Public Safety and Emergency Preparedness Canada
Sécurité publique et Protection civile Canada

Critical Information Infrastructure Accountability in Canada

Canada

Acknowledgments

This publication has been prepared for:

Public Safety and Emergency Preparedness Canada

340 Laurier Avenue West, 12th Floor
Ottawa, Ontario K1A 0P8
Internet: www.psepc-sppcc.gc.ca

Authors:

Donald B. Johnston – Project Leader
Robert Fabian
Keith L. Geurts
Donald S. Hicks
Andrew Huzar
Norman D. Inkster
Alan Jaffee
Paul McLennan
Douglas J. Nash
E. Michael Power
Mark Stirling

Gowling Lafleur Henderson LLP
Barristers & Solicitors
Patent & Trademark Agents
Suite 5800, Scotia Plaza
40 King Street West
Toronto, Ontario, Canada M5H 3Z7
Telephone: 416-369-7200

This material is based upon work supported by the Division of Research and Development (DRD) in the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), under Contract Reference No. 2003D022. On 12 December 2003, the Office of Critical Infrastructure Protection and Emergency Preparedness was integrated into a new department, Public Safety and Emergency Preparedness Canada (PSEPC). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Public Safety and Emergency Preparedness Canada.

Catalogue No.: PS48-7/2004E-PDF
ISBN: 0-662-38155-6

Executive Summary

OBJECTIVES

There was broad and general agreement throughout our extensive research that Canada is becoming increasingly dependent on the Information Infrastructure for both our safety and the functioning of our society. As our dependency on this critical infrastructure increases, questions about accountability may become more important.

In this report we build an extensive picture of current thinking related to Canada's Critical Information Infrastructure, and further, we examine the broad range of issues and concerns that arise in connection with accountability. More specifically, we examined:

1. The current state and future evolution of the Information Infrastructure;
2. The concept of accountability as it relates to the Critical Information Infrastructure;
3. Accountability mechanisms currently in place that affect the Critical Information Infrastructure;
4. Accountability lessons from other environments that may be relevant to the Critical Information Infrastructure;
5. As perceived by major stakeholders, the current state of accountability for Canada's Critical Information Infrastructure;
6. Major issues, questions, and concerns about accountability; and
7. Suggestions for improving the reliability, security and functionality of the Critical Information Infrastructure.

THE RESEARCH

We conducted telephone interviews with key stakeholders in Canada and the U.S. regarding the areas listed above. We also undertook a substantial amount of secondary research. The materials that we examined are listed in the Bibliography section of the report.

INFORMATION INFRASTRUCTURE DEVELOPMENT

The report includes a section on the background leading to Canada's current Information Infrastructure. This section also includes material on development trends in each of the key Information Infrastructure components – hardware, software, networks, and services. Broad technology projections out to 2020 provide a future context.

The Internet is an important source of ideas and technology to be used in our Information Infrastructure. The Internet is also a component of our Critical Information Infrastructure and a key resource to be used by Canada's Critical Information Infrastructure. We include a brief history of the Internet in the U.S., and then move into Canada, paying particular attention to the period after 1994 when commercial use was allowed.

Moore's Law is used to explain many past and future hardware developments. Software is explained in terms of programming generations leading to the visual programming possibilities of today, where the diagram for a program *is* the program. Networks are examined in terms of the key changes that are likely to be observed. The services story today is largely about outsourcing – inshore, nearshore, and farshore.

The technology projection to 2020 draws heavily on a RAND study done for the U.S. military. It concluded that by 2020 there will be an increasingly fuzzy distinction between physical objects and their cyber image. Wireless technology will be pervasive, providing high capacity connections. Hardware will find ways to continue to follow Moore's Law. The network will be our universal connection. We provide a summary of the RAND report's findings.

CRITICAL INFORMATION INFRASTRUCTURE ACCOUNTABILITY OBJECTIVES

The following are some of the questions that the research team asked in order to gain a better understanding of the entire Critical Information Infrastructure, as well as the actual, potential, or possible role of accountability within it:

1. How does the level, or allocation of accountability among participants in the Critical Information Infrastructure affect the development and operation of the Critical Information Infrastructure?
2. In what ways has accountability contributed to a desirable, or undesirable, state of the Critical Information Infrastructure?
3. What attributes are best used to describe the current and future Critical Information Infrastructure, and what are the corresponding metrics?
4. What current research is available about each such attribute, and what else should be known?
5. How and in what way is the desired future state of the Critical Information Infrastructure related to each such attribute?
6. What are the inter-relationships among the various relevant attributes of the Critical Information Infrastructure, and what are the trade-offs among them?
7. What are the inter-relationships, including trade-offs, between various attributes of the Critical Information Infrastructure and the policies that govern it?

Our research indicated strongly that there are two mechanisms that can help to enhance the reliability and functionality of the Critical Information Infrastructure: diversity and accountability. In a perfect world, we might have a Critical Information Infrastructure that was composed of a number of diverse, but functionally equivalent components at each level. We might have clear and meaningful accountability for all aspects. This would give us two separate failsafe mechanisms. In the real world, there may be difficulties in achieving diversity and high levels of accountability.

ACCOUNTABILITY IN OTHER ENVIRONMENTS

The challenge of getting accountability 'right' for critical infrastructures is universal. It extends to both other critical infrastructures and other jurisdictions. Many lessons have been learned, both from specific initiatives, and from the general evolution of accountability. We believe that a number of these lessons may have relevance to Critical Information Infrastructure accountability and we discuss that relevance.

Healthcare and Legal

Professions are in the position to define standards and enforce compliance with them. The threat of regulation ensures integrity. Professional standards may be necessary if we are to achieve meaningful accountability in the Critical Information Infrastructure.

Financial Services

Public sector regulation may be required under certain circumstances. In volatile and globally connected environments, formal processes may be required, with regular review and updating. Agreed upon measurements and processes may be required to hold entities accountable. Finally, when an entity does not control all inputs, the most effective type of accountability is often for process.

