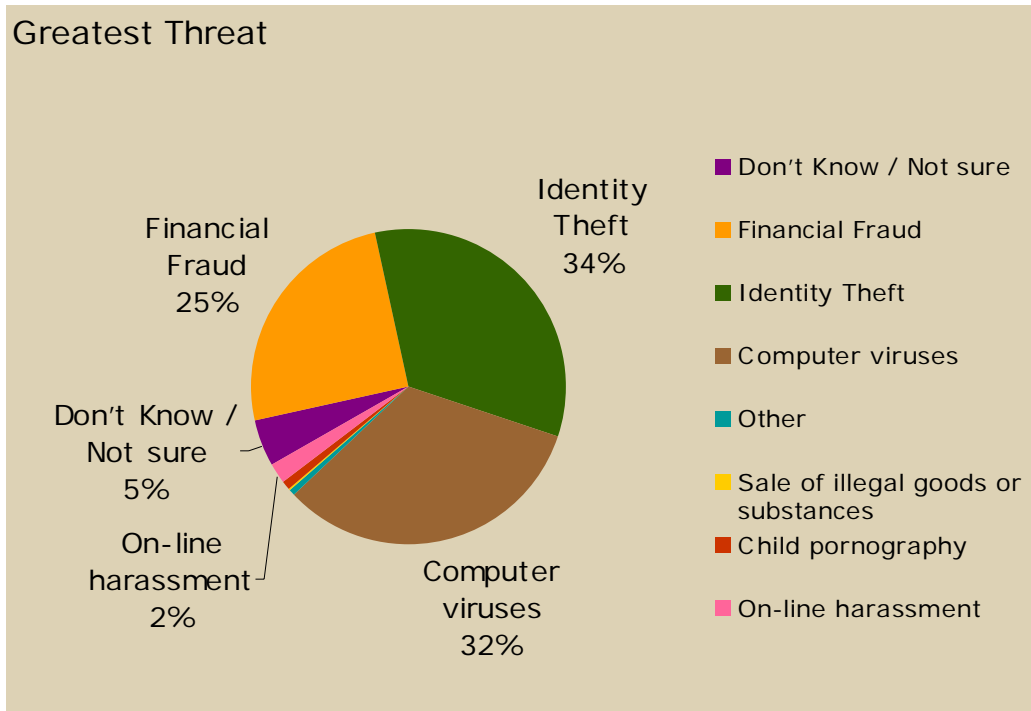
Q12b. What do you see as the next biggest threat to you in terms of Cybercrime?

Greatest Threat

Don't Know / Not Sure 7%

On-line harassment 8%

Child pornography 4%

Sale of illegal goods or substances 2%

Financial Fraud 29%

Computer viruses 23%

Identity Theft 27%

- Don't Know / Not Sure
- Financial Fraud
- Identity Theft
- Computer viruses
- Other
- Sale of illegal goods or substances
- Child pornography
- On-line harassment
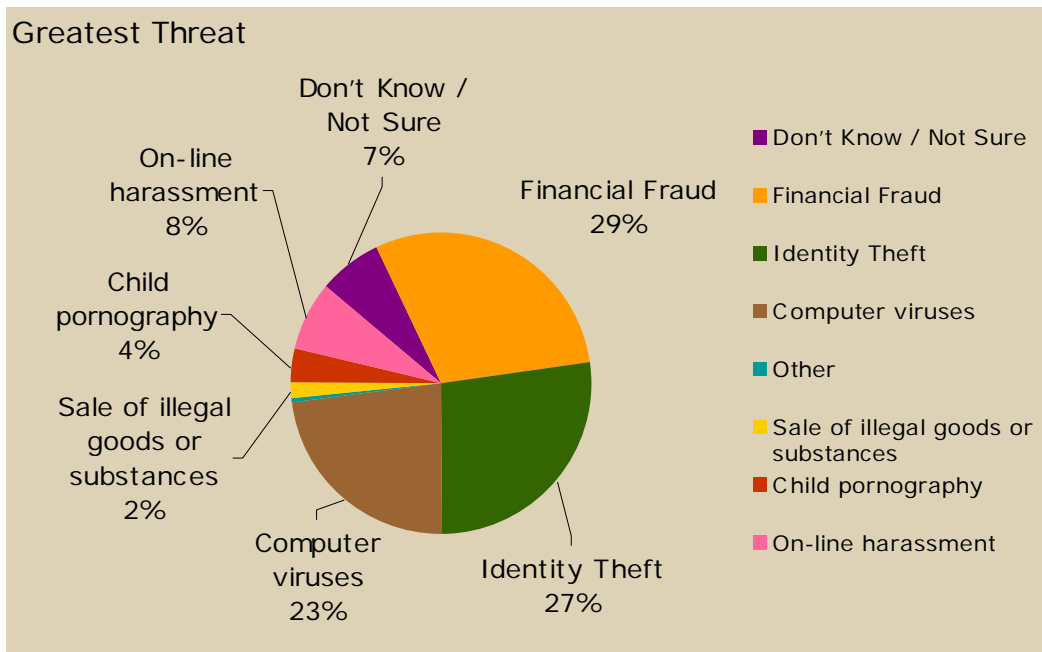
There were 561 responses to this question.

