INTERNATIONAL TELECOMMUNICATION UNION

**ITU WORKSHOP ON
CREATING TRUST IN CRITICAL
NETWORK INFRASTRUCTURES**

**Document: CNI/07
20 May 2002**

Seoul, Republic of Korea — 20 - 22 May 2002

CREATING TRUST IN CRITICAL NETWORK INFRASTRUCTURES:

CANADIAN CASE STUDY

This case study has been prepared by Mike Harrop, President of the Cottingham Group and former Senior Project Officer with the Canadian Treasury Board Secretariat: < mharrop@magma.ca >. *Creating Trust in Critical Network Infrastructures: Canadian Case Study* is part of a series of telecommunication case studies produced under the New Initiatives Programme of the Office of the Secretary General of the International Telecommunication Union (ITU). Other country case studies on critical network infrastructures, can be found at <http://www.itu.int/cni>. The opinions expressed in this study are those of the author and do not necessarily reflect the views of the International Telecommunication Union, its membership or the Canadian Government. The author gratefully acknowledges the generous assistance of all those who have contributed information for this report.. In particular, thanks are due to staff of Industry Canada and the Office of Critical Infrastructure Protection and Emergency Preparedness for their help and suggestions and also for their permission to draw extensively on the reports "The Canadian Telecommunications Service Industry: 1999-2000", "Telecommunications Service in Canada: An Industry Overview, 2000-2001", and "Canadian Infrastructures and their Dependencies". Thanks are also due to the Communications Security Establishment, the Treasury Board Secretariat and e-Witness Internet Security Inc. for permission to include the material used to compile the case study, and for their kind assistance.

Table of contents

Executive Summary

This report presents an overview of the Canadian environment relating to the operation and use of telecommunications, particularly data communications, together with a look at critical infrastructures, their interdependencies and the organizations involved in their protection.

Canada is a vast country with an unusual richness of natural resources and a well-developed technological and communications infrastructure. Industry, government and the population as a whole are highly dependent on the traditional communications infrastructure and there is a growing dependence on the Internet in all areas. The size of the country, the diversity of the terrain, the remoteness of some communities, and the fact that centres of population are, to a large extent, widely separated, all combine to emphasize the importance of communications and to create major challenges to establishing and maintaining communications.

Responsibility for emergency measures in Canada is shared among three levels of government though the federal government is now leading and coordinating the overall effort towards critical infrastructure protection. Individual industries have working groups and committees examining protection of their own infrastructures and there is close liaison with the government agencies responsible for infrastructure protection.

Legal issues relating to network and data security are, for the most part, addressed by provisions of the Canadian Criminal Code, rather than by drafting individual laws to deal with network and data abuse.

In addition to being very important to all sectors of the Canadian economy, the telecommunications service industry is itself a key sector of the economy, employing 116,000 people in the year 2000 and generating revenues of CAD 32.6 billion. The sector covers all aspects of public communications services - wireline services, wireless, cable, and satellite as well as Internet services and private research networks.

With the exception of Internet services, most of the publicly-offered telecommunications services in Canada are subject to some degree of regulation, though deregulation has resulted in competition to at least some degree in most of the services. Under the *Telecommunications Act*, the federal government has a broad range of powers to ensure that rates are just and reasonable and that Canadian carriers do not discriminate unjustly or accord any undue preference with respect to the telecommunications services they offer.

The federal government's convergence policy announced in 1996 to encourage, among other things, interconnection, interoperability, unbundling of network facilities, and competition, has resulted in significant convergence of the broadcasting, telecommunications and publishing sectors.

Both government and the financial services industry are highly dependent on public and private telecommunications facilities for internal operations as well as for service delivery. Both sectors use private networks extensively and both sectors are also increasingly dependent on the public Internet for service delivery. Although the financial services industry is very reluctant to disclose information about its networks or about contingency planning, the criticality of networking can be deduced from publicly-available information. Any operations failure on the part of the financial services industry would have a serious impact on the rest of industry and on the economy.

An indication of the magnitude and importance of financial transactions can be deduced from some of the more visible transactions. For example, in 1999, the value of inter-bank settlements was more than 30 times Canada's gross domestic product. Canadians are also world leaders in the use of direct debit cards with the number of transactions in 2001, exceeding 2 billion, which represented CAD 94.9 billion in sales. On the busiest single day in 2001, 10.8 million direct debit transactions were posted. PC & Internet banking showed an increase of almost 74 per cent in 2000 over 1999 while telephone banking increased over 16 per cent in the same period.

All governments in Canada are moving to on-line service delivery with the federal government aggressively pursuing its Government Online initiative. Eleven million federal income tax returns were submitted electronically in 2001.

The report also looks at the relationship of telecommunications and other elements of the Canadian critical infrastructure, especially the importance of networks to business and commerce. In particular, the potential

impact of network failure on various sectors is discussed along with possible mitigation measures. The telecommunications infrastructure itself must be regarded as a vital element of the critical infrastructure. While the primary focus of this part of the report is on the impact of telecommunications failure on other sectors, there is also the question of the infrastructure elements (particularly electricity) on which the telecommunications infrastructure itself is dependent.

A two-part case study is also presented. The first part describes an approach to providing common perimeter defence for a large, diversified organization. The second part describes an approach to protecting sensitive data during transmission and while in storage.

The report contains nine conclusions and identifies areas where further study appears to be warranted.

1 Introduction

This paper presents an overview of the Canadian environment (political, geographic, demographic and economic), the key organizations responsible for infrastructure protection in Canada and the overall networking infrastructure. In addition, the importance of networking infrastructures to the financial and government sectors is reviewed and a summary is provided to illustrate the dependence of sections of the Canadian infrastructure on telecommunications networks. Finally, a case study is included to illustrate two important aspects of protection associated with computer networks.

In general, organizations are understandably reluctant to publish or disclose information about their critical infrastructures or dependencies. The information in this paper has, therefore, been compiled from publicly-available sources. A great many papers and reports have been examined and interviews have been conducted with officials from the public and private sectors. Key input for the report has been derived from comprehensive reports previously prepared for Industry Canada and the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) and from official surveys conducted by Statistics Canada. This data has been supplemented by information from many other government and industry reports and from the interviews.

Many organizations in Canada are engaged in preparing for, or coordinating, emergency measures and responses. In spite of the reluctance of individual sectors to discuss critical dependencies, a large amount of general information is available about critical infrastructures and about organizations and services that would be impacted by their failure. In fact there is far too much information to provide a fully comprehensive look at the entire Canadian environment. As a result, this report focuses on providing a broad overview of the Canadian environment with the objective of highlighting the key organizations, services and infrastructures and providing an indication of some of the most pressing issues that need to be addressed. It is evident from the information used to compile this paper that critical elements of the Canadian economy are highly dependent on telecommunications and that the telecommunications infrastructure itself must be considered a critical infrastructure component.

Although the information and experiences reflected in this report are those of Canada, for the most part the conclusions and lessons learned are applicable in a much broader context. It is hoped that the information presented here will provide valuable input to the international discussions on this important topic.

2 The Canadian environment

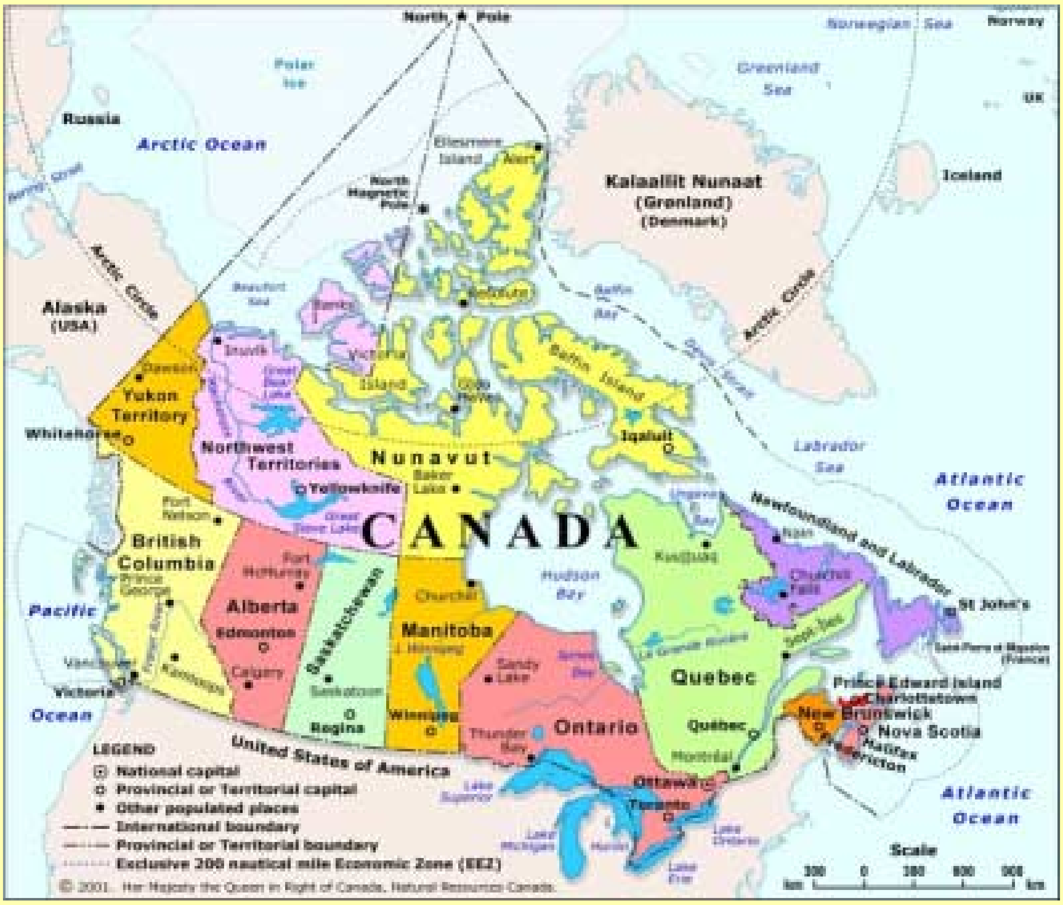
2.1 The Canadian political structure

Canada is a constitutional monarchy and a federal state with a democratic system of government based on the Westminster model. The Head of State is Queen Elizabeth II who is represented in Canada by the Governor General who is appointed by the Queen on the advice of the Prime Minister. The ten provinces and three territories that form the Canadian federation each have their own elected legislatures and governments.

The federal government has responsibility for national defence, foreign relations, interprovincial and international trade and commerce; the banking and monetary system, criminal law and fisheries. In addition, the courts have awarded the federal Parliament regulatory powers in areas such as aeronautics, shipping, railways, telecommunications, and atomic energy. The provincial governments are responsible, within their own jurisdictions, for education, property and civil rights, the administration of justice, health care, natural resources within their borders, social security, and municipal institutions. A number of responsibilities are shared by the federal and provincial governments. In addition, the federal government has delegated some specific federal responsibilities to some of the provinces.

As we shall see in later sections of this report, the federal government has some of the leading policy, regulatory, technical and coordination responsibilities relating to critical infrastructure protection.

Figure 2.1: Canada's Provinces and Territories



Source: Natural Resources Canada

2.2 Geography and demographics

Geography and population distribution have a very significant impact on the provision of network services in Canada.

Few people outside Canada have any real appreciation of the vastness of the country. In fact, Canada is the second largest country in the world with 6.7 percent of the world's land area, encompassing almost 10 million square km., spanning 6 time zones and bounded by the Atlantic, Pacific and Arctic Oceans. Figure 2.1 shows a map of the country with the 10 provinces and 3 territories. In travel time, it takes about 9 hours to fly from the eastern-most city (St. Johns, Newfoundland) to the most westerly city (Victoria, British Columbia). And a flight from southern Ontario to Alert in the far North takes about 10 hours in a Hercules aircraft.

The ten provinces and three territories, which can be seen in Figure 2.1, form six distinct geographic regions. Starting in the far north we have permafrost, tundra and land and water that is frozen for eight or nine months of each year. Moving over to the west of the country have mountainous terrain about 800 kilometres wide, including high mountain ranges, rugged plateaux and deep valleys. The Canadian shield, with its forests, lakes and tundra, occupies about half the country, stretching around Hudson Bay and east to the Atlantic. Southeast of the Canadian Shield is the fertile agricultural land of Southern Ontario and Quebec, the most densely populated and urbanised part of the country. Lastly, in the east of the country, we have the Atlantic Provinces with their highly varied terrain of mountains, ridges, plateaux, valleys, plains and rugged coastlines.

Geography alone creates some interesting challenges in providing a communications infrastructure over such distances and varied terrain. However, the population distribution adds another interesting dimension. The total population of this vast land is just over 31 million people. Most of those people live in the urban centres and, as noted earlier, the most densely populated region is Southern Ontario and Quebec.. Table 2.1 shows population by province and clearly indicates the heavy population concentration in central Canada (62 per cent of the total population live in Ontario and Quebec) . It is to be noted that 50 per cent of the population live in the 10 largest urban centres and that the bulk of the population is concentrated in a 5000 km-long strip of land about 300 km deep along the Canada-US border. Telecommunications service can be provided with relative ease in the urban centres but servicing the smaller, remote communities that in many instances are separated by hundreds, or even thousands, of kilometres, presents some major challenges.

Table 2.1: Population by Province/Territory

Province/Territory	**2001 Population**
Newfoundland	533,761
Prince Edward island	138,514
Nova Scotia	942,691
New Brunswick	757,077
Quebec	7,410,504
Ontario	11,874,436
Manitoba	1,150,034
Saskatchewan	1,015,783
Alberta	3,064,249
British Columbia	4,095,934
Yukon	29,885
Northwest Territories	40,860
Nunavut	28,159

Source: Statistics Canada

2.2.1 The Canadian people

Canada’s aboriginal peoples, the North American Indians and the Inuit, now form a relatively small segment of the population (about 2.8 per cent of the total population). Since the 17th century, immigrants have populated what was (and still is to a large extent) a relatively empty land. Canada’s bilingual (English/French) heritage comes from former links to the British and French empires and until the middle of the last century, most of the country’s immigrants still had British or French roots. Now however, with immigration from all over the world, Canada is becoming more multi-lingual and multicultural. In the 1996, 28 per cent of respondents indicated their ethnic origin as other that Canadian, British or French. Linguistically 59 per cent of the population speak English as their mother tongue and 23 per cent speak French.

Canadians are well educated. Around 15 per cent have a university degree while a further 37 per cent have attained a post-secondary certificate or diploma or have other post-secondary training. Canadian per capita incomes, while not the highest in the world, certainly support a high overall standard of living for the majority of the population. The 1999 pre-tax income for the average two-person economic family was CAD 63,818 and the after-tax income CAD 51,473.[1]

On a personal level, Canadians are heavily dependent on network infrastructures. Telephone service extends to virtually every home in the country and 72 per cent of homes are wired for cable TV. Computers are installed in 54 per cent of the homes. Modems are installed in 47 per cent of homes and 42 per cent of homes have Internet access. Canadians are frequent users of telephone touch-tone services for banking, bill payment and information services. They are also heavy users of credit cards (for which virtually all merchants have on-line verification facilities) and direct debit cards (use of which is also authorized on-line).

2.3 Industry, trade and commerce

As Table 2.3 indicates, the most important contributors to the GDP are the manufacturing and financial services sectors. In summary, manufacturing represents 32.8 per cent of the GDP and services 64.7 per cent.

Table 2.2 summarizes the major exports and imports for the country. Although Canada exports goods and services world-wide, its largest trading partner by far is the United States which accounts for 85 per cent of its exports and 74 per cent of its imports.

Table 2.2: Major Canadian exports and imports in 2000

Major Canadian imports (2000)	**Value (CAD millions)**	**Major Canadian exports (2000)**	**Value (CAD millions)**
Machinery and equipment	122,674.4	Machinery and equipment	106,885.6
Automotive products	77,402.7	Automotive products	97,940.6
Other consumer goods	40,089.2	Industrial goods and materials	65,916.6
Industrial and agricultural machinery	29,810.1	Energy products	52,928.0
Agricultural and fishing products	18,567.9	Forestry products	41,755.8
Energy products	17,863.8	Agricultural and fishing products	27,366.8
Special transactions trade	6,622.8	Other consumer goods	14,805.1
Forestry products	3,063.7		

Source: Statistics Canada

[1] Figures used in this report are in Canadian dollars unless stated otherwise. As of March 2002, the Canadian dollar was worth around USD 0.63 or 1.4 Euros.