Electric Utilities

Accountability for results at the interface between private systems and the larger system may be the only practical approach. The interface provides a point of measurement. The Critical Information Infrastructure is composed of many private systems interfaced to a vast shared system. Operators of the private systems might be held accountable for not 'exporting grief' to the shared system.

Y2K

Our collective success with Y2K can be a source of some pride, but there is no necessary reason to assume that the same approach should be used to protect Canada's Critical Information Infrastructure. Although the approach may not be particularly applicable to the Critical Information Infrastructure, Y2K provides an example of how a threat perceived to be serious enough may be able to galvanize both the public and private sectors to effective action.

Treadway Commission/Sarbanes-Oxley

Understanding a serious potential problem is not enough. Identifying a solution is not enough. The solution must be implemented. This takes resources and will, neither of which may be easy to generate in the absence of a disaster. When disasters happened in the form of major financial scandals (e.g. Enron and WorldCom), resources and will was quickly forthcoming. Sarbanes-Oxley was the result.

EU Directive / PIPEDA (Personal Information Protection and Electronic Documents Act)

Initiatives in one jurisdiction can spawn corresponding positive initiatives in other jurisdictions. Canada's Critical Information Infrastructure is part of the global Information Infrastructure. Initiatives Canada decides to undertake may benefit Canada and spawn corresponding positive benefits elsewhere.

HIPAA (Health Insurance Portability and Accountability Act)
Economics may not be the only or primary driver of significant change. HIPAA provides a compelling counter example. Initiatives that are unpopular with some can still succeed with sufficient popular support. Changes to the accountability framework for CII may add more costs than profits, but the HIPAA experience indicates that this may only be one factor in deciding on action and not the decisive factor.

CRITICAL INFORMATION INFRASTRUCTURE ACCOUNTABILITY MECHANISMS

Accountability is a multi-faceted concept. For the purposes of examining Critical Information Infrastructure accountability, the report examines in considerable detail two key aspects of accountability. There is an examination of the common mechanism used to achieve accountability under Canadian law and in Canadian markets. There is also an examination of the accountability mechanisms that are widely used in the established markets for the goods and services that make up the Critical Information Infrastructure.

The common mechanisms used to achieve accountability can be traced back to more fundamental ideas about indemnification and indemnity. The report includes a simplified definition of indemnity as, "An agreement whereby one party agrees to secure another against an anticipated loss or damage." The question becomes one of examining the common methods by which indemnification has been achieved under Canadian law and in Canadian markets. The report focuses specifically on indemnification in relation to software, systems, services, and hardware.

Broadly, three mechanisms are examined – tort law, criminal law, and insurance. Tort law is generally used as a way in which an injured party can obtain compensation from the party causing the injury. The cause of the injury must have been due to negligence. Therein is the source for endless debate and discussion – negligence can have strongly subjective elements. There are still a great many unanswered questions about how tort law might apply to loss in connection with our Critical Information Infrastructure.

Criminal law takes a different approach. Its concern is with acts deemed to be crimes under the *Criminal Code* of Canada. Following this line of reasoning, the report quotes the RCMP's definition of computer crime as, "any illegal act which involves a computer system whether the computer is the object of the crime, an instrument used to commit a crime or a repository of evidence related to a crime." The report examines how this relates to the three most important players – the lawmakers, the enforcers, and the criminals.

Insurance generated strong opinions in our stakeholder interviews. Some stakeholders felt that insurance can play a pivotal role in securing the Critical Information Infrastructure – they were often insurance executives with strongly vested interests. The report considers in some depth how, why, where, when, and whether insurance may be employed to improve the security, availability, and reliability of our Critical Information Infrastructure. Notwithstanding the promise seen by some stakeholders, there are still a number of important open questions.

The report goes on to examine the accountabilities that are commonly found in connection with software, systems, services, and hardware. The starting point is to examine accountabilities for

software products, custom software, and (software) systems. These reference points were chosen to illustrate the range of accountabilities found in the current Canadian marketplace. Much of what can be observed are the means by which vendors have been able to sharply limit the accountabilities they are required to assume.

Some progress has been achieved in appropriately assigning accountabilities in connection with IT services. The ITIL standard provides a widely accepted framework for the delivery and management of IT services. In addition, ITIL has identified means by which accountabilities can be assigned. The tools are available to assign accountabilities, but they are often not used in practice. With hardware, the observed practices sharply limit accountabilities.

CURRENT STATE OF CRITICAL INFORMATION INFRASTRUCTURE ACCOUNTABILITY

All of the stakeholders we interviewed told us that they believed that there would be at least one major failure of the Critical Information Infrastructure within the next five years. Some informed stakeholders went so far as to assert that an Information Infrastructure failure was one of the main causes of the great power blackout of 2003.

The Microsoft monoculture came up in a number of stakeholder interviews – monocultures are fragile and we have a Microsoft desktop monoculture. Microsoft may have 'caused' the desktop monopoly, but it's unclear what, if anything, should be done about it. Several stakeholders pointed to the benefits that can flow from encouraging diversity.

Our stakeholder interviews strongly supported the view that there are strong interdependencies between adjacent jurisdictions, such as between Canada and the U.S. Effective action may need to be internationally coordinated. Canada is not free to act alone, but others may be prepared to see Canada play a leading role.

The absence of professionals, as in fields such as medicine and accounting, was seen by several stakeholders as a serious limitation on what can be done to improve our Critical Information Infrastructure. Prior to accepting any new class of professionals, however, there was broad agreement that we must develop and accept relevant professional practice standards. Encouragement of the development of such standards is worthy of further consideration.

There was surprising agreement in our stakeholder interviews about the role that government ought to play. There was agreement that government should not play the leading role. It could provide funding; it could encourage promising development; but any central role for government was viewed with a high degree of skepticism.

Notwithstanding the reluctance to see government play the leading role, the stakeholders recognized that public funding would be required. In addition, they felt that more attention could be focused on what is needed to maintain, enhance, and sustain the Critical Information Infrastructure. There was also a clear sense that this concern for our Critical Information Infrastructure needs to be broadly recognized across Canada.