Q13. How much money have you invested to protect yourself against potential Cybercrime? (e.g. Purchase of firewall, virus scan software, new computer)
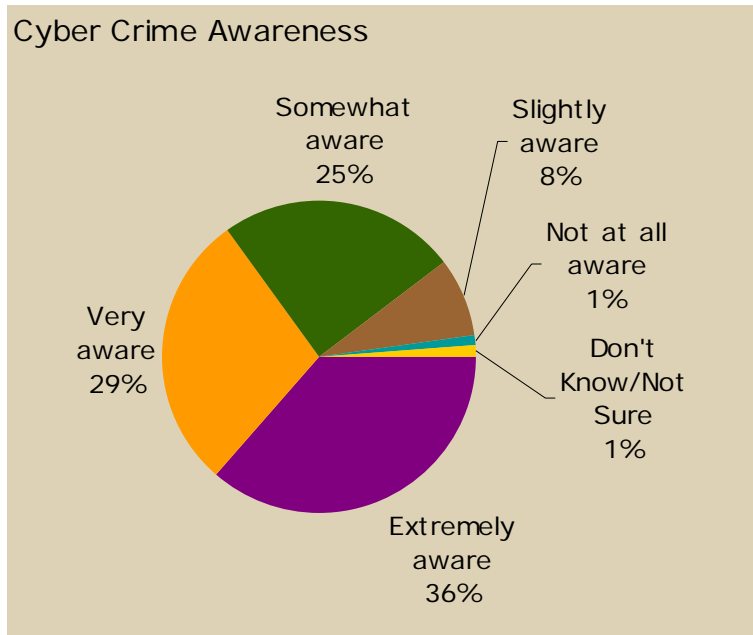