Table 2.3. Gross Domestic Product (GDP) at basic prices

Gross Domestic Product at basic prices	**Year 2000 in** **Constant 1992 CAD (millions)**	**% of Total**
All industries	786,838	100%
Manufacturing	143,122	18.2%
Finance, insurance and real estate industries	126,571	16.1%
Communications and utility industries	56,381	7.1%
Retail industries	50,822	6.5%
Wholesale industries	50,320	6.4%
Business service industries	49,666	6.3%
Government service industries	47,201	6.0%
Health and social service industries	46,449	5.9%
Construction	42,289	5.4%
Educational service industries	40,860	5.19%
Transportation and Storage	36,418	4.2%
Other service industries	29,924	3.8%
Accommodation, food and beverage service industries	21,008	2.7%
Primary Industries	**Constant 1997 CAD (millions)**	**% of Total**
All industries	929,556	100%
Agriculture, forestry, fishing & hunting	22,862	2.5%
Mining and Oil and Gas extraction	36,125	3.9%

Source: Statistics Canada

2.4 Laws and policies that address network security

2.4.1 Legislation

In Canada, for the most part, legal issues relating to network and data security are addressed not in individual laws drafted specifically to deal with network and data abuse, but under provisions of the Canadian Criminal Code, which takes a functional approach to computing, telecommunications devices and services, and data abuse. (This approach is quite different from that of the US which has many different laws covering various aspects of this area.) Many aspects of unlawful behaviour relating to networks and data are therefore, covered by the provisions of the Criminal Code. Similar penalties apply for similar offences, regardless of the instrument of abuse. Whether an offence relates to networks, computing, telecommunications or other services does not make that much difference from an enforcement perspective under the Criminal Code.

For example, data modification, network interference, network sabotage, and virus dissemination are covered under Part XI of section 430 of the Criminal Code which deals with *wilful and forbidden acts in respect of* *certain property*. Data interception, unauthorized access and additional virus dissemination are covered under Part IX of section 342.1 dealing with *offences against rights of property*. Additional data interception provisions dealing with invasion of privacy are addressed in Part VI of section 184 while Part IX of section 322 deals with *data theft and offences against rights of property*. Computer related-fraud is addressed in Part X of section 380 which deals with *fraudulent transactions relating to contracts and trade*. A summary of relevant sections of the Criminal Code is contained in Annex B.

Canada signed the Council of Europe Convention on Cyber-Crime on 23 November, 2001 and continues to be active in the G8 Lyons Group on High-Tech Crime. The Canadian Government is now examining what changes to current criminal law might be required in order to implement the Council of Europe convention. Of particular relevance to protection of networks, Canada is looking at what changes will be needed to current criminal law provisions against virus dissemination.

In response to the attacks of 11 September 2001 in the US, the Canadian Government has introduced a number of legislative proposals to counter the threat of terrorism. The most comprehensive proposals, and those that most directly affect network security and infrastructure protection, are contained in Bill C42 which has not yet completed its review by the House of Commons. Part 10 of this bill amends the *National Defence Act* to allow for the identification and prevention of the unauthorized use of, or interference with, computer systems and networks of the Department of National Defence or the Canadian Forces, and to ensure the protection of those systems and networks. Part 11 amends the *National Energy Board Act* by extending the powers and duties of the National Energy Board to include matters relating to the security of pipelines and international power lines. It authorizes the Board, with the approval of the Governor in Council, to make regulations respecting the security of pipelines and international power lines. It provides the Board with authority to waive the requirement to publish notice of certain applications in the *Canada Gazette* if there is a critical shortage of electricity. It authorizes the Board to take measures in its proceedings and orders to ensure the confidentiality of information that could pose a risk to security, in particular the security of pipelines and international power lines.

More general issues of emergency preparedness are addressed by the Emergency Preparedness Act of 1985 which is designed to cover emergencies of all types including war and other armed conflict. The Act assigns responsibilities for coordination among government institutions and for cooperation with provincial governments, foreign governments and international organizations in the development and implementation of civil emergency plans.

2.4.2 The Government security policy

The federal government security policy (GSP) (ref. 3) applies only to federal departments and agencies but it defines a broad basis for safeguarding the national interest and the government's business objectives by safeguarding employees and assets and assuring the continued delivery of services.

Though not exclusively focused on IT or telecommunications resources, the GSP emphasises the need for departments to monitor their electronic operations because of the extensive reliance of the government on information technology (IT) to provide its services. The GSP prescribes the application of safeguards to reduce the risk of injury, protect employees, preserve the confidentiality, integrity, availability and value of assets, and assure the continued delivery of services.

The GSP is complemented by a series of baseline security standards that address more detailed technical aspects of policy implementation. One of these technical standards, the Technical Security Standard for IT Security (TSSIT) (ref 4), is of particular relevance to IT and network protection. The TSSIT has been developed and issued by the Royal Canadian Mounted Police and provides a technical standard for the protection of classified and designated (i.e. sensitive but unclassified) information stored, processed or communicated on electronic data processing equipment.

Provincial government security policies are generally much less comprehensive than the GSP but all federal policies and standards are available to the provinces should they wish to use them as a basis for their own security policies.

3 Canada's network infrastructure

3.1 Overview of the Canadian telecommunication services industry

The telecommunications service industry is a key sector of the Canadian economy employing 116,000 people in the year 2000 and generating revenues of CAD 32.6 billion. Included in these figures are traditional wireline services, wireless, cable, satellite, and Internet services.

3.1.1 Telecommunication regulatory agencies

The *Canadian Radio-television & Telecommunications Commission* (CRTC), an independent federal agency with quasi-judicial status, is responsible for the regulation and supervision of telecommunications and broadcasting services in Canada. The *Telecommunications Act* gives the CRTC a broad range of powers that include ensuring that rates are just and reasonable and that Canadian carriers do not discriminate unjustly or accord any undue preference with respect to the telecommunications services they offer.

Industry Canada, the federal Department of Industry, has overall responsibility for telecommunications policy, international submarine cable licensing and spectrum policy and allocation. The Minister of Industry has the authority to establish technical standards and to require the CRTC to enforce these standards. One of the roles of Industry Canada is to manage the Emergency Telecommunications Centre in Ottawa and in five regional offices.

3.1.2 An evolving industry

The Canadian telecommunications industry has been in a state of considerable change for a number of years. Deregulation and the increasing emphasis on market forces continue to have a major influence on events. In 1992 the CRTC removed the long-held monopoly of the telephone companies to provide long distance voice services. This led to significant competition in the long distance market as new long distance service providers entered the market. In 1994, the CRTC issued a decision (*Review of Regulatory Framework)* that encouraged the establishment of a new policy framework. This placed greater reliance on market forces and encouraged provision of innovative new services. A CRTC decision in 1997 began the implementation of competition in local telephone service. The net result of these and related CTRC decisions has been to drastically change the face of telephone service in the country. Instead of a small number of cooperating carriers, each with a monopoly in a distinct region (typically a province) we now have a large number of carriers competing across the country in most areas of telephone and telecommunication services. A 1999-2000 survey by Industry Canada shows 52 incumbent wireline carriers (including nine major telephone companies), 562 existing or emerging wireline competitive carriers, 14 wireless providers, and 187 satellite and other providers. Although the telecommunications marketplace is now largely open to competition, only about 60per cent of the services industry actually operates in a competitive marketplace. This is largely a reflection of lack of take-up of the competition in the local service market where expected returns are relatively low.

Another significant telecommunications development has been industry convergence. This has been most evident in the areas of networks, systems, hardware and software related to telecommunications and broadcasting. In 1996, the federal government announced a convergence policy with the objectives of encouraging:

- interconnection, interoperability, unbundling and resale and sharing of network facilities that deliver telecommunication services to the public;
- continued measures to support the production and exhibition of Canadian content in broadcasting; and
- competition in facilities, products and services for the Information Highway.

Since 1997 cable companies have been able to enter the local telephone market. Since 1998 telephone companies have been able to enter the broadcast distribution market. The area of high-speed Internet service provides a good example of convergence, with some of the largest ISPs being telecommunications providers. Bell Canada provides low speed, dial-up Internet access over its traditional telephone circuits as well as high speed ADSL over the same networks. Most of the cable companies offer high speed Internet access over the television cables. Many PCS providers also now offer low speed Internet access over portable web-enabled devices and some interactive pagers are being used to provide e-mail and Internet access. However, convergence does not stop with Internet services. In September 2000, *Bell Canada Enterprises (BCE)*, the largest telecommunications holding company in Canada, created a new market structure that includes *Globemedia* (a multi-media company which encompasses the CTV television network, *Sympatico-Lycos* Internet service and search engine, *The Globe and Mail* newspaper and the Globe and Mail's interactive web-site, *Telesat* Canada (overseas communications provider), and *CGI Group Inc*. a large computer consulting company. Meanwhile, *CanWest Global Communications Corp*. has expanded it's media empire to include television broadcasting, FM radio, newspaper chains, digital speciality channels, film, radio, interactive media and Internet portals.

3.1.3 Teledensity

Teledensity, that is the number of PSTN residential and business individual access lines per 100 inhabitants, provides a measure of telecommunications network deployment. Since 1990, teledensity has included wireless subscribers. Teledensity in Canada has increased from 57.3 access lines per 100 of population in 1990 to 92.1 as of June 2000.

3.2 The economic importance of the telecommunication industry

The importance of the telecommunication service industry to the Canadian economy has already been noted. The year 2000 revenues of CAD 32.6 billion amounted to 2.7per cent of the gross domestic product (GDP). However, there are some other statistics that emphasize both the economic importance of this sector and its rate of growth.

In 2000, telecommunications services produced CAD 21.4 billion of valued added, a 12.8 percent increase from the previous year. As shown in Figure 3.1, telecommunications services growth has out-performed the overall economy since 1994, sometimes exceeding overall economic growth by a factor of five. Year 2000 capital expenditure for wireline and wireless telecommunications services was CAD 6.0 billion in current dollars, a 6.4 per cent increase from the 1999 figure. This represented 4.6 per cent of the economy's total capital investment.

3.2.1 Components of telecommunication services revenue

Deregulation and convergence have greatly blurred the lines of demarcation between traditional telecommunication service providers and their newer competitors and virtually eliminated the geographic limitations on areas of operation. However, largely because of lack of take-up of competitive local service opportunities, the incumbent wireline carriers still dominate in providing local public switched network telephone access .

Around 71 per cent of the total telecommunications services revenues in the year 2000 was generated by the Wireline Incumbent Carriers (i.e. the traditional telephone companies). These include Bell Canada (with around 39 per cent of the total services revenues), Telus Communications (with around 18 per cent), Aliant Communications, Manitoba Telecom Services Inc, SaskTel, and Teleglobe plus 43 independent telephone companies.

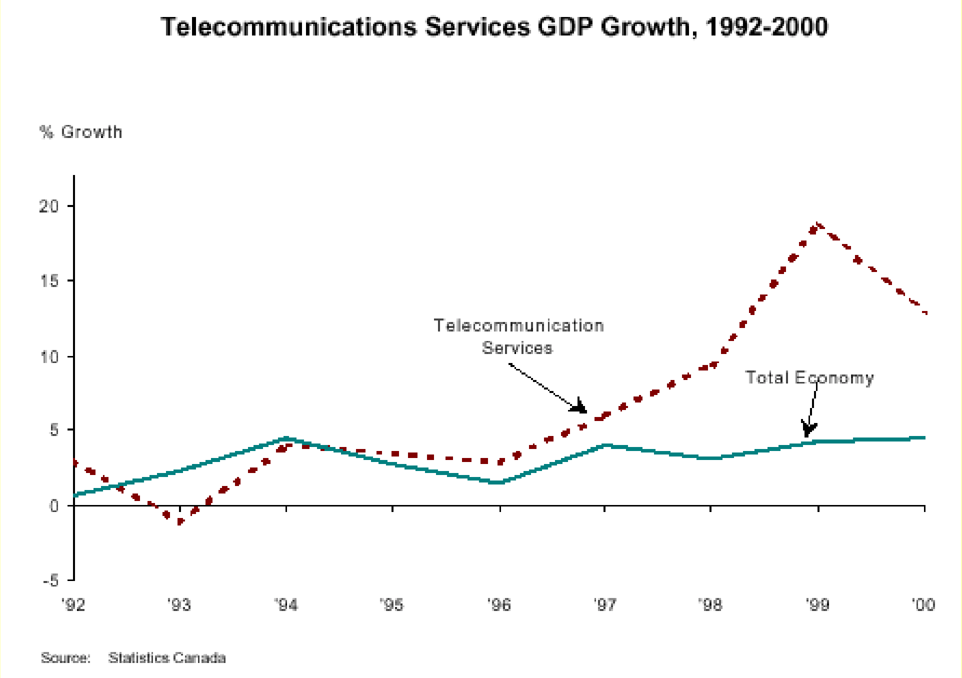
The competitive wireline service providers, who compete with the incumbent providers in local and long distance markets, accounted for around seven per cent of all revenues. These companies include AT&T Canada, Shaw FiberLink, Sprint Canada(Call-Net), and Videotron Telecom..

Wireless service providers, including Bell Wireless, Telus Mobility, Rogers AT&T, Clearnet Communications and Microcell Telecommunications, generated around 16 per cent of revenues.

Lastly in this group are the resellers, satellite and other carriers who generated about six per cent of revenues. This group includes reseller *Primus Telecommunications* and *Telesat Canada*, a satellite carrier.

Local wireline services accounted for the largest portion of revenues followed by wireline and wireless long distance services.

Figure 3.1: Telecommunication services GDP growth, 1992-2000



Source: Statistics Canada

3.3 A closer look at the telecommunication industry components

3.3.1 Local telephone service

As already noted, local wireline services account for the largest portion of telecommunications services revenues, though competition has been slow to develop in this market area. The 1999-2000 Industry Canada Telecommunications Survey reported that 44 companies had registered with the CRTC as Competitive Local Exchange Carriers or had registered their intention to become carriers. Included in these companies are at least six cable television companies that will offer telephony service through the Internet using the Internet Protocol, rather than conventional switching services.

In 1999, these competitive local carriers accounted for less than one per cent of all local wireline revenues.

3.3.2 Long distance services

Liberalization of long distance services began in 1979 but full deregulation of the incumbent carriers' monopoly did not take effect until 1992. In 1999 total long distance revenues were estimated to be CAD 9 billion. This included private line and data/high speed revenues. The incumbent carriers accounted for 67 per cent of these revenues with *Bell Canada* alone accounting for 44 per cent. Wireless long distance accounted for 4 per cent of these revenues, the remaining 29 per cent being accounted for by the competitive wireline carriers and re-sellers.

3.3.3 Wireless and pager services

Canadian wireless offerings include a number of different services and technologies. Services include cellular and digital cellular service in the 800 MHz band, enhanced specialized mobile radiotelephony (ESMR) in the 800 MHz band and Personal Communications Services (PCS) in the 1.9 GHz frequency band. Depending on the supplier, these services are offered as Advanced Mobile Phone Service (AMPS), Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA) and Global Systems Mobile (GSM), paging, high-speed fixed wireless, and satellite services and communication paths.

Mobile ‘phone service represents the greatest part of the wireless market. In addition, paging, high-speed fixed wireless, satellite and PDAs are widely used to provide mobile access to e-mail and Internet services. Wireless services (including cellular and PCS) have experienced dramatic growth through the 1990's. By 1999, total billed minutes amounted to 13.5 billion. Wireless subscribers totalled 8.8 million i.e. over 28 per cent of the population by the end of 2000. Cellular service is available to over 94 per cent of the population overall, while 88 per cent of the population have access to digital cellular service. PCS service is available to around 50 per cent of the population. Pager service subscribers totalled over 1.6 million in 1999. Table 3.1indicates the number of subscribers in 2001 for the major wireless providers.

Increasing use of wireless data services, including e-mail, Internet, and pocket data devices, is expected to continue to fuel wireless growth for the next few years.

3.3.4 International services

Until October 1998, *Teleglobe Canada* held a monopoly on overseas telecommunications services. The ending of the monopoly marked a rush of applications to provide overseas services. By December 1998, 70 licences had been issued for international services. By July 2000, 185 overseas licences had been issued.