After a brief review of the current international difficulties governing the Internet, we were led to the opinion that there is very little acceptance of accountability for any end-to-end public or

shared Information Infrastructure services in Canada. The well-entrenched anti-regulation thinking behind the Internet would need to be to taken into account to establish such accountabilities, should they be determined to be desirable.

BARRIERS TO ACCOUNTABILITY

It's important to understand the practical barriers that may arise should there be a decision to introduce additional accountabilities for Canada's Critical Information Infrastructure. Drawing on the research team's extensive legal and consulting experience, a preliminary list of possible practical barriers is presented. These barriers include:

- Diffusion of responsibility
- Increased costs for goods and services
- Increased costs to enforce laws and regulations
- Reduction in the pace of innovation
- Limitations on Canada's sphere of influence
- Missing standards, both in measurement and practice
- Natural human resistance to change
- Need for a disaster to inspire action
- Difficulty in identifying the Critical Information Infrastructure
- Incomplete understanding of the Critical Information Infrastructure

ACCOUNTABILITY MODEL CHARACTERISTICS

Because the research team felt there may be a future need to consider increased accountabilities for Canada's Critical Information Infrastructure, it was our opinion that an *accountability model* may be required at some point in the future. We drew upon our consulting and management experience to identify the *dimensions* that might be used to build an accountability model and the *mechanisms* that might be used to establish desired levels of accountabilities.

Accountability Dimensions

- Kinds of accountabilities
- Reasons to accept accountability
- Parties accepting accountability
- Enforcement procedures
- Consequences of failure

Accountability Mechanisms

- Public advocacy
- Directed purchasing
- Standards development
- Standards enforcement
- Professional licensing
- Market regulation
- Direct regulation

POTENTIAL APPROACHES FOR IMPROVING THE CRITICAL INFORMATION INFRASTRUCTURE

Our research has highlighted four areas that may merit consideration when exploring how we might improve the reliability, security and functionality of the Critical Information Infrastructure. These suggestions represent the synthesis of the opinions of key stakeholders. They would all require extensive research and consultation before implementation could be contemplated.

Encourage Diversity in the Shared Information Infrastructure

Diversity, properly encouraged, can enhance reliability of Canada's overall Information Infrastructure. There may be significant potential benefits from multiple instances of different, separate, yet functionally equivalent components at each level of the shared Information Infrastructure.

Enforce Accountability for the Shared Information Infrastructure

Greater accountability could be placed on those who build and operate shared services within the Information Infrastructure. Because these services are the result of the cooperative action of many players, most accountability will probably be accountability for process.

Enforce Accountability for the Private Information Infrastructure

Those who operate private services that connect with the shared Information Infrastructure could be held more accountable. Because these services are largely the responsibility of those who operate them, most accountability might be for results. The results might usually be best measured at the interface between the private service and the shared Information Infrastructure.

Encourage Standards Development and Adoption

In general, standards are useful for the implementation of accountability. Standards allow us to measure, certify and interconnect pieces of the Information Infrastructure. International standards may be the most important because of the global nature of the Information Infrastructure, but Canadian standards may also play important roles.

KNOWLEDGE GAPS

If the Critical Information Infrastructure is to continue to evolve and expand in terms of functionality, robustness and security, we should consider the merits of improving overall governance of and accountability for the Critical Information Infrastructure. We would be in a much better position to contemplate such improvement if we filled critical gaps in our knowledge. Selected examples include:

- Identifying the Critical Information Infrastructure
- Identifying the full range of stakeholders and their positions
- Understanding the interactions of information infrastructure components
- Extrapolating the evolution of cyber insurance

Table of Contents

1.0 Objectives

This report takes us one more step down the path of understanding the Critical Information Infrastructure. It is an important path. As Canadians, we are becoming increasingly dependent on the Information Infrastructure for both our safety and the functioning of our society.

We undertook this investigation without any prior bias as to what might be learned, and without any specific agenda to support. Some of the areas that we wanted to examine were:

1. The current state and future evolution of the Information Infrastructure;
2. The concept of accountability as it relates to the Critical Information Infrastructure;
3. Accountability mechanisms currently in place that affect the Critical Information Infrastructure;
4. Relevant accountability lessons from other environments;
5. The current state of accountability for the Canadian Critical Information Infrastructure as perceived by major stakeholders;
6. Major accountability issues; and
7. Suggestions for improving the reliability, security and functionality of the Critical Information Infrastructure.

We recognized early on that there were several key points for us to keep in mind during this project:

1. There is no broadly-accepted precise definition of the Information Infrastructure or the Critical Information Infrastructure, and this report is not intended to provide such definitions. This report adopts the generally-accepted stance that the Information Infrastructure incorporates a broad range of technologies, services, and industry sectors, including computers, networks, software, the Internet, telecommunications, and many others. Sharp distinctions about what does and does not constitute Information Infrastructure are left as the subject of future work and are not intended here.
2. The report may initiate discussion of potential changes to accountability for the Critical Information Infrastructure. This is a contentious subject. Very large amounts of money are at stake, both domestically and internationally.
3. There is a rapidly growing level of concern in many quarters about the effects of any significant failures of the Critical Information Infrastructure. This concern could fuel a growing demand for action.
4. This report can indicate possible ways forward, but it will not be able to present any definitive solutions. Significant amounts of additional investigation and consultation are needed before prudent action can be recommended.
5. The Information Infrastructure is still in its infancy. Legislators, regulators, associations and users have not yet had adequate time to address accountability issues.
6. The Critical Information Infrastructure is a rapidly evolving target. Static ‘solutions’ are obsolete as soon as they are proposed. Solution frameworks are needed that can continuously adapt to the needs of the moment.
7. The Critical Information Infrastructure is a massive subject. Resource limitations required that we restrict the scope of the project.

2.0 Methodology

2.1 How This Report Was Developed

We began with a clear statement of objectives, but without any prior bias as to what might be learned, and without any specific agenda to support. As outlined in the previous section, the objectives were refined in conjunction with Public Safety and Emergency Preparedness Canada (PSEPC) as the report progressed.