Money Invested to protect from Cyber Crime

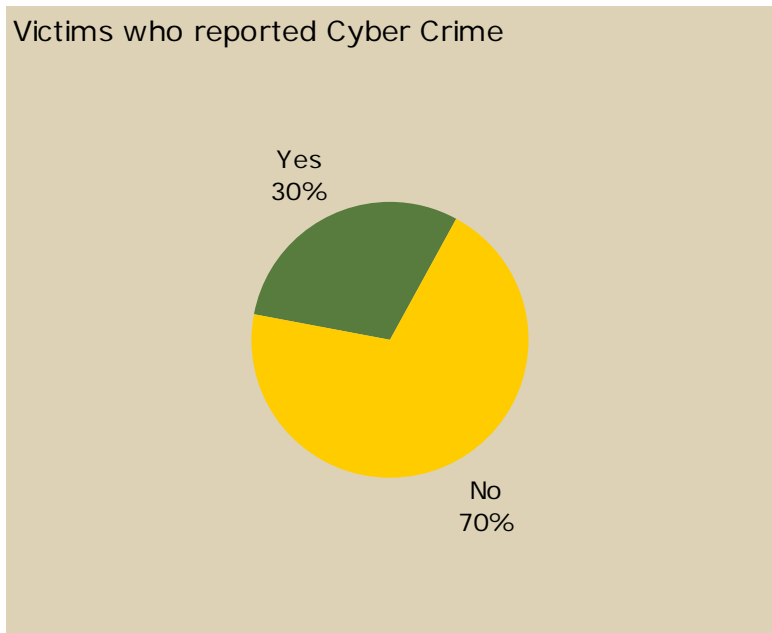**Q14. How has Cybercrime, or the potential threat of Cybercrime, impacted your interaction on the computer?**
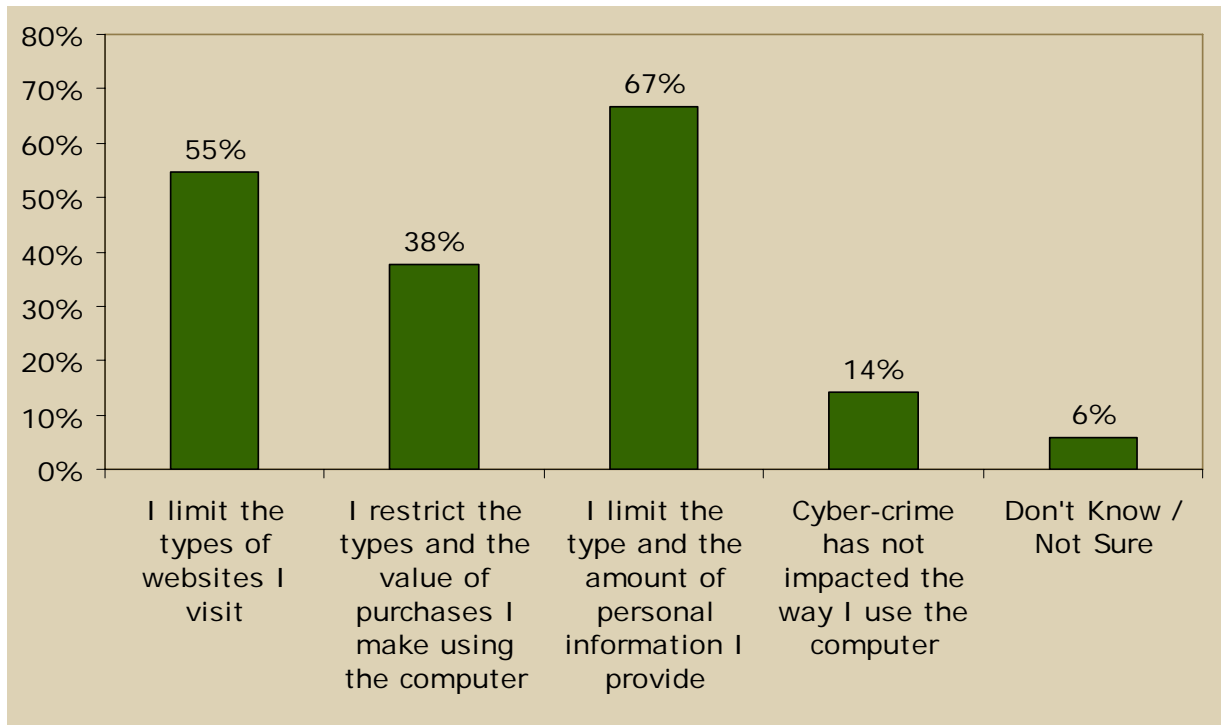
There were 919 responses to this question.

Q15. How aware are you of the threats posed by Cybercrime? (E.g. new email scams)

Cyber Crime Awareness

Somewhat aware 25%

Slightly aware 8%

Not at all aware 1%

Don't Know/Not Sure 1%

Very aware 29%

Extremely aware 36%

There were 755 responses to this question.

Q16. Have you ever reported a Cybercrime?

Victims who reported Cyber Crime

Yes 30%

No 70%

There were 251 responses to this question.

Q16b. Why haven't you ever reported a Cybercrime?

Reason for not reporting Cyber Crime

- ■ Because of the embarrassment of the situation
- ■ Law enforcement is powerless to do anything about it
- ■ Unlikely that any retribution and compensation will result
- ■ Unsure who to contact
- ■ Didn't know it could be reported
- ■ Affected by a computer virus
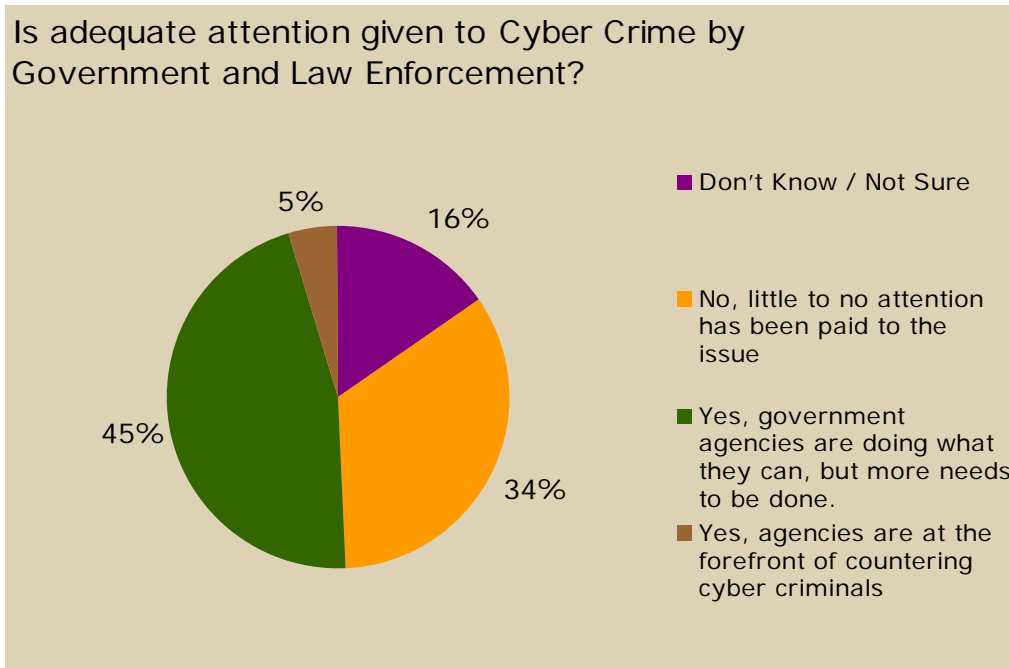- ■ Other
- ■ Don't know / Not sure