In the deregulated environment, Teleglobe, *Call-Net* (Sprint Canada) and *360networks Inc* are prominent, though Teleglobe still has the largest share of the market. Call-Net and 360networks negotiate overseas carrier rates directly with international carriers. *Stratos* is also an international telecom service provider offering customers operating in remote locations with a variety of wireless IP, data, and voice satellite services. Stratos has now taken over from Teleglobe as the national signatory to *Inmarsat*.

As of 1999, Teleglobe had revenues of CAD 1,417m, 360networks CAD 162m and Call-Net CAD 1,250m, though the Call-Net figures are total revenues for all their local and long distance services. 360networks Inc is currently restructuring under court protection.

Incoming international traffic in 1999 amounted to 5500 million minutes of connect time, of which around 65 per cent was from the US. Outgoing traffic for 1999 is estimated at just over 5000 million minutes.

In terms of infrastructure, Teleglobe benefits from its monopoly legacy. It has four of the six Canadian underseas cable landings, international switching centres in New York, Montreal, Toronto and Vancouver plus nodes in Los Angeles, London, Frankfurt, Paris and Madrid. These connect Canadian networks to International networks. Teleglobe satellite earth stations are located in British Columbia, Nova Scotia and Quebec providing links to domestic and international satellites.

3.3.5 Cable services

Cable services are regulated by the CRTC as “broadcasting distribution undertakings” under the Broadcast Act. There are around 200 cable companies in Canada operating over 1900 distinct cable systems. However, over 89 per cent of the customers are served by just six companies: Rogers Cable, Shaw Cablesystems, Vidéotron, Cogéco Ltée, Eastlink Cable Systems, Access Communications. Individual cable systems enjoy a cable monopoly within their licenced area but other services (particularly broadcast satellite and microwave services) compete with the broadcast cable services using different technology. Cable services are available to over 90 per cent of homes with over 75 per cent of homes subscribing to at least one tier of cable services.

Although the primary cable service remains the broadcasting of television, radio and speciality channels (premium and pay TV), other services are also being offered. Cable is one of the two main Canadian high-speed Internet vehicles. Additionally, cable services in some areas include local telephone service and remote monitoring for home security and remote utility meter reading.

3.3.6 Satellite services

Geosynchronous satellites are used by the major telephone companies for backup of their main fibreoptic trunks. Telesat Canada, a subsidiary of BCE, owns four operating satellites, one of which is used for direct broadcasting (including direct-to-home broadcasting). The others are used for TV and radio broadcasting, and voice and data communications. Telesat is the only Canadian company that owns and operates geo-stationary satellites. The Canadian mobile satellite MSAT-1 is owned by Mobile Satellite Ventures (Canada) Inc and operated by Telesat.

Three foreign-owned companies Orbcomm, Globalstar and Iridium, offer low orbit satellite service in Canada. Globalstar is a subsidiary of Qualcomm and Orbital Sciences. Orbcomm and Iridium are operating under new ownership following the bankruptcy of their original owners. Iridium service is marketed in Canada by Infosat which also sells MSAT and Inmarsat service.

It is difficult to estimate actual usage of the low orbit systems, as subscriber numbers and usage profiles are closely guarded secrets. Also, Iridium and Orbcomm have only recently completed their restructuring and re-launch so it may be a while before there is measurable activity in Canada.

3.3.7 International Agreements

Canada is a signatory to the WTO Agreement on Basic Telecommunication services that came into effect in 1997. Negotiations for this agreement were held under the framework of the General Agreement on Trade in Services (GATS) with the primary objectives of allowing more competition in provision of telecommunication services and establishing a transparent and predictable framework for trade and investment in telecommunication services.

Canada's goal in the negotiations was to help Canadian telecommunications companies gain secure access to foreign markets (such as the United States, Europe, Japan and developing markets in Asia and Latin America), and to ensure that Canadians continue to benefit from world-class communication services provided by a strong domestic industry at competitive prices.

3.4 Internet services

The Canadian Internet marketplace provides a good illustration of the convergence of the traditional communication service markets. Internet services are available from a large number of Internet Service Providers (ISPs). Forty-two companies advertise service in every province, all offering dial-up service and over half offering a variety of dedicated high-speed services (including DSL, T1, T3 & Frame Relay). High-speed services are also available to cable subscribers in most, but not all areas. In addition, freenets operate in many parts of the country. Free public Internet access is also available in many public libraries and though community access programs.

According to *Statistics Canada's* Household Internet Use Survey, 51 per cent of all Canadian households measured in 2000 had at least one member who was a regular Internet user from one location or another (e.g. home, work, library). About 40 per cent of respondents indicated that they accessed the Internet from home, i.e. 3.7 million . By December 2000, there were more than 1.3 million subscribers to high-speed Internet, 917,000 of them to cable modem service offered by cable companies and about 500,000 to digital subscriber line (DSL) service offered by ISPs and telecommunications service providers. The number of subscribers to cable Internet in 2000 represented an increase of 155 per cent over 1999.

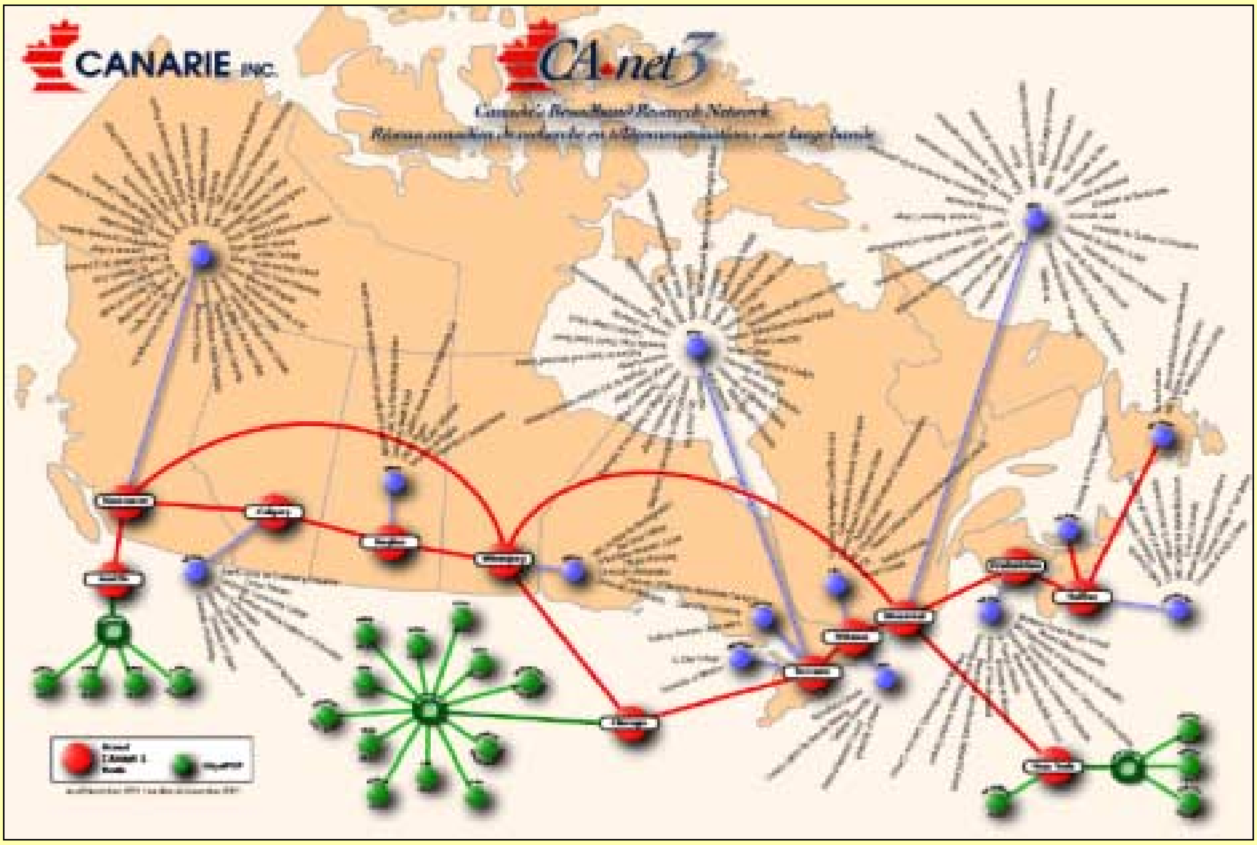
Internet services and ISPs are not licenced or regulated, though they are subject to existing laws on content and service offerings. As with traditional carriers, ISPs cooperate with law enforcement agencies in order to counter cybercrime and traditional crime using cyber channels.

3.5 Canarie – Canada's high-speed research network

3.5.1 Overview of Canarie

CANARIE Inc, a not-for-profit corporation dedicated to advanced Internet development, was established in 1993. Its partners include the research community, industry and the federal government. The Canarie network is a private network that is available to researchers and government laboratories engaged in research and application development for high-performance networks. The third generation Canarie network, CA*net 3 which began operation in 1998, has a backbone system with regional points of presence linking research networks across Canada to the United States, Europe and Asia. CA*net3 is a high performance, national optical Internet that uses Dense Wavelength Division Multiplexing (DWDM) technology to deliver up to 40-gigabit capability which will allow research into next-generation multi-media video conferencing and enhanced virtual reality. CA*net3 was the world's first national network specifically designed to carry the Internet Protocol (IP). CA*net 3 is designed to use up to 32 different colours of light simultaneously, each one capable of delivering the same amount of information now carried by a single beam of light. The topology of the Canarie network is illustrated in Figure 3.2.

Figure 3.2: CA*net3 Connectivity


CANARIE INC.
CA*net3
Canada's Broadband Research Network
Réseau canadien de recherche en télécommunications à large bande
Calgary

Source: Ca*net3

4 The importance of telecommunications to selected sectors of the economy

In addition to being very important to all sectors of the Canadian economy, the telecommunications service industry is itself a key sector of the economy. The sector covers all aspects of public communications services - wireline services, wireless, cable, and satellite as well as Internet services and private research networks. Competition to at least some degree now exists in most of the services. However, with the exception of Internet services, most of the publicly-offered services are subject to some degree of regulation.

This section of the report presents some examples of the importance of network infrastructures to both the public and private sectors. From the private sector, we look at the financial services industry, which impacts virtually every other sector of the economy. A number of public sector initiatives have been selected, most of which are concerned with improving government service delivery and encouraging wider use of public networks.

4.1 The financial services industry and its use of networks

Understandably, the financial services industry is very reluctant to disclose information about its networks or about contingency planning. However, a picture of the industry and the criticality of networking can be deduced from publicly-available information.

Although there are over 3000 organizations involved in financial services in Canada, only the largest of the clearing banks offer a complete range of services coast to coast. The six largest full-service banks also operate internationally and are aggressively expanding their overseas business lines, particularly in investment trading and wealth management. Financial institutions have long been leaders in the use of data communications. Private networks are heavily used internally, for some client delivery services (such as automatic teller machines and Visa authorization), and for inter-industry transfers. As the institutions expand their reach and their services, heavy emphasis is being placed on electronic banking, investment management and electronic commerce as key strategies and these are based, to an increasing extent, on the public Internet, rather than on private networks.

4.1.1 Financial services networks

Financial services networks use an operate a variety of networks including local area networks, metropolitan area financial networks, wide area networks, public switched networks and the public Internet. Depending on the specific purpose, the networks may be private or public. In some instances networks may be shared with industry partners on a restricted access basis (closed user groups). It is not possible to estimate the number of internal transactions on the private networks. However, driven by the e-commerce value chain, the need to lower costs, and the need to speed up delivery, the financial sector is moving increasingly towards a real-time commerce base which means increasing use of public networks. As clients interact directly with the financial institutions over electronic channels, the actual number of transactions becomes increasingly visible. It is also reasonable to assume that each instance of a client processing a transaction directly over an electronic link means one less internal banking transaction (e.g. bank teller to main branch). In fact, it is evident that, in some areas at least, electronic transactions exceed in-branch transactions both in volume and value.

To probe further into the financial networking environment we need to look at some of the specific transactions and how they are conducted.

4.1.2 The clearing and settlement system

The Bank for International Settlements, in its 1994 Annual Report stated "Payment and settlement systems are to economic activity what roads are to traffic - necessary but typically taken for granted unless they cause an accident or bottlenecks to develop." Given that most of Canada's banking transactions are settled via an electronic process, the disruption that could be caused by a serious network failure is potentially immense.

Canada's clearing and settlement system is operated by the *Canadian Payments Association* (CPA), a not-for-profit organization created by an Act of Parliament in 1980[2]. Essentially, the CPA sets the rules governing the settling of different types of payments (cheques, wire transfers, direct deposits, pre-authorized debits, bill payments and point-of-sale debits). The CPA also sets down rules and guidelines for its members. One publication relevant to secure networking is *Principles and Guidelines for payments over Open Communication Networks* (ref 2).

CPA members may be financial institutions such as banks, trust companies, credit unions, caisses populaires, provincial savings offices, life insurance companies, securities dealers, and money market mutual funds. The CPA owns and operates two major payment systems in Canada: the *Automated Clearing Settlement System,* which is used to clear and settle cheques and certain types of automated payments (such as direct deposits, pre-authorized debits, and bill payments); and *the Large Value Transfer System*, an electronic wire transfer system that transfers real-time payments irreversibly and that extends to international payments.

Settlement is a three-step process: *fund deposit or payment* (e.g. by cheque, debit card, direct deposit); *clearing,* a daily process in which members exchange deposited payment items, and determine the net amounts owed to each other; and *settlement* where members use funds on deposit with the Bank of Canada to settle their obligations.

On any day, around 15 million transactions are settled through this system with an average value in excess of CAD 135 million. In 1999, the value of settlements was more than 30 times Canada's GDP. Note that these transactions are all inter-bank transactions. Transactions conducted directly between a client and his/her financial institution are not processed by the CPA and would not be included in these numbers.

4.1.3 The Interac Direct Payment system

Interac® Direct Payment is a payment using a debit card sponsored by one of the members of the Interac® Association, a not-for-profit organization comprising over 130 members representing banks and other financial services companies. Interac® is a nationally-available service that includes both debit card payments for goods and services and cash dispensing from the automatic banking machines of the member companies. Canadians are world leaders in the use of debit cards. In 2001, Interac® transactions for the year exceeded 2.24 billion representing CAD 94.9 billion in sales. On the busiest single day (December 22nd) 10.8 million transactions were posted.

Interac® has a over 460,000 special purpose terminals located at over 325,000 merchants across the country. In addition, over 35,000 shared cash dispensing machines allow Interac® cardholders to withdraw cash from their bank accounts. The Interac® network is a private network operated exclusively for its members and merchants.

4.1.4 Credit card transactions

Although there are a great many different credit cards in circulation in Canada, many are issued by individual department store chains or speciality stores. In general, these are not usable beyond the issuer's stores, so any transmission of these transactions would be kept within the issuer's own network (which could be private or could be via the public switched network).

Four credit cards are widely accepted (Visa, Mastercard, American Express, and Diner's Club) and of these, Visa and Mastercard account for the largest volume of transactions.

Canadian Bankers Association figures for 2001 indicate that over 1.2 million merchants accept Visa and Mastercard. In most cases, on-line authorization of a transaction is required and the vast majority of these merchants have some form of on-line authorization terminal. In many cases (mostly smaller retailers) these terminals dial-up the authorization centre over the public switched network each time a card is used, though high volume retail outlets use dedicated connections to the authorization centre. The number of credit card sales slips (i.e. transactions) processed in 2001 was 1,226 million and the net retail volume processed was valued at CAD 121.8 billion.

[2] The mission of the CPA is: 1. to establish and operate national systems for the clearing and settlement of payments and other arrangements for the making or exchange of payments; 2. to facilitate the interaction of the CPA's systems with others involved in the exchange,3. clearing and settlement of payments; and 4. to facilitate the development of new payment methods and technologies.

4.1.5 On-line and telephone banking

Although some banks and brokerage services have in the past offered personal computer banking via a direct dial-up connection over the switched telephone network, virtually all PC-based on-line banking now uses the public Internet. Telephone banking, of course, relies on the public switched telephone network.