To define the scope of the report, we compiled a draft Table of Contents. The Table of Contents was modified and expanded throughout the course of the project to keep it aligned with the objectives. We considered what information would ideally be covered in each section, and how this information could be obtained. This led us to the development of a research plan that we incorporated into the overall project plan.

Once we had a detailed understanding of the scope of the project, we assembled a multidisciplinary team with the range of expertise needed to deliver the project as planned. The responsibility for each section of the report was assigned to the team member with the appropriate expertise. By making these assignments early, each team member was able to direct his/her sections as mini-projects within the scope of the larger effort. A project manager ensured that everyone's efforts stayed coordinated.

We undertook a substantial amount of secondary research. This provided us with a solid base of information, as well as enabling us to discover the key organizations concerned with the Information Infrastructure. The results of this research are summarized in the bibliography section of this report.

A primary research initiative supplemented our secondary research. We identified opinion leaders within various types of key organizations and conducted highly focused interviews to scope the range of thoughts about Critical Information Infrastructure accountability. Public sector representatives were excluded from our interview sample frame in order to focus on the private and not-for-profit sectors. We found that there was a high degree of reluctance to participate in interviews. This reluctance was broad-based, and was not because people were too busy. Accountability is clearly a sensitive topic that many people would rather not discuss. Overall, we requested interviews from 108 people. Twenty-four agreed to participate and were interviewed.

In parallel with our secondary research and interviews, we conducted a series of internal think-tank sessions throughout the project. These sessions generated a body of original thought and helped to keep our efforts focused on the objectives.

Project progress was tracked through weekly status meetings that were documented and distributed to the team. These meetings allowed us to identify emerging challenges early.

Frequent communication with PSEPC, both formal and informal, ensured that we maintained a collaborative approach throughout the project. As initial drafts of report sections were produced, we shared them with PSEPC for comment. This allowed us maximum flexibility to make adjustments as the report took shape. Upon completion of the first draft, a detailed technical edit

was performed by a qualified third party. PSEPC reviewed the draft and provided comments which we then incorporated, as appropriate, into the final report.

2.2 Miscellaneous Points

In consultation with PSEPC, we have elected to use the Canadian Guide to Uniform Legal Citation standard for footnotes throughout this report. All Web pages referenced in the footnotes and the bibliography were active as of 18 March 2004.

All references to laws and organizations can be assumed to be Canadian unless otherwise stated.

3.0 Information Infrastructure Development

3.1 Internet History

The entire history of computing could be included in this report as background leading up to Canada's current Information Infrastructure. It's interesting that the University of Toronto's 1952 UTEC[1] computer provided Canada with one of the first operating computers in North America. It's also interesting that the Canadian Commodore 64,[2] introduced at the 1977 Consumer Electronics Show, preceded the Apple II and Radio Shack TRS80 by several months. It was the first 'real' computer to achieve significant sales through retail channels.

Those are interesting facts about the history of computing in Canada.[3] During much of that history there was nothing that could be called Canada's Information Infrastructure. There were a growing number of Canadian computer networks in the 1970s and 1980s, but it was difficult and expensive to arrange connections between these early networks. The 1994 introduction of the commercial use[4] of the Internet in Canada changed all of that. More and more Canadian networks followed the Internet protocol (IP).[5] Inter-networking became increasingly common – the Canadian Information Infrastructure was born.

3.1.1 Global Internet Developments

There is a large and growing body of literature on the Internet. Searching[6] amazon.ca for books on the subject "Internet" yields 20,795 hits. Fortunately, many of the people responsible for the development of the Internet are still alive and active. "A Brief History of the Internet"[7] is a description of the beginnings of the Internet, as told by the people who made it happen. Very early in the use of computers leading thinkers recognized the potential of large-scale networks of computers.

> The first recorded description of the social interactions that could be enabled through networking was a series of memos written by J.C.R. Licklider of MIT in August 1962 discussing his 'Galactic Network' concept. He envisioned a globally interconnected set of

---

[1]Michael R. Williams, "UTEC and Ferut: The University of Toronto's Computation Centre" *IEEE Annals of the History of Computing* 16:2 (Summer 1994).

[2]Ian Matthews, "The Amazing Commodore PET" *Commodore Business Machines Product Line Up* (22 February 2003), online: Commodore Computers <http://www.commodore.ca/products/pet/commodore_pet.htm>.

[3]The CBC has an archive section titled "Computer Invasion: A History of Automation in Canada." It provides an anecdotal history of computing in Canada. It can be seen online: at <http://archives.cbc.ca/IDD-1-75-710/science_technology/computers/>.

[4]Prior to 1994, the U.S. funding model for the Internet prohibited the use of the network for commercial purposes. Before 1994 the Internet was used exclusively for academic, government (and military) purposes. After 1994, commercial use was allowed.

[5]"Internet Protocol is a standardized method of transporting information across the Internet in packets of data. It is often linked to Transmission Control Protocol, which assembles the packets once they have been delivered to the intended location." See, online: the *Campus Information Technologies and Educational Services - Glossary of Acronyms and Technical Terms* <http://www.cites.uiuc.edu/glossary/#i>.

[6]Search conducted on 27 February 2004.

[7]Vinton G. Cerf *et al.*, "A Brief History of the Internet" *Internet Histories* (10 Dec 2003), online: The Internet Society <http://www.isoc.org/internet/history/brief.shtml>.

> computers through which everyone could quickly access data and programs from any site. In spirit, the concept was very much like the Internet of today.[8]

Back then, the only wide-area network was the one supporting the telephone system. That network relied on switching circuits to establish a continuous connection between two communicating parties. Any larger network using that approach would have to work through a central switching point. Such a central switching point would fast become *the* network bottleneck. An alternative approach was proposed by Leonard Kleinrock in 1961.[9] The alternative used data packets.