2%
10%
22%
4%
9%
7%
1%
45%
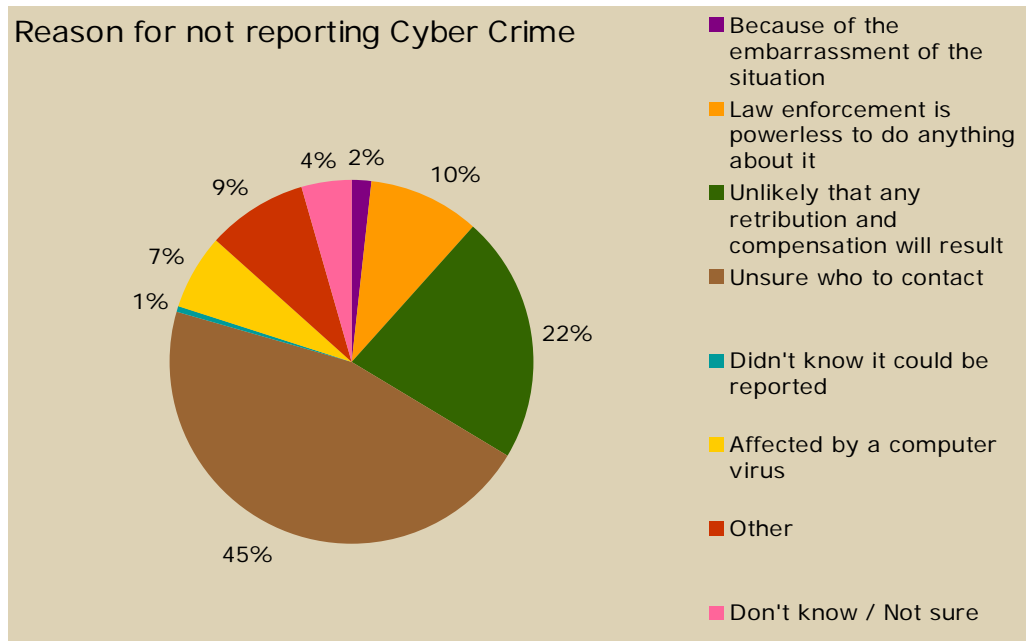
There were 179 responses to this question.

Q17. Do you think preventing Cybercrime is an important priority for government or law enforcement?