Some banks are securing their Internet banking and brokerage services with public key technology but the majority seem now to be relying on standard web browser encryption (SSL).

The figures for online banking use in 1999 and 2000 shown in Table 4.1 indicate a strong growth in on-line (Internet) banking and moderate growth in telephone banking.

Table 4.1:Electronic and telephone banking

Delivery Channel	Transactions 2000 (millions)	Transactions 1999 (millions)	Percentage change
PC/Internet Banking	47.2	27.2	73.5%
Transfers	10.5	7.0	50.0%
Bill payments	36.7	20.2	81.7%
Telephone Banking	74.0	63.5	16.5%
Transfers	16.1	13.7	17.5%
Bill Payments	57.9	49.7	16.5%

Source: Canadian Bankers Association

4.1.6 Electronic commerce

Electronic commerce is closely linked to the financial services sector, largely because of the payment mechanisms used. Electronic commerce is not new: services like electronic data interchange, electronic payment and settlement systems, and electronic business-to-business transactions have been in common use for over 20 years. What is new is the rapid rise in electronic commerce transactions by the general public over the Internet. The financial services sector is responding to the challenge of facilitating on-line payments by providing advice to would-be online merchants and shoppers about payment methods (including protection the payment vehicle) and by issuing special on-line purchase vehicles such as low-limit credit cards and single-debit electronic wallets.

According to Statistics Canada, the total value of private sector sales over the Internet, with or without on-line payment, rose dramatically in 2000. Canadian businesses received CAD 7.2 billion in Internet orders in 2000, up 73.4 per cent from 1999. Despite these numbers, Internet sales accounted for only 0.4 per cent of total operating revenue in 2000. (These figures exclude EDI, ABM and regular electronic banking transactions.)[3]

4.2 Government use of networks

Over the past 30 years, governments at all levels have become increasingly reliant on data communications to the point where all governments are now highly dependent on communication networks. Like the financial community, governments use a combination of wide area, metropolitan area and local area networks, both private and public but, increasingly, administrations are relying on the public Internet for external service delivery. Initial moves to the Internet were relatively cautious, focusing on e-mail plus some informational web pages but, with the move to on-line service delivery, the Internet has taken on the role of *the* major service delivery channel of the future.

Although electronic service delivery is taking place at all levels of government it is not possible, in a study of

[3] An IDC study suggests that 811,000 Canadians shopped on-line in 1999. This number is predicted to grow to 6.5 million by 2003.

this size, to quantify the full extent to which the Internet is being used for on-line service delivery. Instead, in this part of the paper, we focus on some specific examples drawn from major federal government initiatives. These give an indication of the volume of transactions in some specific areas.

4.2.1 Online Government

In an effort to reduce costs and diversify service delivery channels, governments at all levels across the country are actively making both information and transaction-based services available on-line. Figures are not currently available to indicate the extent of on-line service usage at all levels of government but the federal government's Government Online (GOL) program provides a useful indication of services and usage at the national level.

The federal Government has 126 federal departments and agencies responsible for over 1,600 programs and services.

- The main Canada web site (www.canada.gc.ca) is currently receiving almost 4 million page requests per week.
- The online Job Bank is receiving 100,000 visitors to every day.
- Eleven million electronic (i.e. Internet, dial-in electronic filing, or telephone) tax returns were filed in 2001, including 1.5 million via the Internet

There are approximately 6 million e-mail exchanges within government every day (via departmental intranets and the Internet.)

Central funding of CAD 280 million has been made available to expedite GOL with up to CAD 130 million being allocated to accelerate services on-line and to fund the most popular/large reach services. Up to CAD 135 million has been allocated to build the infrastructure for secure on-line services. Departments and agencies are also leveraging their own funds and/or related policy/program initiatives.

The intention is to expand and expedite the federal GOL so that by 2004, citizens and businesses will be able to request and receive all key federal services through secure, interactive and timely on-line transactions.

In addition to the federal effort, the individual provinces offer differing levels of online services, typically covering health care, education, permits (driver's licences, hunting and fishing permits) and tourism. For example, the Government of Ontario, the largest province, offers business registration, application for licences, business and other information over the Internet in addition to having 70 kiosks throughout the province that allow citizens to renew health cards, drivers licences and other similar tasks.

Municipalities offer online payment of taxes, water and utility bills (via on-line banking services), online access to libraries (information, book renewal and book reservations) and community information and services.

4.2.2 SchoolNet

SchoolNet encourages the integration of information technology in learning to help students acquire the knowledge to use the Internet for research and communication. SchoolNet is a federal initiative in cooperation with a national advisory board of provincial and territorial governments, universities and colleges, and educational associations. The SchoolNet Web site provides educational resources for educators and students and offers users more than 1000 learning services and resources, including training and research tools.

All schools throughout the country are now connected to the Internet via SchoolNet. As of May 2000, the number of computers connected under the program in schools throughout the country totalled almost half a million.

4.2.3 The Community Access Program

The *Community Access Program* (CAP) was established in 1995 by Industry Canada as a key component of the federal government's *Connecting Canadians* initiative. The program aims to give residents of rural, remote, and urban communities across Canada affordable access to the Internet.

The Community Access Program is a partnership between governments, the private sector, and community organizations. So far 8,800 communities have either been approved or included in this program.

Involvement in the program, which includes a large element of education and familiarization for the community residents, is very much a grass-roots effort that is resulting in a national network of CAP communities and champions. Local community web sites are being developed and other local innovations are being encouraged.

4.2.4 Federal government network security initiatives

All federal departments are heavy network users. Regardless of the option chosen, all departments are ultimately responsible for ensuring their own security (according to the Government Security Policy). In some cases federal departments have contracted directly with telecommunication carriers for their departmental networks. In other cases departments have opted to use the cost-recoverable GENet common network facilities contracted by the *Government Telecommunications and Informatics Services* (part of *Public Works and Government Services Canada*) on behalf of the federal government.

The federal government has embarked on two very significant network security initiatives that will have a major impact on internal network security and on the security of service delivery. First of all, the *Government of Canada Public Key Infrastructure* (GoC/PKI), which has been in development since 1996, offers protection to all desktop systems in the federal government. Several provinces are following the lead of the federal government and adopting both the GoC/PKI technology and the certificate policies of the federal government. The second major initiative in this area is the development of a *Secure Channel*, which will be a common network service offering to succeed GENet. The Secure Channel will offer network services, security services (access control, authentication, authorization, confidentiality, data integrity and non-repudiation), Directory services, and support for common applications. The Secure Channel will be a major infrastructure component for the Government Online project.

5 Critical infrastructure dependencies

To this point in the paper we have looked at the political and geographic environment, the telecommunications infrastructure, the economic importance of networks to the financial and public sectors, and some of the key organizations involved in infrastructure protection. We now look at the relationship of communications networks and elements of the Canadian critical infrastructure. In particular we examine the importance of networks to the Canadian business environment as a whole by examining the potential impact of network failure on various sectors. Also we indicate possible mitigation measures.

To a large extent this analysis relies on work done for the *National Contingency Planning Group* in preparation for Year 2000 transition and documented in the report *Canadian Infrastructures and their Dependencies* (ref 7). Although this work was done 2-3 years ago, for the most part it remains valid. This work was premised upon four tenets, stated below in order of priority:

- no loss of life;
- basic community needs should continue to be met;
- business should continue as usual; and
- confidence in government should be maintained.

Note that financial services and government services, which are also critical elements of the national infrastructure and have a high dependence on telecommunications networks, are not included in this section as they have been discussed in some detail in section 4.

5.1 The national telecommunication infrastructure

5.1.1 Impact

Such is the dependence on the basic telephone system that catastrophic failure, even within a relatively small region, could have a very severe impact. The public would be unable to make emergency calls or conduct any business that relies on the switched network (including dial-up Internet access). Failure of the telecommunications infrastructure would have a serious impact on business and government at all levels. The potential impact on individual segments of the economy is discussed in the following sub-sections of this section of the report.

The immediate impact on some public services would be severe. Emergency services (police, fire ambulance etc.), if located in the affected area, would have to be switched to alternate facilities. Emergency callers located in the affected area would be unable to make calls until service was restored unless they were able to use alternative facilities (e.g. cellular telephones).

All business conducted through the affected facilities (voice, data, fax) would be instantly disrupted until service was restored or alternativee facilities arranged.

5.1.2 Critical elements

The diversified nature of the elements of the telecommunications infrastructure (telephone, data lines, cellular and PCS systems, pagers, satellite, cable, wireless broadband, radio and television) means that total failure is virtually inconceivable. What is more likely is that one or two elements (e.g. voice and data lines) could fail but the other elements would be unaffected.

The most critical elements of the traditional telephone network are the switches, of which there are around 3600 in Canada, some of them very large. Catastrophic failure of a switch e.g. due to earthquake or fire, could disable 100,000 telephone lines and 3000 data lines.

5.1.3 Vulnerabilities and mitigation strategies

Full restoration of a switch could take about one week. In the interim, a mobile switch could be used. Depending on the severity of the incident, Industry Canada may well be called upon to coordinate a response and individual carriers would likely invoke their mutual aid provisions.

Aside from natural and man-made disasters, the telecommunications facilities are also vulnerable to power failure, though all switches have battery backup. Beyond that, major central offices have generators with fuel to last several days.

Lack of ability to access facilities can, in some instances, constitute a vulnerability. If the carrier is prevented from gaining access to facilities e.g. by bad weather, failed access routes or even administrative restrictions (such as happened during the recent foot-and-mouth disease outbreak in Britain, where some facilities were located in restricted access areas) restoration can be severely delayed.

Businesses and individuals could mitigate the effect of failure by using alternative communications channels or using services in a nearby, unaffected community.

5.2 The electricity industry

5.2.1 Impact

In this report we are concerned primarily with the impact that a critical failure in telecommunications would have on industry, rather than the impact of the failure of any industry segment on the telecommunications infrastructure. However, in the case of the electricity industry there is such a degree of interdependence that the effect of serious electrical failure on critical telecommunications infrastructure cannot be ignored.

As already noted in the previous section, the telecommunications infrastructure is dependent on power, though mitigation strategies using back-up batteries and generators are routine and successful in all but the most extreme instances. Further, since telephones are powered from the local office, rather than from the subscriber’s premises, power failures per se do not generally affect the basic telephone service. (During the Ice Storm that occurred in Eastern Canada in 1998, some rural communities were without power for as long as three weeks but able to use the telephones during that period.)

For citizens and businesses relying on data communications services, however, a severe electricity failure would render many of the computers unusable with the result that no transactions (whether dependent on telecommunications or not) could processed for the duration of the power failure. An even worse scenario is that of “brown-outs”, where power is reduced to the point where only low-demand devices operate and power spikes occur when the power is restored, with the risk that equipment is damaged by the surge. During the ice storm, both of these scenarios were fairly frequent occurrences. Brown-outs prevented the proper operation of computers and their displays while power spikes (which occurred frequently within short spaces of time as attempts were made to restore power) caused equipment to burn out. A further risk is that data becomes corrupted or that the storage devices suffer physical damage. Where third party service providers (e.g. Internet Service Providers) suffer power failures, all users of that ISP are impacted by loss of service and there is a risk that data and messages could be lost.

Thus, electrical failure has a very severe effect on data services at the subscriber level and even reduced power levels can have a serious and lasting impact.

From the electricity supplier standpoint, telecommunications failure would impact the process control systems and the communications between control centres, generation facilities and local facilities (transformers, substations and switches).

5.2.2 Critical elements in electricity supply

The electricity supply components most dependent on telecommunications are the process control systems. Communication between the system control centres and the generating stations, transformers, switching stations and substations must be reliable and secure. Electricity supply operations depend on a very precise “just-in-time” delivery. Any communications failure that disrupts the network monitoring or control jeopardizes that reliability.

5.2.3 Vulnerabilities and mitigation strategies

Most electricity companies protect against possible communications failure by using both their own communications facilities and externally-supplied facilities. Back-up facilities, including satellite links are in place to assume critical communications functions in the event of failure of the normal systems.

Like all utilities that use telecommunications networks for remote monitoring, the electricity supply industry is vulnerable to cyber attacks launched over the Internet.

As electricity supply in Canada is a provincial responsibility, any legislated requirements for emergency preparedness apply on a province-by-province basis, rather than nationally.

Mitigation strategies for telecommunications users who would be affected by electrical failure include back-up power supplies (battery for short periods, generators where prolonged outages are unacceptable) and surge protectors to safeguard equipment from power fluctuations.

5.3 Internet services

5.3.1 Impact

Although not part of any single industry group, Internet services are considered here as they constitute an area of growing significance with respect to critical dependencies. As we have already seen, the financial services industry and government on-line service delivery are relying heavily on the Internet. In addition, education, business and personal e-mail services, healthcare delivery systems and an increasing number of business-related on-line services (such as on-line reservation systems) are dependent on the Internet. The importance of the Internet to industry sectors will also be noted in the discussions below. A serious failure of the Internet at the national or regional level would be highly disruptive to government and business alike. Even local failure of individual Internet Service Provider (ISP) services would cause wide public inconvenience and business disruption.

Another very important aspect of the Internet is its potential to be used as a conduit for the launch of cyber attacks against any individual or organization that relies on the Internet. This potential extends to attacks on other infrastructure elements, particularly large public utilities that use network-based facilities to control of elements of the infrastructure remotely. (In one well-publicised case, a hacker gained access to a sewage processing plant in Australia and released large volumes of sewage, but Internet-based attacks have been launched against most large organizations and public utilities).

5.3.2 Vulnerabilities

In general, because of the robust design and built-in redundancy of routing, the Internet backbones are not vulnerable to major failures of equipment or communications links on individual legs of the network. A major failure in one leg would simply result in re-routing of messages to alternative routes. The greatest risk of hardware and/or communications failure is between the subscriber and his/her ISP (or in the case of large users who interface directly to the Internet, a failure at the user's premises). If an ISP suffers a hardware failure, restoration capability generally depends on the individual ISP, with some being more robust than others (for example in being able to switch quickly to a backup server). If the ISP itself suffers a major failure such as an electricity blackout, fire or other major disaster, restoration could take hours, days or weeks. In cases of very serious ISP failure, subscribers would be forced to seek alternative ISP services. (Few subscribers actually have active accounts with more than one ISP.) For users with dial-up Internet access, the communications links between the subscriber and the ISP are as robust as the telephone service and local communications redundancy is built into the service. For users of cable or DSL services, communications failure could result in a prolonged outage and in the event of a failure of the ISP, establishing service with an alternate ISP would be less easy than for a dial-up service user. Given the vast number of users, and the number and variety of distinct ISP services, it is impossible to estimate the likely impact of any particular type of failure. However, a recent example of a server failure at one Canadian cable company provides some insight into what could happen. The company has 300,000 subscribers to its cable Internet service. It operates 10 servers and typically handles 2.5 million e-mails per day. On 19 March 2002, during the peak traffic period of 8pm to 10pm, one of the servers crashed due to overload. During the 30 minutes the system was down, an estimated 10,000 to 12,500 e-mails were lost and irrecoverable.

However, the most serious Internet vulnerabilities are not those inherent in the equipment or communications facilities: they are the vulnerabilities arising from the Internet service itself and its users. The issue of viruses, malicious code and denial of service attacks have received wide publicity. Most ISPs and organizations, in addition to many individual users, spend a great deal of money, time and resources implementing layers of protection to try to evade the most serious threats. Unfortunately, the reality is that serious service disruptions caused by malicious code and denial of service attacks continue to be almost daily routine for many Internet users. Meanwhile, the software companies, firewall suppliers and suppliers of filters and scanners struggle to respond to the growing inventiveness of the hackers and cyber criminals. A further point is that the damage resulting from a malicious code or virus attack is not isolated to a discrete part of the infrastructure: it is generally widely spread among many users and can cause serious damage to files and software, sometimes to the point of destruction. Recovery must be effected on an individual basis and can take much longer than even fairly serious disruptions caused by network or ISP failure.