The idea now seems obvious. All of the computers would connect to a shared network. Computer A would talk to computer B by sending packets of information down the shared network addressed to B. Only B would read the packets addressed to it. The idea was revolutionary, especially to the engineers responsible for the telephone network. With the help of U.S. Department of Defense (DoD) funding, the initial packet switching ARPANET[10] had grown to include four computers by 1969. The story continues…

> In October 1972 Kahn organized a large, very successful demonstration of the ARPANET at the International Computer Communication Conference (ICCC). This was the first demonstration of this new network technology to the public. It was also in 1972 that the initial 'hot' application, electronic mail, was introduced. In March, Ray Tomlinson at BBN wrote the basic email message send and read software, motivated by the need of the ARPANET developers for an easy coordination mechanism.[11]

Through the 1970s and into the 1980s, most of the computer networks were purpose-built, specifically they were intended for, and largely restricted to, closed communities. This was true for academic as well as commercial communities. But there was an academic desire to have an all-inclusive network of networks. The British JANET network in 1984 and the U.S. NSFNET in 1985 were designed to be inter-networks, with National Science Foundation (NSF) funding requiring that "the connection must be available to ALL qualified users on campus."[12] The seeds were sown for the Internet, as we know it today.

The one critical additional ingredient was freeing the Internet from its dependency on U.S. public money and with it the restriction of Internet use to the non-profit sector of the economy. That shift happened gradually in the early 1990s. By April 1995, U.S. NSF funding was withdrawn from the backbone North American network. Full and unfettered commercial use of the Internet was allowed. The foundation for the North American Information Infrastructure was established.

---

[8] *Ibid.* at <http://www.isoc.org/internet/history/brief.shtml#Origins>.
[9] Leonard Kleinrock, "Information Flow in Large Communication Nets" *RLE Quarterly Progress Report* (July 1961).
[10] "(Advanced Research Projects Agency Network) - The precursor to the Internet. Developed in the late 60's and early 70's by the U.S. Department of Defence as an experiment in wide-area-networking that would survive a nuclear war." See glossary, online: at <http://www.easynet.com/investorinfo/investorinfo_glossary.asp>.
[11] Cerf, *supra* note 7.
[12] *Ibid.*

3.1.2 Canadian Internet Developments

There are significant parallels between the development of inter-networking in Canada and the U.S. We are fortunate in having extensive documentation on this aspect of Canada's recent history.[13] "This historical account of the Canadian Internet is told by the people who worked on the front lines – the believers, the researchers, the innovators, the businessmen and the politicians."[14]

There were a number of early computer networks established by individual Canadian universities and individual Canadian businesses. In 1978, Bell Canada began to offer Datapac,[15] a nation-wide packet switched data network. This was one of the first packet switched networks offered by any telephone company in the world. While Datapac used packet switching, it also followed the established telephone company practice of time- and distance-sensitive pricing. Back then the telephone companies in Canada had complete control of their networks, data as well as voice. They controlled *all* of the devices that directly connected to their networks.

Canadian academics soon recognized the benefits of the 'free' message-passing service used by their U.S. colleagues. By 1979, Canada was connected to Usenet.[16] That Usenet connection provided a back door into the ARPANET community. Our official ARPANET connection had to wait until 1983 when a link was forged to our own DREnet.[17] This early Canadian packet switching network was never planned to be large in scale – its target was to include no more than a dozen computers.[18]

In 1984, OUnet[19] came into being. It expanded the simple connection between the University of Waterloo and the University of Guelph to include the University of Toronto, York University, the University of Western Ontario, Queens University, Humber College, and Ryerson Polytechnic Institute. As this basic network was being established, a new request to connect came in from Lakehead University in Thunder Bay, and from three out of province universities: the University of Manitoba, McGill University, and the University of New Brunswick.

Within a year plans were launched for NetNorth.[20] The major Ontario node in this wider network was to be located at the University of Guelph. It would be through this node that Canada would connect into the U.S. BITNET.[21] York University would be the Toronto anchor, with McGill

---

[13]Canarie, *A Nation Goes Online - Canada's Internet History* (Montreal: CA*net Institute, 2001), online: CANARIE Inc. <http://www.canarie.ca/press/publications/ango.pdf>.
[14]*Ibid.* at 5.
[15]*Ibid*. at 24.
[16]"A world-wide system of discussion groups, with comments passed among hundreds of thousands of machines. Not all USENET machines are on the Internet. USENET is completely decentralised, with over 10,000 discussion areas, called newsgroups." See glossary, online: at <http://www.easynet.com/investorinfo/investorinfo_glossary.asp>.
[17]Canarie, *supra* note 13 at 38.
[18]*Ibid*. at 37.
[19]*Ibid*. at 49.
[20]*Ibid*. at 55.
[21]"(Bulletin Board System) - An academic computer network that provides interactive electronic mail and file transfer services, using a store-and-forward protocol, based on IBM Network Job Entry protocols. Bitnet-II

funding the bridge over to Montreal. The University of New Brunswick would connect through Montreal and would, in turn, provide connections to the University of PEI and Memorial University through a bridge at Dalhousie University in Halifax. By 1989, NetNorth had grown to include 65 nodes.[22]

The connection to BITNET was useful to send messages between researchers in Canada and the U.S. It was not a direct connection to NSFNet,[23] the academic successor to ARPANET. In October 1988, the University of Toronto established a direct connection to NSFNet.[24] Canada and NetNorth were beginning to forge the connection to the U.S. inter-network that would develop into the Internet. This was but a way station on the path to Canada's own CA*net. In June of 1989, the National Research Council was granted approval to issue a Request for Proposal (RFP) for what was to become CA*net.[25] In August 1990, the CA*net Board of Directors received news that the network was up and running with all provincial nodes connected.[26]

The foundation was established. CANARIE (or the Canadian Network for the Advancement of Research, Industry and Education) was proposed in 1992.[27] Phase 1, for 1993, would see CA*net upgraded to a T1 (1.5 Mbps, or millions of bits per second) connection across Canada. The next phase, to be completed by December 1995, would see a further upgrade to T3 (45 Mbps). The final phase was to coincide with the end of the century and see a fully upgraded production network where government would withdraw from the project. The commercial basis for Canada's Information Infrastructure would be established in time for the new century.