Is Cyber Crime a Priority to Government and Law Enforcement

Somewhat important 17%

Slightly important 6%

Not at all important 4%

Very important 35%

Don't know / Not sure 1%

Extremely important 37%
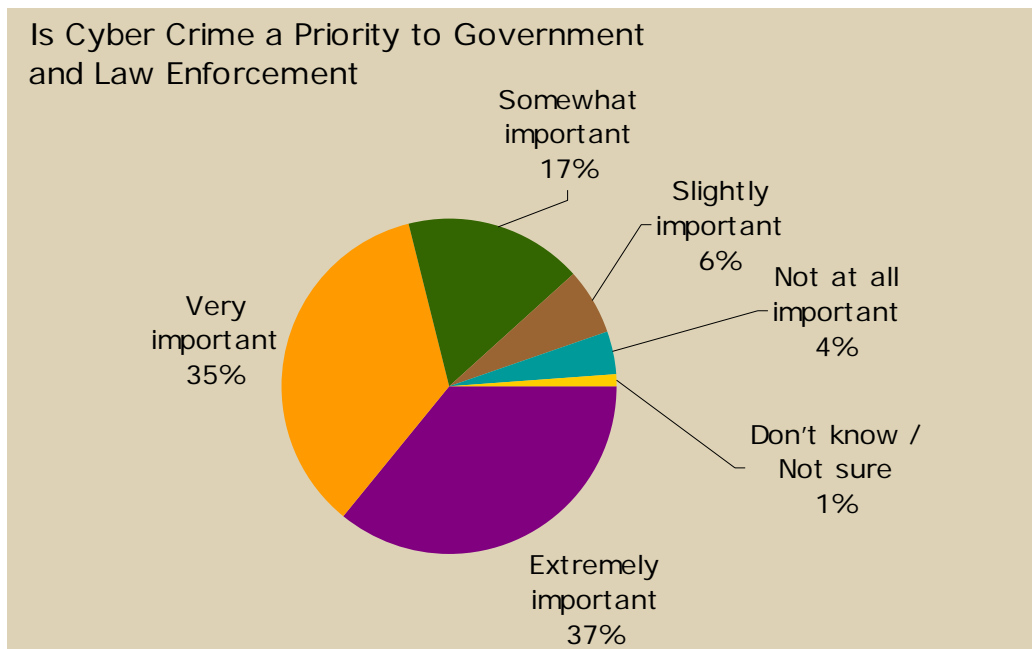
Q18. Do you believe that there is adequate effort given by governing bodies and law enforcement in combating Cybercrime?

Is adequate attention given to Cyber Crime by Government and Law Enforcement?

- ■ Don't Know / Not Sure
- ■ No, little to no attention has been paid to the issue
- ■ Yes, government agencies are doing what they can, but more needs to be done.
- ■ Yes, agencies are at the forefront of countering cyber criminals

5%
16%
45%
34%

Q19. Whose responsibility do you think it is to keep me safe from Cybercrime?

Who is responsible to protect us from Cyber Crime?

Internet Service Provider 21%

Government 12%

My own responsibility 34%

Online Service Provider 17%

Law Enforcement 16%
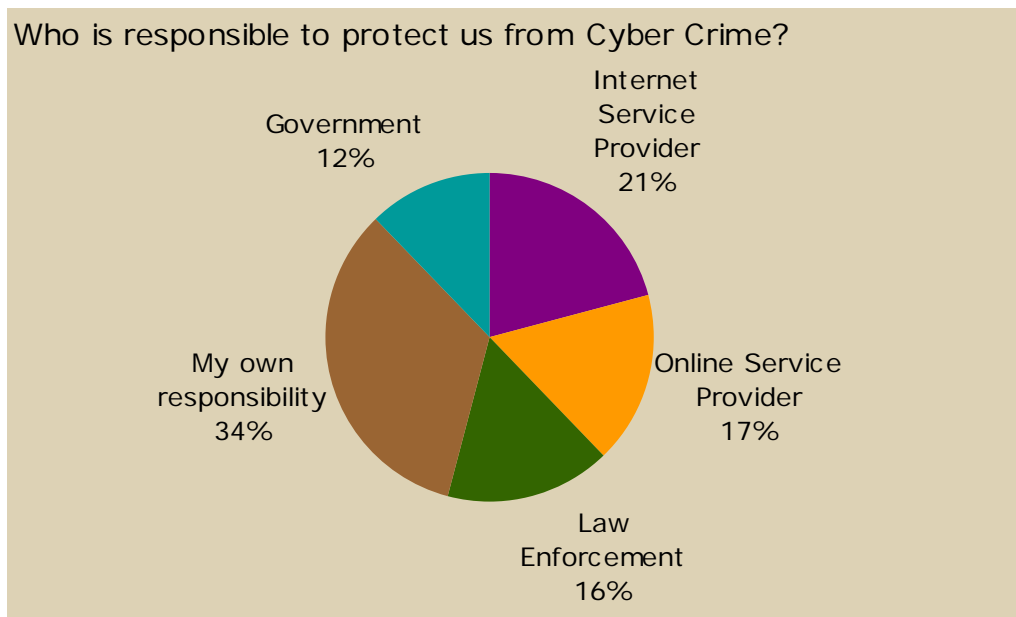
www.deloitte.ca

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services through more than 7,600 people in 56 offices. Deloitte operates in Québec as Samson Bélair/Deloitte & Touche s.e.n.c.r.l. The firm is dedicated to helping its clients and its people excel. Deloitte is the Canadian member firm of Deloitte Touche Tohmatsu.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms have any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

Member of
Deloitte Touche Tohmatsu