5.3.3 Mitigation strategies

Firewalls, virus scanners and filtering devices can detect and often block *known* malware, provided the filters and virus definitions are up-to-date, but they are seldom able to protect against new forms of attack. Strict computer hygiene measures and enforcement of appropriate use policies can also help reduce vulnerabilities. Ensuring that installed software is properly maintained (including ensuing that current, approved patches are installed and operational) can also reduce the risk of an attack (including a denial of service attack) succeeding. Taking regular backups of important files can assist in the recovery process, should an attack succeed. However, none of these measures can eliminate or even reduce the *threat* or guarantee that an attack will not succeed. Given the ubiquitous nature of the Internet, the virtually uncontrolled trans-national data flows, the lack of uniformity in national laws protecting against cyber attacks, and the inconsistent application of laws that do exist, it is likely that the Internet will remain seriously vulnerable and will be a major conduit for attacks on the infrastructure for some years to come.

5.4 The oil and gas industry

5.4.1 Impact

Canadians are highly dependent on natural gas and oil for home heating and for industrial use. The largest production areas are in the western provinces, though there is some production in Ontario, the northern parts of the country and off the eastern coast. Large volumes of oil and gas are shipped across the country and to the US by pipeline. Failure of any of the collection or delivery pipelines would have a major impact.

5.4.2 Dependence on telecommunications

Voice and data telecommunications are used by the oil and gas industries to manage distribution and delivery of the products. Customer deliveries of oil at the retail level, and re-supply of local oil depots and notification of problems (e.g. gas leaks) are coordinated by telephone or e-mail. Oil and gas pipelines use telecommunication links between the control centres and remote pumping stations. Remote gas compressor stations are centrally controlled via telecommunications.

5.4.3 Mitigation strategies

The National Energy Board requires that all suppliers have business resumption plans in place.

5.5 Surface transportation

5.5.1 Road transport

Road transport (which includes trucking and local and inter-city bus services) is dependent on telecommunications for: scheduling; (wireless) communications between the vehicle or vessel and base; business communications (for reservations, ticketing and business management); and passenger information systems.

5.5.2 Rail services

Freight and passenger services rely on voice and data telecommunications for coordinating and managing the transportation services, and for communicating with clients and other transportation companies (e.g. road haulage companies that coordinate deliveries with the railways). Telecommunication services are also used in control and signalling systems. Lastly, passenger services are increasingly relying on on-line service delivery systems for passenger information and reservations.

5.5.3 Marine and ferry services

Marine services in Canada include shipping (ocean and inland), ports, navigation, St Lawrence Seaway services and icebreaker services. Ferries operate on the Atlantic and Pacific coasts as well as on the Great Lakes and some rivers.

All shipping is highly dependent on communications between vessel and shore to exchange information on weather conditions, positions and status, to coordinate movements with suppliers and clients, and to serve in case of medical emergency or potential disaster.

Seaway traffic is dependent on voice and data for business transactions between freight forwarders, shipping owners, agents, government agencies and private industry. Seaway business transactions make heavy use of electronic data interchange.

Icebreakers require constant communications to ensure safe movement in shipping lanes and safe and speedy operation of the Coast Guard fleet.

Marine navigation relies on dedicated transmitters, antenna farms and coastal radar sites and there is a heavy dependency on local telecommunications infrastructure.

Passenger ferries are increasingly using on-line services for passenger information and reservations.

5.6 Air transportation and airports

Airports, air carriers, navigation services and related support systems are included in this category.

5.6.1 Airports

Without effective and reliable national and international communications, airports and their support services simply could not function. Communications-dependent services include ramp control, security, passenger notifications, reservations and ticketing. Loss of communications has a massive impact.

5.6.2 Navigation systems

Air navigation systems are totally dependent on telecommunications. The effect of failure of communications would be immediate and very serious. Although the armed forces could assist in developing alternative communications systems the time to effect such operations would be lengthy.

5.6.3 Air carriers

Air carriers are highly dependent on communications systems for airport communications, communication with navigation services and for virtually the entire range of airport support services including maintenance, ramp control, baggage handling, emergency services and trucking.

Commercial air carriers and private aircraft rely on communications for interfacing with customs and immigration and, where necessary, law enforcement.

Passenger air carriers are increasingly moving to on-line services for information, passenger contact, reservations and electronic ticketing.

5.7 Food production and distribution

Included under this category are: food production; food supply and distribution services; and food safety services, including inspection, monitoring, investigation, import/export and emergency response.

Telecommunications services are essential for the food inspection services to communicate with the public and, particularly, to issue emergency notices in the event of recalls.

Food distributors use telecommunications and EDI for dealing with suppliers and clients and for coordinating the supply chain activities.

The grain transportation system relies on communications among partners.

Primary producers are increasingly using on-line services, particularly Internet services, for information about weather conditions, markets and trade, and agricultural programs and services.

5.8 Health care

The health care sector includes services at all levels of government in addition to primary health care delivery (hospitals, clinics and doctors offices).

At the federal level health care responsibility includes: remote health care services (First Nations and Inuit); veterans services; federal emergency services and disease control; drug and appliance inspection services; blood services; occupational health and safety; and managing food-borne diseases. Provincially, responsibilities include: the provincial health care delivery systems (including publicly funded hospital medical services); ambulance services (also municipal and private ambulances); community healthcare including vaccination and immunization services (which are also handled at the municipal level); and administration of the provincial medicare and provincial drug plan insurance systems.

Totally reliable telecommunications are essential for coordinating emergency responses (e.g. ambulance and related services) and for communicating information relating to emergency situations (e.g. outbreaks of disease and biological, chemical and other contamination).

Health care delivery systems (doctors, hospitals and private clinics) rely on on-line services to validate patient health cards with the province providing the medicare coverage.

Doctors and hospitals rely primarily on voice communications to transmit patient prescription information to pharmacies. Doctors are also increasingly relying on-line databases of patient information.

Hospital services use broadband transmission to permit remote monitoring of patient conditions and surgery. Hospital staff are increasingly using video conferencing systems to communicate with remote locations. Detailed patient information, including X-ray and other diagnostic materials, is routinely exchanged using broadband services.

5.9 Summary

As the examples above indicate, telecommunications services are vitally important to a broad cross-section of industry, commerce and the public sector. In addition, these sectors are increasingly dependent on the Internet. The traditional communications infrastructure has effective mitigation and restoration strategies, and in some cases alternative communications channels exist. Overall, the traditional networking infrastructure is fairly robust. However, although the Internet backbone network is robust, the Internet is highly vulnerable at the local level mainly due to malicious code, viruses and denial of service attacks. In addition, because of its ubiquity and its role as the primary conduit of cyber attacks, the Internet itself poses a threat to critical network infrastructures.

6 Network security case study

This case study is in two parts. The first part is a fairly detailed look at the work done in developing a common standard for perimeter defence for an enterprise that comprises many relatively autonomous organizations. However, while perimeter defence is very important, it is not enough. The second part of the case study examines a specific security implementation that is designed to protect sensitive data at all times, wherever it is located.

The perimeter defence solution has been drafted as a federal government standard but not yet implemented. However, the proposal has been validated by a series of consultations with some of the targeted users, and some of the results of these consultations are included. The second part of the case study reports on a solution that has already been implemented in the health care sector.

6.1 IT Security Zones - a common solution for perimeter defence

6.1.1 Environment

The Government of Canada (GoC) comprises over 150 distinct departments and agencies ranging from very large units with broad and diversified mandates to small, highly focussed units. All rely on communications networks, e-mail and the Internet and all are vulnerable to serious disruption from viruses, malicious code, mobile code and denial of service attacks. Some departments have established their own networks, others use the common network services available from *Government Telecommunications and Informatics Services*, part of *Public Works and Government Services Canada*. However, all departments are faced with the need to address perimeter defence. All departments and agencies are required to comply with the Government Security Policy but departments are individually accountable for protecting their assets and the assets of Canadians. This is influential in determining the security approaches and solutions. (Accountability for security is actually vested in the deputy minister of each department.)

Up to this point, departments have developed or adopted their own individual perimeter defence solutions and this has resulted in a variety of approaches that, in some cases, impair agency interoperability and could make it difficult to realize some of the Government Online objectives. The overall objective of the *Baseline Requirements for IT Security Zones* standard (ref. 8) that has recently been completed is to assist departments and agencies to secure government networks and implement perimeter defence measures in a consistent manner.

Note that the IT Security Zones address only perimeter defence. They are not intended to meet all of the IT security requirements needed to safeguard end systems, applications or data.

6.1.2 Basic concepts of IT Security Zones

Network security is concerned with countering threats that originate in the external network (i.e. the network external to the enterprise) and those from within the network itself. Although Internet-based threats are pervasive and growing rapidly, for most organizations *insider* threats constitute the dominant threat to networks and end-systems. The insider threat originates from three sources: hostile insiders; compromised nodes; and human, system or configuration errors.

Network security fulfils three functions:

- it protects the network itself from accidental and malicious threats;
- it protects end-systems and applications using network facilities from malicious traffic; and
- it supports the provision of services to protect user data in transit.

The notion of physical security zones is well established. For example, the GoC Security Policy identifies five types of physical security zone: a Public Zone, a Reception Zone, an Operations Zone, a Security Zone, and a High Security Zone. These physical security zones are distinguished by the strength of perimeter defence, the degree of control over the individuals and equipment allowed in the zone, the degree to which movement within the zone is monitored, and the trust assigned to the individuals allowed in the zone. For example, the public is allowed access to a Public Zone without an escort but access to a High Security Zone is strictly controlled and movement is often monitored. The type of zone determines the sensitivity of data that can be processed the zone (e.g. sensitive data cannot be processed in a public zone).

Similarly, the concept of a *security domain* is a well-accepted construct for establishing security boundaries and accountabilities. An *IT Security Zon*e is a special type of security domain that is defined as a networking environment with a well-defined boundary, a security authority and a quantifiable network threat.

Different types of IT Security Zone are distinguished by their characteristics which are defined by technical security requirements for interfaces, traffic control, data protection, host configuration control and network configuration control.

The GoC IT Security Zone model defines seven types of security zone:

i) A *Public Zone*, which is entirely open and includes public networks such as the Internet. No restrictions are placed on this zone as it is entirely outside the control of the federal government. The Public Zone environment is assumed to be extremely hostile;

ii) A *Public Access Zone* (PAZ), which mediates access between operational systems and the Public Zone. The PAZ is a tightly controlled domain that protects internal government networks and applications from a hostile Public Zone environment and also acts as a screen to hide and limit exposure of internal resources from the Public Zone. Access to Government Online services will be implemented in the PAZ;

iii) An *Operations Zone* (OZ) which provides a relatively secure network environment and is the standard environment for routine government operations but is not suitable for sensitive or critical applications;

iv) A *Security Zone* (SZ) which provides a tightly controlled network environment suitable for critical servers or systems processing sensitive information;

v) A *High Security Zone* (HSZ) which provides a tightly controlled network environment suitable for safety-critical applications or systems processing classified information;

vi) A *Special Access Zone* (SAZ) which is a tightly controlled network environment suitable for special processing needs; and

vii) A *Secure Extranet Zone* (SEZ) which supports directly connected extranet services with highly trusted partners.

The IT Security Zones define the network boundaries and associated perimeter defence requirements by:

- Defining the entities that populate network security zones;
- Identifying discrete entry points (i.e. gateways);
- Filtering network traffic at gateways;
- Monitoring the state of the network;
- Authenticating the identity of network entities; and
- Monitoring network traffic at the entry points.

The logical model of perimeter defence has two components: Boundary Integrity, which addresses the threat of unauthorized network interfaces; and Traffic Control, which counters threats such as denial of service, malicious traffic and unauthorized content.

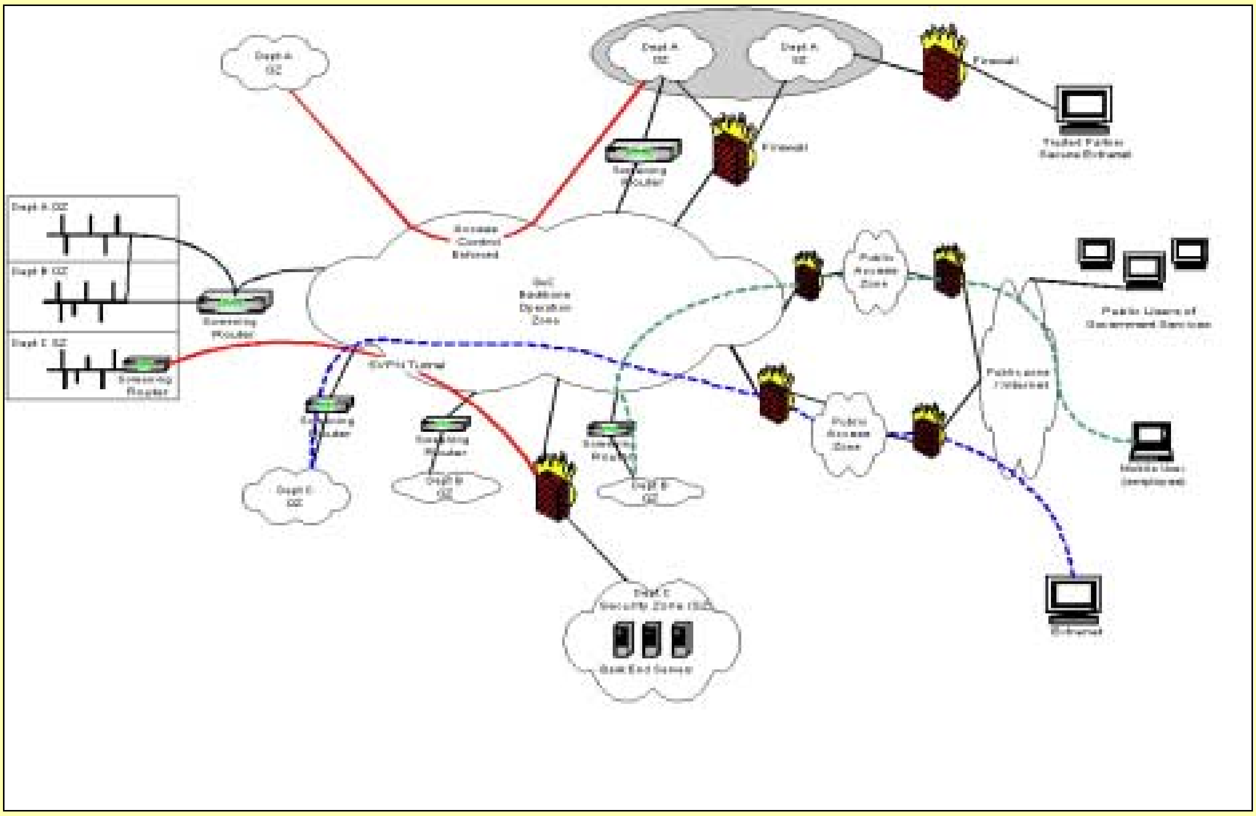
Figure 6.1 illustrates how the IT Security Zones might be realized in practice. In Figure 6.1, a GoC common backbone network has been implemented as an Operations Zone. All departments access the Public Zone (e.g. Internet) through this common backbone using one of the Public Access Zones provided as part of a common infrastructure.

Department A implements three zones: two Operations Zones and a Security Zone. Each of these zones has a single point of presence in the GoC inter-network as shown by the fire-walled connection to the backbone. One of the Operations Zones is implemented as two enclaves that are connected via a secure tunnel over the GoC backbone. Department A also supports a secure extranet connection to a trusted partner.

Department B implements three Operations Zones and supports mobile users through secure remote access to one of these zones. Departments A and B share Data Link and Physical Layer infrastructure between Operations Zones installed in a building.