3.2 Broad Trends in Development of Technology

The focus of this report specifically concerns the future of Canada's Critical Information Infrastructure. But there are important overlapping areas, which should be considered in order to build a full understanding of our Critical Information Infrastructure. On a broad level, it is helpful to place our Critical Information Infrastructure in the context of technology developments that we can expect to see within the next ten years.

RAND prepared a recent report on *The Global Technology Revolution*,[28] subtitled "Bio/Nano/Materials Trends and Their Synergies with Information Technology." RAND is a

---

encapsulates the Bitnet protocol within IP packets and depends on the Internet to route them." See glossary, online: at <http://www.easynet.com/investorinfo/investorinfo_glossary.asp>.

[22] *Canarie*, *supra* note 13 at 58

[23] "National Science Foundation Network. The National Science Foundation followed on the earlier ARPANet by creating NSFNet in 1986 as a 56 Kbps backbone for the Internet." See, online: *Walt's Internet Glossary - Glossary of Internet Terms* - Letter N <http://www.walthowe.com/glossary/n.html>.

[24] *Canarie*, *supra* note 13 at 68.

[25] *Ibid*. at 92.

[26] *Ibid. at* 101.

[27] *Ibid*. at 110.

[28] Philip S. Anton, Richard Silberglift & James Schneider, *The Global Technology Revolution – Bio/Nano/Materials Trends and Their Synergies with Information Technology by 2015*, A Report Prepared for the National Intelligence Council by RAND National Defence Research Institute, (Santa Monica: RAND, 2001) (approved for public release; distribution unlimited).

U.S. non-profit institution that helps improve policy and decision-making through research and analysis. It's a think-tank, undertaking research for the U.S. military, intelligence, and foreign service communities. The first paragraph in their summary sets the stage in a useful way:

> Life in 2015 will be revolutionized by the growing effect of multidisciplinary technology across all dimensions of life: social, economic, political, and personal. Biotechnology will enable us to identify, understand, manipulate, improve, and control living organisms (including ourselves). The revolution of information availability and utility will continue to profoundly affect the world in all these dimensions. Smart materials, agile manufacturing, and nanotechnology will change the way we produce devices while expanding their capabilities. These technologies may also be joined by 'wild cards' in 2015 if barriers to their development are resolved in time.[29]

The report identifies five key Meta-Trends.[30] These will be fundamental forces shaping developments in technology.

1. **Accelerating pace of technological change** – The pace at which new technologies are developed continues to accelerate. There is a parallel pace at which older technologies are displaced. The resulting 'creative destruction' is not always seen as a positive by those directly involved.
2. **Increasingly multidisciplinary nature of technology** – The boundaries between technologies continue to blur. Specifically relevant to Critical Information Infrastructure is the development of microelectromechnical systems (MEMS[31]). These small sensors will allow everything to be connected to everything using the Information Infrastructure.
3. **Competition for technology development leadership** – RAND recognized that technology development leadership does not automatically rest with any single nation or regional block. Canada's Critical Information Infrastructure will be shaped by developments unleashed through the world.
4. **Continued globalization** – The global Information Infrastructure is enabling and often driving globalization. Our communication and manufacturing technologies allow goods and services to be produced wherever costs are lowest. The process is irreversible, short of major social upheaval.
5. **Latent lateral penetration** – The study projects that technologies will continue to filter down into less developed areas, possibly after modification to make them more attractive locally.

---

[29] *Ibid.* at xi.
[30] *Ibid.* at xvi.
[31] "Micro-Electro-Mechanical Systems (MEMS) is the integration of mechanical elements, sensors, actuators, and electronics on a common silicon substrate through microfabrication technology. While the electronics are fabricated using integrated circuit (IC) process sequences (e.g., CMOS, Bipolar, or BICMOS processes), the micromechanical components are fabricated using compatible "micromachining" processes that selectively etch away parts of the silicon wafer or add new structural layers to form the mechanical and electromechanical devices." See, online: *MEMS and Nanotechnology Clearinghouse*, "What is MEMS Technology?" (February 23, 2004) <http://www.memsnet.org/mems/what-is.html>.

The study offers a number of important conclusions. One summary paragraph offers a clear description of the world we can expect in the future:

> Beyond the agricultural and industrial revolutions of the past, a broad, multidisciplinary *technology revolution* is changing the world. Information technology is already revolutionizing our lives (especially in the developed world) and will continue to be aided by breakthroughs in materials and nanotechnology. Biotechnology will revolutionize living organisms. Materials and nanotechnology will enable the development of new devices with unforeseen capabilities. Not only are these technologies having impact on our lives, but also they are heavily intertwined, making the technology revolution highly multidisciplinary and accelerating progress in each area.[32]

Canada's Information Infrastructure will be one of the keys to our participation in these broad future technological developments. There is an important final note that needs to be added. The RAND study identified three 'Concerns and Tensions'[33] that already exist and may have a growing impact in the years to come.

1. **Class disparities** – The benefits of new technologies will fall unevenly on regions, nations, and classes. Some will be clear 'winners', others will not. There will be inevitable tensions as a result.
2. **Reduced privacy** – The Information Infrastructure will provide the means to make more and more information globally available. New sensor technologies will be used to gather more detailed information. Privacy could suffer.
3. **Cultural threats** – The 'traditional' way of life in many cultures could be threatened by the bright promise of new technologies. Certainly, there are those who may see such change as threatening basic cultural values.[34]

The smooth progression of technological advances could be derailed by these concerns and tensions. In thinking about the future, it would be wise to recognize that there will be inevitable tensions unleashed by the 'creative destruction' which often accompanies the introduction of fundamentally new technologies.

---

[32] *Ibid. at* xvii.
[33] *Ibid.*
[34] At the time of this writing, a Mennonite man from the U.S. is lingering in Canada, temporarily unable to return to his native U.S. because he does not have "picture I.D.". According to the man, he is not permitted by the tenets of his faith from carrying a "graven image".