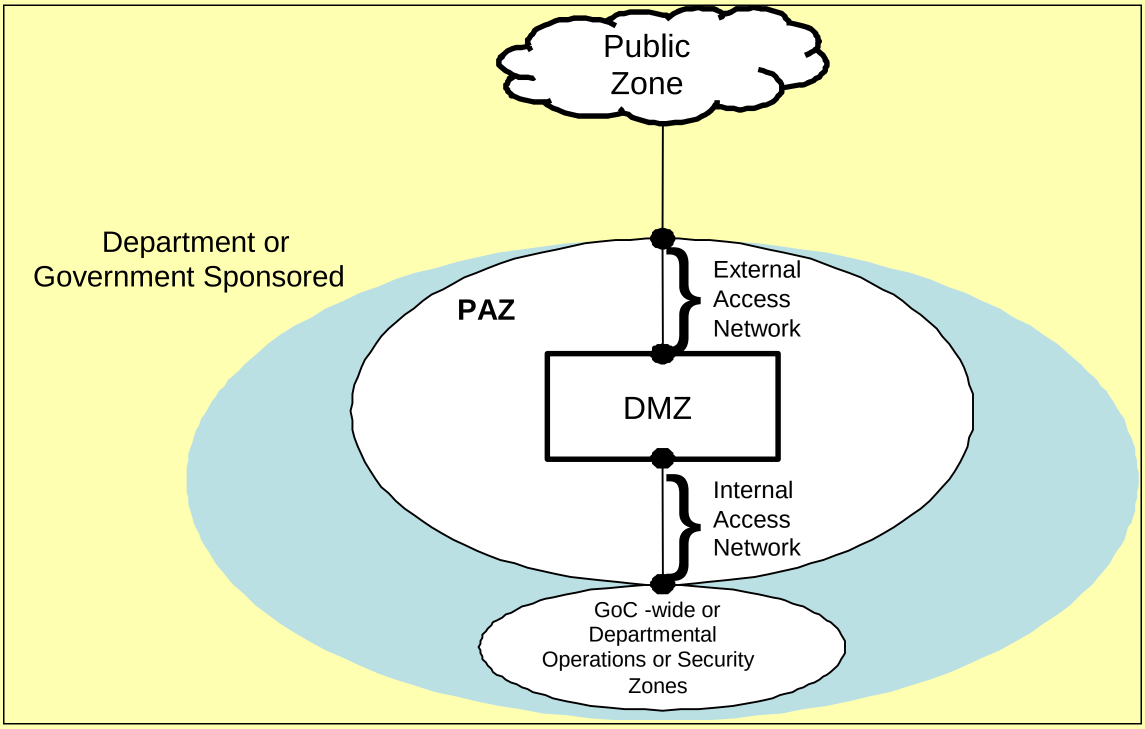
Department C implements a Security Zone as two enclaves connected by a secure tunnel. Department C uses a full VPN (e.g., IPSEC) to provide confidentiality of traffic as it moves across the backbone. Department C also implements an Operations Zone and supports extranet services to partners.

Figure 6.1: Example of how IT security zones could be realized



Source: IT Security Zones: Baseline Security Requirements, Communications Security Establishment, March 28th 2002.

Figure 6.2 The public access zone


Public Zone
Department or Government Sponsored
PAZ
External Access Network
DMZ
Internal Access Network
GoC -wide or Departmental Operations or Security Zones

Source: IT Security Zones: Baseline Security Requirements, Communications Security Establishment, March 28th 2002.

6.1.3 The public access zone

At this point, only the PAZ has been specified in detail but, given the critical role of the PAZ as the buffer between the hostile public Internet and the internal resources, one could argue that this is the most critical zone. Figure 6.2 illustrates the three components of the PAZ, an external access network, a demilitarized zone (DMZ) and an internal access network. Firewall type devices would normally be placed at both the internal and external access network boundary points with the DMZ. Application proxies for common government services and applications such as e-mail, web access, remote/mobile access and extranet services would normally be located in the DMZ.

As illustrated in Figure 6.1, Public Access Zones could be implemented for a single department or several departments could share a single PAZ.

6.1.4 Consultations with users on the proposed standard

In order to validate the proposed standard, in-depth consultations were conducted with selected departments. These consultations provided a reality check on the proposals and also produced some interesting and sometimes unexpected responses.

<u>Overall support for proposals and likely impact</u>

Very good support was indicated for the common perimeter approach. In some cases departments already implement a similar security zone approach to perimeter defence but the proposals would result in a common approach across the entire enterprise.

The likely impact of implementing the proposals was judged as low to moderate.

One concern expressed was the cost of implementing a system that involved more than one firewall, but this was not viewed as a major concern.

Particular vulnerabilities

E-mail (particularly X.400 mail which is not filtered), extranet services and the WAP gateway were all identified as being prone to particular vulnerabilities and presenting problems for departments. In addition, web servers and proxies, virus scanning for web content, Internet news groups, DNS and streaming media proxies, were all identified as frequent sources of security alerts.

Growth in Internet usage

Annual increases in departmental bandwidth usage of the Internet were reported as being in the range of 300 per cent-600 per cent.

Common/shared perimeter defence service

It was generally felt that some security services, such as virus scanning and content filtering might well be provided in a common PAZ. As expected though there was concern over accountability for security breaches. Each department has different levels of accountability and different requirements regarding privacy protection. Since departments are individually accountable for protection of their assets, the question of how accountability would be assigned in the event of incidents that occur when using common security services was fully expected. In spite of this most departments indicated they would be comfortable sharing services with departments that had common requirements and similar levels of protection. However, one unexpected concern raised was that of maintaining trust. While it is possible establish trust with other agencies by conducting detailed, one-on-one, inspections of configurations and security provisions, it is very difficult to have confidence that such trust is maintained as systems are in a continual state of change.

Troubleshooting and auditing

Not surprisingly, the troubleshooting and auditing of security breaches was identified as a major consumer of resources. What was surprising here was to find that troubleshooting and auditing of internal breaches is often considerably more complex than that for breaches from outside. The reason for this is that internal breaches have to be treated as potential criminal investigations, particularly where departments have made a decision to prosecute in all cases of criminal misconduct.

Firewall configuration

Firewall configuration and filter management were identified as tasks that require significant engineering effort. Firewall configuration in particular is a largely manual process that requires examination and cross checking by several individuals plus independent verification of any changes to the ruleset before any action is confirmed. Errors have been found to be much more frequent when implementations are hurried. As a result, strict procedures are usually put in place that allow sufficient time for the installation and examination of proposed rule changes. A serious problem identified by one large department was that of failure of users to honour the configuration process by demanding immediate changes, and bypassing the established security implementation processes by escalating their requirements through the management chain.

In summary, the draft standard for a common approach to perimeter defence based on IT security zones has received a promising reception and indications are that the standard can be implemented without major impact on departments or agencies. Work remains to be done on defining the requirements for the other security zones but implementation of Public Access Zone requirements can begin in the near future. Although the standard has been drafted from the perspective of a large public sector organization, many large private sector organizations with relatively autonomous divisions could adopt a similar approach to perimeter defence.

6.2 Securing the data: Beyond perimeter defence

Perimeter defence is very important but, as noted in the first part of this case study, it is not intended to meet all of the IT security requirements to safeguard end systems, applications or data. In fact, the IT Security Zone standard described above recognizes the need, for example, to protect the confidentiality and integrity of data during transmission.

The particular example chosen for this second part of the case study has been selected for two reasons. Firstly, it recognizes that protection is needed over and above that provided by perimeter defence. Data must be protected at all stages, whether in transit or in storage. Secondly, this solution was developed in direct response to the needs of the user community. The implementation described uses an established security technology (PKI) but the application evolved from the Ontario College of Pharmacists which was concerned about the need to provide adequate protection for business processes.

6.2.1 Securing Internet transactions

The implementation described here relates to the protection of medical information. However, before examining the details of the implementation, we will spend a few moments reviewing the more general background leading up to the specific implementation.

Additional business requirement is that there be legal and auditable records of contractual obligations and transactions. In the paper world, we trust the written records such as contracts and invoices because they are signed by persons authorized to act on behalf of the organization. In the digital world though, we need to vouch for the identity and authority of the sender and receiver, as well as the validity and integrity of the electronic document. In addition, there is a need to protect the integrity and validity of the transaction both before and after it has been transmitted electronically.

Most e-commerce transactions currently do not meet the requirements of contract law or even the various e-commerce laws being passed in Canada and the US. In most cases, applications rely on web browser Secure Socket Layer (SSL) which protects the data as it moves across the Internet and authenticates the server that the user is communicating with. However, SSL does not authenticate the sender or recipient and does not protect the data before or after transmission.

A Public Key Infrastructure (PKI) can provide a much stronger form of protection than SSL in that it can provide the digital evidence for a transaction, protecting the business process and making it legally binding. It can also be used to protect the data in local storage, before and after transmission.

6.2.2 Protecting patient medical records

The crux of this application is protecting patient healthcare records from unauthorized modification or disclosure while ensuring that relevant information is made available to authorized healthcare professionals. Patient medical records are particularly sensitive but parts of them need to be accessed by different medical professionals - physicians, specialists, nurses, medical technicians, pharmacists etc who are often located in different cities or even different countries. Additionally some of the information may be useful to researchers. Increasingly we are witnessing a need for patient records that are portable and can be accessed electronically by a community of medical practitioners and researchers.

This application was originally developed for the Statum Group by a team of health care professionals and technology specialists. It is now being used by an entire community of physicians.

The application maintains an on-line and off-line version of patient health records. Each patient record contains such information as doctors' reports and treatment recommendations, diagnostic reports (ECGs, x-rays, MRI, CAT scans), laboratory test results, immunization records, allergies, medications, organ donor consent, details of any implanted devices, and emergency contacts. In other words, the patient records are both complete and very sensitive. The on-line version is contained in an encyption-protected database: the off-line version is a portable medical record, in the form of a mini-CD, the size and shape of a credit card or health card, that the patient carries at all times. The main database is maintained as the central repository and is updated as needed by healthcare professionals who are authorized to access the database. Updated CDs are re-issued, as appropriate, from the central database. The primary healthcare provider, creates and has access to, the most complete record of a patient’s health and treatment. The record includes their own diagnostics and treatment plans, as well as those of other healthcare providers. In an acute medical situation, attending medical personnel simply access the CD to obtain access to personal identification, medical history, and emergency contacts.

Because the CD is held personally by the patient, and because patient records may need to be accessed in an emergency by medical personnel who do not have pre-authorized access to the central database, the information on the CD is not encrypted. Sensitive data on the central database is encrypted at all times (and regularly backed-up to off-site storage). All transmitted records, such as updates to the central database from a patient’s physician, are encrypted and signed.

6.2.3 Specific security issues

The heart of the system is a browser-based PKI plug-in that uses standard HTML tags and works with any web browser. Two keys are used for the PKI, one for digital signature the other for encryption. User authentication can be as simple as a password or can be based on much stronger methods including biometric techniques. The system permits creation of legally-binding transactions over the Internet.

Because doctors use a variety of document formats and processing techniques in their offices, the application has been developed to accommodate a variety of input data formats, including fax, XML, scanned data and direct browser entry. Whatever the source of the input data, it is all encrypted and stored in the database. An audit trail function applies to the data collection process.

An important innovation allows the developer to define the specific fields that are to be protected from unauthorized access. Encryption can then be performed selectively at the field-level of the database. Patient data such as name, address, telephone and health card numbers are encrypted ensuring the privacy of the patient. At the same time information such as gender age and medical problems are left unencrypted, providing healthcare professionals an excellent source for epidemiological studies. Datamining and data privacy are supported simultaneously.

The data security module controls every user's session-access to patient data on the central servers. Access control functionality is based on who the accessing party is and what they are able to do and see.

Security at the doctor's level limits the doctor's ability to view and modify records over the Internet to the records of those patients for whom he or she is responsible. Logs are maintained on patient file activities so that all changes are tracked. No data is ever deleted. Figure 6.3 illustrates the overall process.

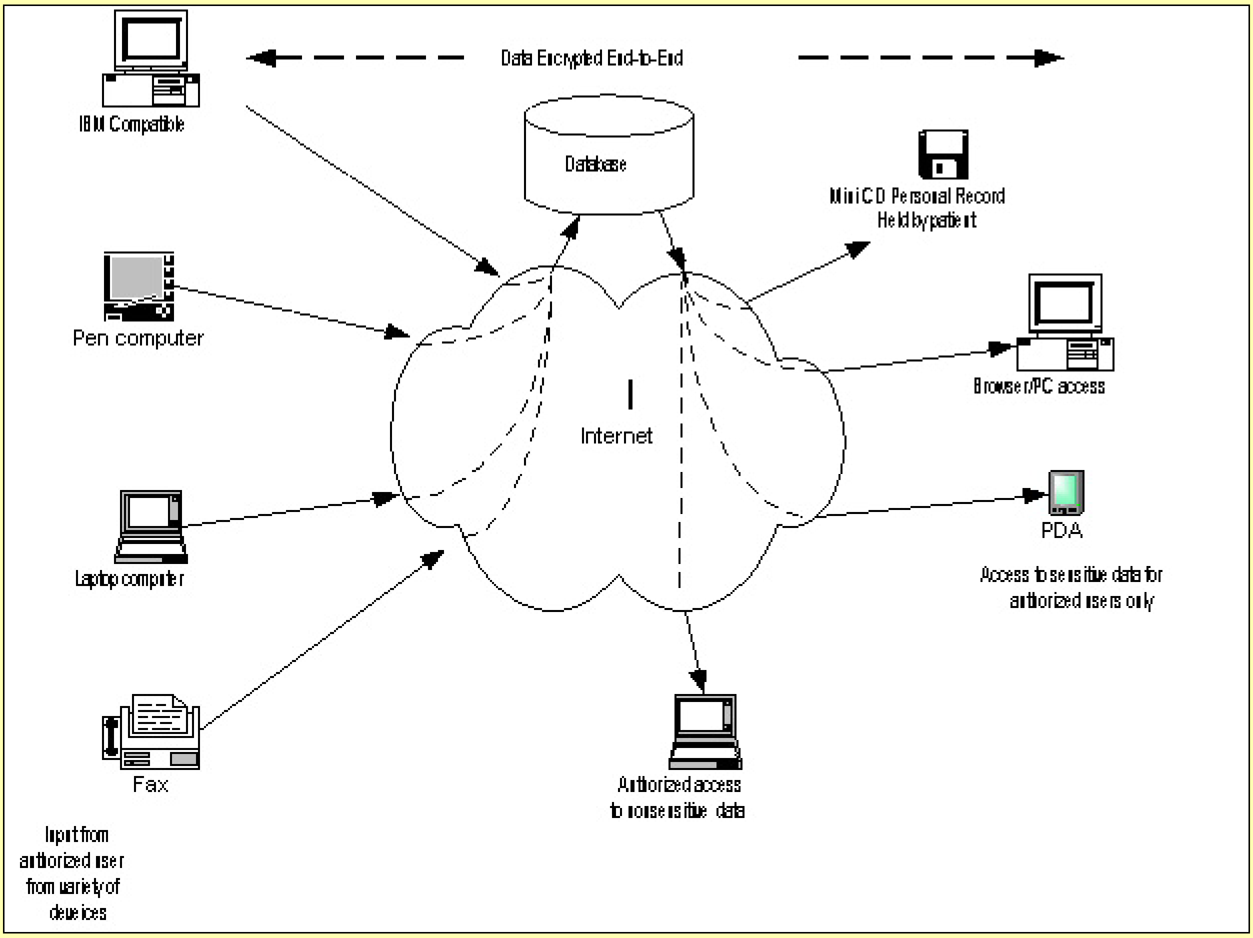
The plug-in is capable of encrypting data for the patient's file such that the file can be seen only by decrypting the data, a task that requires both positive authentication of the user and confirmation of the user’s authorization to view the data. Data submitted via the web application is encrypted and then transmitted to the server where the data is decrypted, enhanced and formatted. After the ASP has completed all the production functions, the raw data is then re-encrypted using the public key of the contributing physician and stored on the server. Only the physician or clinic that contributed the data has access to it at that point.

The use of selective field encryption means that non-sensitive information in the database can be made available to other healthcare professionals (such as pharmacists and laboratory services for example) or for demographic or research purposes, without compromising personal data.

6.2.4 Plugging the wireless gap

Wireless devices (such as Personal Digital Assistants) can be used to access the patient data in this application and their use is growing. However, wireless devices pose a particular challenge to network security. The most common use of the wireless access protocol (WAP) standards requires the session to be terminated at the WAP gateway where the data is decrypted. It is then re-encrypted before it is moved to the next destination. This offers a major opportunity for “man-in-the-middle” attacks at the gateway (otherwise known as “the gap in WAP”) before the data is moved into the enterprise. The PKI encryption used in this application provides full, end-to-end encryption of the data. ensuring its security at all stages during the transmission. The application provides for interoperability between WAP and web and solves the “gap in WAP” problem.

Figure 6.3: Illustration of end-to-end protection of patient information


Data Encrypted End-to-End
IBM Compatible
Database
MiniCD Personal Record Held by patient
Pen computer
Browser/PC access
Internet
Laptop computer
PDA
Access to sensitive data for authorized users only
Fax
Authorized access to nonsensitive data
Input from authorized user from variety of devices

Source: E-witness Internet Security Inc.

6.3 Lessons learned and overall summary of case studies

The threat to networked computers, networks and infrastructures that rely on networks, comes both from within the organization and from outside the organization. It is essential that security countermeasures take account of both sources of threats.

Strong and effective perimeter defence is vital in the fight against both accidental and intentional threats to the network. But perimeter defence alone is not sufficient. Data must be protected while in transit and in storage. Strong cryptographic mechanisms are required to provide effective confidentiality, integrity and non-repudiation services. Access control mechanisms and strong authentication mechanisms are also required to ensure adequate protection of the data resource.

A combination of effective perimeter defence and continuous protection of the data assets can provide strong defence against both network-originated threats and threats that originate within an organization. However, complete protection also requires a full complement of additional countermeasures including physical and personnel security, trusted functionality, audit collection and analysis and business continuity/resumption planning.

Lastly, adequate resources to manage the installation securely, plus management respect for, and commitment to, effective security are essential.

7 Conclusions and possible areas for further study

7.1 The importance of networking infrastructures to the Canadian economy

The available statistics clearly indicate the importance of network infrastructures to the Canadian economy. The large volumes of financial transactions processed electronically every day; the dependence of almost all sectors of industry and government on networks to at least some extent; the increasing emphasis by business and government on online service delivery; and the projected growth in on-line retail commerce, all provide strong evidence of high and growing dependence on both traditional carrier-based networks and the public Internet.

Conclusion 7.1 (a): Both public and private sectors of the Canadian economy are highly dependent on networking infrastructures for their day-to-day operations and this dependence is growing

All sectors of the economy are heavily dependent on the traditional network infrastructures for business communications (voice, fax & data). Increasingly, communications strategies are relying on the public Internet for particular aspects of communication and service delivery. However, it appears that in larger organizations at least, the traditional (carrier-based) communications infrastructure is still being relied upon for essential services and those services most critical, that is services where failure would have a major negative impact. Services offered over the Internet tend to be those where a major failure would cause inconvenience, rather than serious risk to the organization.

Conclusion 7.1 (b): Although both the public and private sectors are increasingly relying on the public Internet for service delivery, to a large extent, Canadian organizations appear to be still using traditional communications channels, rather than the Internet, for their most critical applications.

7.2 Efforts needed to address the criticalities and understand the interdependencies

Although individual aspects of critical infrastructure protection have been addressed for many years, it is only relatively recently that the vital importance of the interdependencies has begun to receive serious attention. The work done in preparation for Y2K was very valuable in highlighting many of the interdependencies, but this work was focused primarily on a single threat, i.e. systems failure due to inability to handle the date correctly. In practice we are faced with a variety of threat agents from many possible sources, in many possible forms and at a time that cannot be predicted. There is, therefore, a need to re-examine the infrastructure criticalities in a broader context and in a more quantifiable way, to identify the points of risk and determine how to protect them.

Conclusion 7.2 (a): There is a need to re-examine infrastructure criticalities to identify the points of risk and to determine how to protect them.

Infrastructure protection approaches are traditionally very compartmentalized. The two solitudes of the traditional emergency measures organizations (who deal with natural disasters) and the computer emergency response teams (who deal with cyber incidents) are very evident. But industry also approaches infrastructure protection in a very compartmentalized way, with individual industry groups (the carriers, the financial services industry, the utilities etc) each preferring to address their infrastructure protection issues individually and in a very low-key way, with little focus on the broader interdependencies. The need for a high degree of coordination in infrastructure protection is strongly indicated.

Conclusion 7.2 (b): There is a need for a coordinated approach that addresses both the emergency measures aspects and the cyber security aspects of infrastructure protection.

The interdependencies, and the ripple effect of failure in one area on other areas, are still not well understood. There is a need to get a better overall understanding of the interdependencies. Once the interdependencies have been assessed, the issues of how to protect them and who will bear the cost of that protection need to be determined.

There is also a growing concern over the possible impact that identifying criticalities might have on corporate liability. If, for example, a national or international organization were to identify certain private sector criticalities, would that increase industry’s liability and would insurance premiums rise? Would some industries find it impossible to get insurance at all as a result?

There is clearly an enormous amount of work to do to gain a better understanding of the interdependencies of critical infrastructure components and to determine the implications of those interdependencies.

Conclusion 7.2 (c): Critical Infrastructure Protection comprises many facets, the interdependencies of which are not yet well understood. Much work needs to be done to identify the interdependencies and the potential implications of those interdependencies.

7.3 The robustness of networks

The long-established business-resumption planning and back-up procedures associated with the traditional carrier networks, together with centrally-coordinated emergency planning and restoration, provide a reasonable degree of confidence that recovery from serious network failure could be effected reasonably quickly in most cases.

The public Internet, while inherently robust in design, suffers from a number of vulnerabilities that make its reliability problematic in some circumstances. To a large extent, lack of robustness on the Internet side is between the local Internet Service Provider (ISP) and the end user. Individual ISPs offer varying degrees of reliability and restoration capability. Additionally, the ability of an ISP to resist malicious code and denial of service attacks differs greatly from company to company. Lastly, individual end-user systems are vulnerable to a wide range of Internet-based attacks, many of which, if realized, could cause serious and prolonged failure of the end system.

Conclusion 7.3: Traditional carrier networks are relatively robust: the Internet much less so.

7.4 The risk to network infrastructures

Prior to deregulation, carriers operated in a monopoly environment in which there were relatively few players and in which cooperation and mutual trust were largely the order of the day. Deregulation, while having many obvious benefits, has resulted in carriers operating under looser rules, with much greater competitiveness between carriers and a lessening of trust, cooperation and voluntary mutual aid. This is particularly the case with respect to the newer carriers. In today’s Internet environment, there are almost no rules with respect to who can offer services as an ISP, and yet ISPs effectively have the right to use the traditional communications infrastructure. Carriers are obliged to make their facilities available, even though the ISP may have no track record and there may be zero trust between the carrier and the ISP. A terrorist organization could quite easily establish an ISP and gain access to information about the network infrastructures. Such information could be used to facilitate serious cyber attacks.

Whereas the traditional carrier infrastructure had a hierarchy with quite distinct interfaces between the users (i.e. between the user and the network) and the carriers (network to network), the Internet infrastructure is flat and gives users much more control. Users can easily obtain network addressing capabilities with access to routers, hubs and bridges. Voice-over-IP means the ISPs can gain access to signalling systems. The result is that it is possible for a subscriber to gain control of the network infrastructure.

In this environment it is very difficult to prevent either accidental or malicious attacks on the network infrastructure.

Conclusion 7.4: Traditional network infrastructures are at risk as a result of the changed communications environment.

7.5 The impact of Internet-based threats

The Internet is a major communications conduit but it is highly vulnerable to a wide range of threats, mostly due to malicious users, but also due to inherent weaknesses in commonly-used software. The reality is that the Internet was not designed to handle many of the types of transaction for which it is now being used. Specifically, it was designed as very open network without much thought being given to protecting against the kind of security threat that it incubates and nurtures so well. Threat agents have been greatly assisted by changing circumstances, particularly the dramatic increase in use of the Internet itself and the changes in the regulatory environment.

The Internet has long been recognized as a primary conduit of malicious attacks. In the current environment it is entirely possible to attack vulnerable elements of the critical infrastructure through the Internet, particularly where the infrastructure controls are administered remotely over a network. The ability of users to gain control of the network infrastructure mentioned above is one element of this problem.

A second, and possibly even more pervasive threat, results from deficiencies in the software (particularly management software, but other software as well) used on Internet-based systems. Sources of software vulnerabilities have been generally identified as: sloppy hand-coding of protocols; sloppy practice in protocol implementation and set-up; lack of rigorous verification testing; and failure to use formal methods. Certification and accreditation of products could largely eliminate these problems by proving code and processes to be correct.

Testing by Oulu University in Finland recently exposed serious vulnerabilities in the widely-used version 1 of the Simple Network Management Protocol (SNMP) and the Light Directory Access Protocol (LDAP). The formal definition language Abstract Syntax Notation 1 (ASN1) has been implicated in both of these vulnerabilities but experts have not agreed on whether the problem lies with the Basic Encoding Rules for ASN1 or the way the rules are used in implementations. Since the Basic Encoding Rules are used very widely in protocols running on the world-wide telecommunications infrastructure, the problem has serious implications regardless of the root cause.

Vulnerabilities in vendor proprietary software are commonplace and now we are seeing serious vulnerabilities in the open source/open standards specifications. To some extent we are again coming face-to-face with the philosophical and practical divide between the formal standards processes, which require a thorough review process before approval of the standards, and the Internet standards processes in which review is open but the primary requirement for adoption is two inter-operable implementations.

Given that software suppliers and users of Internet software (particularly the ISPs but also anyone with a direct attachment to the Internet) are almost totally uncontrolled, it is going to be very difficult to mandate the used of “correct” software. However, in view of the potential for damage to the critical infrastructure though Internet-borne acts of malfeasance, one has to question how much longer the Internet-espoused philosophy of “rough consensus and running code” can prevail.

Conclusion 7.5: Critical infrastructures are at risk from Internet-based threats. There is a need for aggressive defensive measures to protect systems and information from attack and for much more effort to be put into ensuring the “correctness” of networking software and systems.

7.6 The application of cyber-crime laws

Canada has a reasonably effective set of legislative measures that can be used in the fight against cyber-crime. However, given the ubiquity of the Internet, strong international cooperation and action is required. Not only is there a lack of consistency in the cyber-crime laws from country-to-country, but there are also varying degrees of enthusiasm on the part of national administrations in the fight against cyber crime. As a result, some regions of the world have effectively become sanctuaries for hackers and Internet fraud artists. There is an urgent need for consistent laws dealing with Internet use, and consistent and vigorous application of those laws. In recognition of this need, Canada has signed the Council of Europe Convention on Cyber-Crime and is active in the G8 Lyons Group on High-Tech Crime.

Conclusion 7.6: Cyber-crime laws and their application are not consistent from country to country. There is a need for greater consistency in cyber-crime laws and in their application.

8 References and Web addresses

This paper has been developed using information from a number of sources. In addition to the explicit references below, data has been obtained from publicly-available resource material obtained from the following sources:

Canadian Embassy, Canberra

Canadian Embassy, Washington

Canadian Security Establishment

Department of Justice, Canada

Foreign Affairs and International Trade

Statistics Canada

Office of Critical Infrastructure Protection
and Emergency Preparedness

Industry Canada

Information Canada

National Resources Canada

Department of the Solicitor General of Canada

Treasury Board Secretariat

Royal Canadian Mounted Police

Specific reference documents

1. *Building Trusted e-Government* - Report on the activities of the Public Sector CIO Council Subcommittee on Information Protection From January 1999/ April 2000

2. *Principles and Guidelines for payments over Open Communication Networks*, Canadian Payments Association, October 5th 2000.

3. *Government of Canada Security Policy*, Treasury Board Secretariat, February 2002.

4. *Technical Security Standard for IT Security*, Royal Canadian Mounted Police, 1997

5. *The Canadian Telecommunications Service Industry: 1999-2000*, Industry Canada, 2001

6. *Telecommunications Service in Canada: An Industry Overview, 2000-2001*, Industry Canada, 2002

7. *Canadian Infrastructures and their Dependencies*, prepared by the National Contingency Planning Group, 2000

8. *IT Security Zones: Baseline Security Requirements*, Communications Security Establishment, March 28th 2002.

Relevant websites

Government of Canada	http://canada.gc.ca/main_e.html
Statistics Canada	http://www.statcan.ca/
RCMP Technical Security Branch	http://www.rcmp-grc.gc.ca/tsb/index.htm
OCIPEP	http://www.ocipep-bpiepc.gc.ca
Communications Security Establishment	http://www.cse.dnd.ca/
Industry Canada	http://www.ic.gc.ca/
Treasury Board Secretariat	http://www.tbs-sct.gc.ca/
Canadian Centre for Emergency Preparedness (has links to federal, provincial and municipal emergency preparedness sites in Canada plus many US links)	http://www.ccep.ca/ccep.ca

Annex A: Key organizations in critical infrastructure protection

Although individual organizations have been involved in addressing various aspects of infrastructure protection (particularly the areas of emergency preparedness, telecommunications and IT security) for many years, it is only recently that the issue of critical infrastructure protection has begun to be approached in a coordinated manner. Cooperation between agencies and organizations in specific areas is well established but the broad range of vulnerabilities and their interdependencies is only now becoming fully recognized. This realization is mainly due to three factors: the result of the extensive preparations for the Year 2000 (Y2K) and the concomitant recognition of interdependencies; the growing reliance of all sectors of the economy on the public Internet; and the dramatic increase in terrorist and criminal activities directed both towards cyberspace and traditional infrastructures.

Effective critical infrastructure protection requires coordinated action across industry and at all levels of government. The effort in Canada is being spearheaded by a relatively small number of lead agencies, most of which have historically had some role in national or civil defence, in fighting crime, or in countering computer/communications threats.

This section provides an overview of the key organizations involved in protecting Canada’s critical infrastructure.

Federal government lead agencies

The summaries below are extracted from the published mandates of the departments and agencies.

The Office of Critical Infrastructure Protection and Emergency Preparedness

The *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP) was established in February 2001. OCIPEP is a civilian organization that reports to the Minister of National Defence and combines the responsibilities of *Emergency Preparedness Canada* with broad expertise gained during the preparations for Y2K and the increasing recognition of need for a comprehensive approach to protecting critical infrastructure. The Office is charged with developing and implementing a comprehensive approach to protecting Canada's critical infrastructure in both its physical and cyber dimensions, regardless of the source of threats and vulnerabilities. It also acts as the government’s primary agency for ensuring national civil emergency preparedness.

In fulfilling it’s mandate, the Office aims to:

– - build partnerships with the private sector, the provinces, territories and municipalities, and key international partners, the US in particular;

– - promote dialogue among Canada's critical infrastructure owners and operators and foster information sharing on threats and vulnerabilities;

– - provide a focal point for the federal government's own cyber incident analysis and coordination efforts and support federal departments and agencies in meeting their responsibilities for protecting their IT systems and networks;

– - promote other areas of cooperation such as raising awareness, enhancing education and training, and promoting information technology security research and development; and

– - achieve an appropriate level of national civil emergency preparedness.

The Communications Security Establishment

The *Communications Security Establishment* (CSE), an arm of the *Department of National Defence*, is mandated to:

- provide advice, guidance and services to help ensure the protection of Government of Canada electronic information and information infrastructures;
- acquire and provide foreign signals intelligence; and
- provide technical and operational assistance to federal law enforcement and security agencies.

CSE provides technical advice, guidance and services to the Government of Canada to maintain the security of its information and information infrastructures. CSE is recognized for is expertise in information assurance and is a trusted supplier of made-for-Canada solutions to protect information, and services to assess the security of IT products, systems and networks.

In fulfilling its IT security mandate CSE helps to protect Canada's electronic information assets and information infrastructures by:

- supporting the development of IT security policy and standards for the Government;
- analyzing vulnerabilities in IT products, systems and networks, and recommending appropriate countermeasures;
- approving cryptographic, computer and network security products and systems for the protection of electronic information and electronic commerce;
- developing and supporting the development of IT security products, systems and services; and
- providing IT security consulting services and support to the federal government, and to other levels of government and Canadian organizations.

CSE's ITS programme provides leadership and support to many secure e-government initiatives including Critical Infrastructure Protection, the Government of Canada Information Protection Co-ordination Centre and the Government of Canada Public Key Infrastructure.

CSE’s mandate under the National Defence Act has recently been amended to allow the collection of communications of a legitimate foreign intelligence target located abroad if those communications go into or out of Canada and to provide the necessary technical assistance to those responsible for Canadian government computer systems and networks in order to effectively protect them from mischief, unauthorized use or interference.

CSE maintains unique partnerships with the US National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ), Australia's Defence Signals Directorate (DSD), and New Zealand's Government Communications Security Bureau (GCSB).