3.3 Information Infrastructure Technology Development

There are four broad technology components in the Information Infrastructure: Hardware, Software, Networks, and Services. This section provides a thumbnail history and a high-level overview of likely development trends in each of these areas.

3.3.1 Hardware Development

A large part of what has happened with hardware can be explained by pointing to Moore's Law.[35] Gordon Moore is one of the co-founders of the international chip giant Intel. Back in 1965, he predicted that the number of transistors on a chip would double every 12 months. That early prediction was based on very limited experience. With more experience, Moore's Law is now presented as a doubling of transistor density every couple of years. The law has held for nearly 40 years, and is likely to hold for a number of years into the future.[36]

In some sense, the law has become a self-fulfilling prophecy. Everyone expects that transistor density will double every couple years – crudely translated as "twice as much bang for the buck every two years." The microprocessor chip giants, with Intel in the lead, are expected to deliver that kind of ever increasing processing power. Everyone builds their dependent product plans based on Moore's Law. There is massive pressure on the chip vendors to live up to the law. Whatever the complex technical, social, and market forces driving the chip vendors, there is a confident prediction that Moore's Law will continue to hold.[37]

This means that chip performance improves by a factor of 1,000 every 20 years. That has become an incredible engine driving hardware change. It means that the world's most powerful computer in 1964 had become an average desktop computer in 1984 and then was transformed into a smart telephone by 2003. Within 20 years, that much processing power will be available for use in products that cost only pennies – the age of the 'smart' package will have arrived.

In a more immediate way, this can be described as a move towards computer power becoming a commodity. More and more powerful computers will become 'off-the-shelf' products. The progress of Dell Inc. is illustrative of what is happening in this market. The company was founded by Michael Dell in 1983. Its revenue in the last four quarters was US$41.4 billion, and it employs 46,000 team members throughout the world.[38] In the beginning, Dell sold computers

---

[35]Gordon E. Moore, "Cramming more components onto integrated circuits" *Electronics* 38:8 (19 April 1965), online: <ftp://download.intel.com/research/silicon/moorespaper.pdf>.

[36]INTEL maintains an informative Web page on Moore's Law, online: <http://www.intel.com/research/silicon/mooreslaw.htm>.

[37]"To extend Moore's Law, Intel researchers are aggressively identifying and eliminating any barriers that impede the company's ability to fulfill it. By focusing on fundamentals of silicon technology and manufacturing, including improvements and innovations in process and manufacturing technology, transistor structure and materials, and packaging—Intel breakthroughs in the past two years alone have removed barriers to the continuance of Moore's Law for at least another decade—and likely beyond." See "Expanding Moore's Law – The Exponential Opportunity" *Intel Technology Update* (Fall, 2002), online: Intel Corporation <ftp://download.intel.com/labs/eml/download/EML_opportunity.pdf>.

[38]There is extensive information about Dell on its Web site (<http://www.dell.com>). Indeed, the company does much of its business on the Internet. These company facts can be found at Dell Corporation Web Site, online: http://www1.us.dell.com/content/topics/global.aspx/corp/background/en/facts?c=us&l=en&s=corp&~section=000.

direct to the public using the telephone. It has advanced to become the leading world-wide seller of personal computers. In recent years, it has moved from an exclusive focus on personal computers to the sale of servers, storage, and networks to small, medium, large, and very large organizations throughout the world.[39]

'Commodity' computers and associated devices are covering an ever wider range of the hardware used in organizations of all sizes. This trend can be expected to continue. IBM provides another illustrative example of this trend. When Lou Gerstner was called in to take over IBM in 1993, the company was clearly in trouble. His first move was to cut costs, but he soon moved the company to take a network-centric view of computing.[40] His successor, Sam Palmisano, has shifted the focus to 'on demand' computing.[41] The goal is to provide customers with as much computing power as they require, whenever and wherever that power is needed. This will bring commoditization with a vengeance.

3.3.2 Software Development

Software and the languages used to write software (programming languages) have a rich and extensive history. In 1969, Jean Sammet of IBM published a 'definitive' history of programming languages[42]; it listed some 120 widely used languages. By 1990, it was time to publish Milestone and Best Paper compendia that focused on software. Two useful volumes appeared in that year.[43] There have been two constant concerns in the history of software:

- **Productivity** – Moore's Law[44] drove hardware vendors to dramatic performance improvements. There has been a continuing struggle to improve the productivity of those who develop and maintain software.
- **Quality** – Software projects have often failed to meet their targets. A 1997 KPMG study in Canada concluded that 61% of software projects were deemed to have failed. Similar results were obtained elsewhere.[45]

[39]The range of Dell's current offerings can be seen in the description is provides for its offerings aimed at Medium and Large Businesses. See, online: <http://www1.us.dell.com/content/default.aspx?c=us&cs=555&l=en&s=biz>.
[40]Ira Sager, "The View from IBM" *Business Week* (30 October 1995), online: Business Week Archives <http://www.businessweek.com/1995/44/b34481.htm>.
[41]"Sam Palmisano Presentation Transcript" *IBM Business Leadership Forum - San Francisco* (12 November 2003), online: <http://www.ibm.com/ibm/sjp/11-12-2003.shtml>.
[42]Jean E. Sammet, *Programming Languages: History and Fundamentals*, (Englewood Cliffs: Prentice-Hall, 1969).
[43]Paul W. Oman & Ted G. Lewis, eds., *Milestones in Software Evolution* (Los Angeles: IEEE Computer Society Press, 1990); and Tom DeMarco & Timothy Lister, eds., *Software State-of-the-Art: Selected Papers* (New York: Dorset House Publishing, 1990).
[44]See the previous section on Moore's Law.
[45]See "Failure Rate," online: IT Cortex <http://www.it-cortex.com/Stat_Failure_Rate.htm>.