The Royal Canadian Mounted Police

The *Royal Canadian Mounted Police* (RCMP), known almost universally as “The Mounties” is the Canadian national police service and an agency of the *Ministry of the Solicitor General of Canada*. The RCMP is unique in the world in that it is a national, federal, provincial and municipal policing body, providing federal policing service to all Canadians and contracted policing services to all provinces except Ontario and Quebec, to the territories, to approximately 198 municipalities and, under 172 individual agreements, to 192 First Nations communities.

The Technical Security Branch of the RCMP is responsible for many aspects of physical and information technology security within the federal government including: developing technical documentation and operational standards relating to physical and IT security and advising on their application; providing advice on threat and risk assessments; conducting specialized training; providing technical assistance to investigations involving IT; and providing security advice relating to contract compliance and site facilities. The RCMP is the lead government agency for providing advice and guidance in the selection and deployment of cost-effective physical security safeguards, and the development of physical security standards. In addition, the Counter Technical Intrusion Section carries out technical inspection services (sweeps) for the federal, provincial and municipal governments and for other police forces, carries out technical evaluations in cases of theft or interception of telecommunication services, and provides expert witnesses in court cases.

The RCMP works closely with other federal agencies and with other police forces in Canada and around the world. The Canadian Police Information Centre computer system, which is accessed by police forces across the country, is regarded as the electronic backbone of Canadian law enforcement. The RCMP recently has reached an agreement to underwrite PKI-secured communications that will allow police forces all across the country to communicate with one another securely over the Internet. When the technology is rolled out across the country there will be approximately 75,000 users of this technology within the RCMP, municipal, and provincial police forces.

The Canadian Security Intelligence Service

The primary objective of the *Canadian Security Intelligence Service* (CSIS) is to investigate and report on threats to the security of Canada. CSIS's mandate is to collect, analyze and retain information or intelligence on activities that may, on reasonable grounds, be suspected of constituting threats to the security of the nation, and to report to and advise the Government of Canada. CSIS also provides security assessments, on request, to all federal departments and agencies, with the exception of the RCMP. CSIS does not have law enforcement powers, therefore, all law enforcement functions are the responsibility of police authorities.

In response to the rise of terrorism world-wide and the demise of the Cold War, CSIS has made public safety its first priority.

The Treasury Board Secretariat

The *Treasury Board Secretariat* (TBS) is a central government agency. Its mission is to help the Government of Canada manage its human, financial, information and technology resources. Its responsibilities for the general management of the government affect initiatives, issues and activities that cut across all policy sectors managed by 22 operating departments and some 100 other organizational entities.

The Secretariat acts as the general manager and employer of the Public Service. It provides leadership, direction and advice to departments and agencies on expenditure management, financial and information management regulatory affairs, property and material management, use of technology and information management, business process renewal and contracting management.

Of particular interest in the context of this report is the Secretariat's responsibility for the *Government Security Policy* (ref. 3) (which applies to protection of the federal government's information assets) and it's derivative technical security policies, standards and guidelines that are developed in close consultation with the Communications Security Establishment and the Royal Canadian Mounted Police. In addition, TBS leads the implementation and policy development work of Government of Canada Public Key Infrastructure (GoC/PKI) initiative.

The Solicitor General of Canada

The *Ministry of the Solicitor General* is responsible for protecting Canadians and helping to maintain Canada as a peaceful and safe society.

The Solicitor General portfolio consists of the Department and four agencies: the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), the Correctional Service of Canada (CSC) and the National Parole Board (NPB). There are also four Ministry review bodies that ensure accountability and full respect for the rule of law.

The department works closely with the *Department of Justice*, which has the primary responsibility for criminal justice policy at the federal level, and also has extensive dealings with other federal departments, provincial and territorial governments, as well as the voluntary and private sectors.

Internationally, the department works closely with the United States on trans-national crimes such as terrorism, smuggling, organized crime and crimes using computers.

Industry Canada

Industry Canada has a number of responsibilities relating to research, regulation, licencing and operation of telecommunications in Canada. In general, these powers are granted under three Acts of Parliament: the Telecommunication Act, the Radiocommunication Act and the Industry Canada Act. Industry Canada maintains an *Emergency Telecommunications Operations Centre* (EOC) in Ottawa and in five regional offices. In an emergency, the EOC works with the *Government Emergency Operation Centre* and provincial emergency coordination centres to coordinate telecommunications services. Industry Canada maintains a close working relationship with the Canadian Telecommunication Emergency Preparedness Association (CTEPA) and the Government of Canada Emergency Programs and Operation Centres to mitigate the disruptive effects of emergencies on domestic and external telecommunications. Industry Canada also maintains a database of emergency numbers that are provided with three services: Priority Access to Dial Tone; Load Line Control; and Priority Restoration. The database, which covers only essential users identified in government plans, includes 5000 municipalities, 1000 federal and provincial government departments and non-government organizations. The organizations included in the database cover emergency users (e.g. hospitals, emergency services, critical industries and key emergency personnel), essential services and all functions directly related to supporting essential goods and services to maintain law and order, health and security.

Based on this emergency response expertise and on expertise with respect to security issues around e-commerce, Industry Canada has been identified by OCIPEP as the sectoral lead for CIP activities focused on the telecommunications sector. The department will be developing additional activities that focus on partnering with industry around CIP, as well as working closely with OCIPEP on CIP issues and the telecommunications industry sector.

Provincial, territorial and municipal roles

Because of the large number of organizations involved at the provincial and municipal levels of government, no detailed breakdown of individual organizations will be attempted in this report. Instead, an overview of the more general approaches is presented.

Critical infrastructure protection and emergency preparedness in the provinces and territories has traditionally focussed more on the human and physical infrastructure, rather than cyber protection. That is now changing somewhat, though there are still quite different perspectives depending on whether one comes from an emergency preparedness or an IT background. Provincial and territorial responsibility is assigned to an existing ministry that varies from administration to administration. Typically, responsibility tends to be lodged in the Ministry of Municipal Affairs or the Ministry of the Solicitor General.

Both federally and provincially, there has traditionally been close liaison with municipalities in areas such as emergency preparedness, as the municipalities traditionally play a major role in responding to emergencies through the fire, police and ambulance services.

OCIPEP is now cooperating closely with the provinces even to the extent that federal and provincial teams are being co-located, sharing facilities and knowledge.

One organization that is sponsoring cooperation on information protection issues among the various levels of government through one of its subgroups is the Public Sector Chief Information Officer's Council.

Public Sector Chief Information Officer's Council

The *Public Sector Chief Information Officer's Council* represents all federal, provincial and territorial governments. Through its subcommittee on information protection, it encourages governments at all levels to work together towards information protection and to forge nationally-affirmed protective measures.

The goals of the National CIO Sub-committee on Information Protection are to initiate activities:

- to secure electronic service delivery and commerce;
- to take a proactive approach in dealing with emerging network security issues;
- to improve trust and confidence in electronic network and transactions;
- to maintain a consistent approach to information protection;
- to act as a focal point for federal and provincial efforts in the maintenance of public trust in government networks;
- to give immediate and careful attention to the creation of a capability to assess and reduce vulnerabilities in critical technical infrastructures; and
- to develop organizations and mechanisms to prevent and respond to cyber or physical attacks on networks and computational infrastructure.

Private sector organizations

In general, private sector groups take a very low-visibility approach with respect to publicizing their emergency preparedness and infrastructure protection activities. That is not to imply that nothing much is being done. In fact, a considerable amount of effort is being expended on these topics, but it is generally felt that such preparations are not for public discussion.

Organizations that belong to federally regulated sectors are often obligated to implement emergency readiness and business resumption planning measures. Examples include the financial services sector (governed by regulations from the *Bank of Canada*, the *Department of Finance* and the *Office of the Superintendent of Financial Institutions*) and the energy sector which is subject to *National Energy Board* requirements regarding emergency and business continuity planning.

To a large extent, and from a sector standpoint, emergency planning is developed collaboratively through industry or sectoral associations. For example, the both the *Canadian Bankers Association* (the main representative body for banks in Canada whose membership includes over 40 domestic and foreign-chartered banks) and the *Canadian Electricity Association* (whose membership represents about 95 percent of Canada's installed generating capacity plus major electrical manufacturers) have sub-groups that specifically address these topics.

With telecommunications deregulation, the traditional carriers no longer have a single association. However, the Industry Canada Emergency Telecommunications Service liaises closely with all carriers and the carriers have working agreements that provide for mutual assistance in the event of an emergency. Two carrier groups have been established to address emergency preparedness: the *Canadian Telecommunications Emergency Preparedness Association* and the *Canadian Carrier Service Forum.*

A private sector organization operates *CanCERT*™ , Canada’s first national Computer Emergency Response Team.

The Canadian Telecommunications Emergency Preparedness Association

The *Canadian Telecommunications Emergency Preparedness Association* (CTEPA) is an association of Emergency Planners representing the wireline, wireless and satellite facility-based telecommunications companies in Canada.

The members share a united commitment and vision for telecom emergency preparedness related to an International, National or Regional Disaster. They share and exchange information on common emergency preparedness issues. The association provides a forum for building a network of emergency planners and to promote emergency preparedness within the telecommunications industry.

CTEPA maintain a close working relationship with governments via Industry Canada - Emergency Telecommunications.

The Canadian Carrier Service Forum

The *Canadian Carrier Service Forum* admits only corporate members. The forum comprises mainly the carriers’ network managers. The primary focus of the group is the use of network management tools to respond to emergency situations. The group focuses on both voice and data aspects of networking.

CanCERT™

CanCERT™ , Canada’s first national Computer Emergency Response Team has operated a 24/7 service since 1998. It’s mission is to be the trusted centre for the collection and dissemination of information related to networked computer threats, vulnerabilities, incidents and incident response for Canadian Government, business and academic organizations.

Annex B: Relevant extracts from the Canadian Criminal Code

PART VI: INVASION OF PRIVACY

Definitions

183. In this Part,

"authorization" means an authorization to intercept a private communication given under section 186 or subsection 184.2(3), 184.3(6) or 188(2);

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept a private communication, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"intercept" includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof;

...

"private communication" means any oral communication or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it;

"public switched telephone network" means a telecommunication facility the primary purpose of

which is to provide a land line-based telephone service to the public for compensation;

"radio-based telephone communication" means any radiocommunication within the meaning of the Radiocommunication Act that is made over apparatus that is used primarily for connection to a public switched telephone network;

.....

Consent to interception

183.1 Where a private communication is originated by more than one person or is intended by the originator thereof to be received by more than one person, a consent to the interception thereof by any one of those persons is sufficient consent for the purposes of any provision of this

Interception of Communications

Interception

184. (1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device,

wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

(2) Subsection (1) does not apply to

(a) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it;

(b) a person who intercepts a private communication in accordance with an authorization or pursuant to section 184.4 or any person who in good faith aids in any way another person who the aiding person believes on reasonable grounds is acting with an authorization or pursuant to section 184.4;

(c) a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,

(i) if the interception is necessary for the purpose of providing the service,

(ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or

(iii) if the interception is necessary to protect the person's rights or property directly related to providing the service; or

(d) an officer or servant of Her Majesty in right of Canada who engages in radio frequency spectrum management, in respect of a private communication intercepted by that officer or servant for the purpose of identifying, isolating or preventing an unauthorized or interfering use of a frequency or of a transmission.

184.6 For greater certainty, an application for an authorization under this Part may be made with respect to both private communications and radio-based telephone communications at the same time.

[http://canada.justice.gc.ca/en/laws/C-46/35184.html]

PART IX: OFFENCES AGAINST RIGHTS OF PROPERTY

322. (1) Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another

person, anything, whether animate or inanimate, with intent

(a) to deprive, temporarily or absolutely, the owner of it, or a person who has a special property or interest in it, of the thing or of his property or interest in it;

(b) to pledge it or deposit it as security;

(c) to part with it under a condition with respect to its return that the person who parts with it may be unable to perform; or

(d) to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted.

(2) A person commits theft when, with intent to steal anything, he moves it or causes it to move or to be moved,or begins to cause it to become movable.

(3) A taking or conversion of anything may be fraudulent notwithstanding that it is effected without secrecy or attempt at concealment.

(4) For the purposes of this Act, the question whether anything that is converted is taken for the purpose of conversion, or whether it is, at the time it is converted, in the lawful possession of the person who converts it is not material.

[http://canada.justice.gc.ca/en/laws/C-46/35685.htm]

PART IX: OFFENCES AGAINST RIGHTS OF PROPERTY

Unauthorized use of a computer

342.1 (1) Every one who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service,

(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or

(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Definitions

(2) In this section,

"computer password" means any data by which a computer service or computer system is capable of being obtained or used;

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(a) contains computer programs or other data, and

(b) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other function;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.

"traffic" means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way.

Possession of device to obtain computer service

342.2 (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under

circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or

(b) is guilty of an offence punishable on summary conviction.

[http://canada.justice.gc.ca/en/laws/C-46/35685.html]

PART X: FRAUDULENT TRANSACTIONS RELATING TO CONTRACTS AND TRADE

380. (1) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service,

(a) is guilty of an indictable offence and liable to a term of imprisonment not exceeding ten years, where the subject-matter of the offence is a testamentary instrument or the value of the subject-matter of the offence exceeds five thousand dollars; or

(b) is guilty

(i) of an indictable offence and is liable to imprisonment for a term not exceeding two years, or

(ii) of an offence punishable on summary conviction, where the value of the subject-matter of the offence does not exceed five thousand dollars.

(2) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, with intent to defraud, affects the public market price of stocks, shares, merchandise or anything that is offered for sale to the public is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years.

381. Every one who makes use of the mails for the purpose of transmitting or delivering letters or circulars concerning schemes devised or intended to deceive or defraud the public, or for the purpose of obtaining money under false pretences, is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

[http://canada.justice.gc.ca/en/laws/C-46/35885.html]

PART XI: WILFUL AND FORBIDDEN ACTS IN RESPECT OF CERTAIN PROPERTY

430. (1) Every one commits mischief who wilfully

(a) destroys or damages property;

(b) renders property dangerous, useless, inoperative or ineffective;

(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or

(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

(1.1) Every one commits mischief who wilfully

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the lawful use of data; or

(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

(2) Every one who commits mischief that causes actual danger to life is guilty of an indictable offence and liable to imprisonment for life.

(3) Every one who commits mischief in relation to property that is a testamentary instrument or the value of which exceeds five thousand dollars

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(b) is guilty of an offence punishable on summary conviction.

(4) Every one who commits mischief in relation to property, other than property described in subsection (3),

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or

(b) is guilty of an offence punishable on summary conviction.

(5) Every one who commits mischief in relation to data

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(b) is guilty of an offence punishable on summary conviction.

(5.1) Every one who wilfully does an act or wilfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or

(b) is guilty of an offence punishable on summary conviction.

(6) No person commits mischief within the meaning of this section by reason only that

(a) he stops work as a result of the failure of his employer and himself to agree on any matter relating to his employment;

(b) he stops work as a result of the failure of his employer and a bargaining agent acting on his behalf to agree on any matter relating to his employment; or

(c) he stops work as a result of his taking part in a combination of workmen or employees for their own reasonable protection as workmen or employees.

(7) No person commits mischief within the meaning of this section by reason only that he attends at or near or approaches a dwelling-house or place for the purpose only of obtaining or communicating information.

(8) In this section, "data" has the same meaning as in section 342.1.

[http://canada.justice.gc.ca/en/laws/C-46/35885.html#rid-36034]

List of Acronyms and Abbreviations

ATM	Automatic Teller Machine
CAP	Community Access Program
CBA	Canadian Banker’s Association
CPA	Canadian Payments Association
CRTC	Canadian Radio-television & Telecommunications Commission
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DND	Department of National Defence
EDI	Electronic Data Interchange
GDP	Gross Domestic Product
GoC	Government of Canada
GOL	Government Online
GSP	Government of Canada Security Policy
ISP	Internet Service Provider
IT	Information Technology
OCIPEP	Office of Critical Infrastructure Protection and Emergency Preparedness
OSFI	Office of the Supervisor of Financial Institutions
PC	Personal Computer
PCS	Personal Communications Services
PKI	Public Key Infrastructure
RCMP	Royal Canadian Mounted Police
SSL	Secure Sockets Layer
Statcan	Statistics Canada
TSSIT	Technical Security Standard for IT Security
TBS	Treasury Board Secretariat
VPN	Virtual Private Network
WAP	Wireless Access Protocol
Y2K	Year 2000