The history of programming largely describes a continuing search for ever more productive ways to deliver quality software. The general purpose programming language path has been described in terms of first, second, third, fourth and fifth-generation languages. A useful collection of definitions of programming terms contains a simple description of the different generations:[46]

1. The first-generation languages (or 1GL) are low-level machine languages. These languages were designed to be optimal for machines; people's needs were rarely considered.
2. The second-generation languages (or 2GL) are also low-level, generally consisting of assembly languages. These languages were designed to put a user-friendly face on machine instructions, but still required one assembler language instruction for each machine instruction.
3. The third-generation languages (or 3GL) are high-level languages such as Fortran, Algol, PL/I, and C. At this point in the evolution, one instruction in a 3GL could result in the execution of many machine instructions. Programmers had the ability to say such things as "take the value from A, add it to the value from B, and place the sum in C."
4. The fourth-generation languages (or 4GL) consist of statements similar to statements in a human language. Fourth-generation languages are commonly used in database programming and scripts.
5. The fifth-generation languages (or 5GL) are programming languages that contain visual tools to help develop and represent programs. These languages lead to a full visual approach to programming.[47]

The ultimate goal is to eliminate the need for programming. Once the desired program has been fully described, automatic translation into operating software should be possible. With the arrival of fifth-generation languages that goal is getting closer. These languages allow the software designer to build programs by connecting a visual representation of off-the-shelf components using a flow or control structure. The diagram then *is* the program. The automatic language translator takes care of everything required to have a complete, operating software system. This technology is not yet widely used, but there are actual 5GL systems available in the marketplace.[48] Continued progress can be expected.

There have been a number of parallel trends in software development. Today, software is recognized as being the most valuable component in many computer systems. In the early days, software was included with the hardware. Prior to June 1969, IBM 'bundled' software and support services into the monthly rental price for its computers. IBM was the dominant supplier of computers. There was very little market for software – the dominant supplier gave away the software that ran on their computers. There was understandable opposition to this practice from

[46]Adopted from "Programming Definitions," online: Computer Hope Web Site <http://www.computerhope.com/jargon/program.htm>.
[47]See Paul Lyon's pages, online: <http://www-ist.massey.ac.nz/~plyons/711_html/VPL%20papers.html>.
[48]"Kinzan Inc. this week will release Kinzan Studio & Server 3.0, a development and deployment environment that lets developers build enterprise applications through an assembly model by simply linking components in a drag-and-drop format." See Darryl K. Taft, "Building Java, .Net Apps Sans Coding" *EWeek-Enterprise News and Reviews* (23 February 2004), online: <http://www.eweek.com/article2/0,4149,1536587,00&.asp>.

IBM's competitors. The U.S. Department of Justice sued IBM. One result was that in June 1969 IBM decided to 'unbundle' its software and services from hardware rental.[49]

The software industry was born. The logic was compelling. If the cost of developing software could be shared across many organizations, the result ought to be software systems that were superior to anything that could be developed in-house. This bright promise fuelled the software industry and gave rise to a continuing stream of new software products and new software vendors. Several things happened to transform the software industry. The personal computer entered the scene, with the first IBM personal computer (PC) offered for sale in 1981.[50] Almost everyone began to use the IBM PC or clone as their personal workstation. There was a veritable explosion of vendors offering software for the new PC. Within two decades, Microsoft had come to dominate the market for software for the PC. One recent study puts the Microsoft Windows operating system at almost a 98% share[51] of the desktop operating system market.

At the same time as Microsoft was winning a dominant position in the desktop software market, the market for enterprise-wide software applications was also undergoing major change. Perhaps the most important change was the degree to which enterprise-wide applications were being planned and installed at the close of the last century. Integration was critical to success in these software-driven undertakings. And integration between the offerings of a single software vendor is almost always easier to achieve than integration between applications from different vendors. This is almost in the nature of a self-evident truth in the marketplace for enterprise-wide applications. The German software vendor SAP[52] is the leader in integrated, enterprise-wide applications. And the Californian database vendor Oracle[53] is the leader in applications built from a shared database.

But the nature of the market for these large software applications is quite different from the desktop software market. On the desktop there is a single dominant vendor. In the enterprise application field, the market follows the more traditional pattern of the leading vendor having twice the market share of the second place vendor, and the second place vendor having twice the market share of the third place vendor, with only a tiny market share for all the remaining vendors. The leading vendors would obviously like to see the enterprise-wide software application market go in the direction of the desktop software market. Recent moves by Oracle to

---

[49]There is an extensive literature on the IBM consent decrees. One overview can be found in the following article: Sara Baase, "IBM: Producer or Predator" *Reason* (April 1974) pp. 4-10, online: <http://www-rohan.sdsu.edu/faculty/giftfire/ibm.html>.

[50]"The IBM PC model 5150 was announced at a press conference in New York on August 12, 1981 and became available for purchase in early Fall 1981. This is the computer that as manufactured by IBM and in clone form became the de facto standard for business use for the remainder of the decade and beyond. The base model retailed for $2880 and included 64 kilobytes of RAM and a single-sided 160K 5.25" floppy drive. Adding a hard drive or increasing the memory could drive the price up considerably. The IBM PC was powered by a 3.77 MHz Intel 8088 processor." See "1981: The IBM Personal Computer is Introduced" *CED in the History of Media Technology*, online: CED Magic Web Site <http://www.cedmagic.com/history/ibm-pc-5150.html>.

[51]See "Microsoft's Windows OS global market share is more than 97% according to OneStat.com" (10 September 2002), online: <http://www.onestat.com/html/aboutus_pressbox10.html>.

[52]See "SAP Info," online: SAP INFO <http://www.sap.info/en/>.

[53]See, online: Oracle Web Site <http://www.oracle.com/>.

take over PeopleSoft[54] are but one highly visible action to strengthen a leading vendor's market position.

There is one additional factor that needs to be considered about software development. There is a growing move towards open-source software. Software developers freely contribute their time and energy towards building software. The resulting software is made freely available for use by whomsoever wishes. The Linux operating system[55] is now the recognized foundation for open-source applications. At least two important drives can be offered to explain the enthusiasm of individuals and organizations for open-source software:

- **Hacker pride** – It's clear that many of the contributors to open source applications are driven by pride in and enthusiasm for their professional accomplishments. The individuals are 'hackers'[56] and proud of it. It doesn't hurt that recognized, well-formed open-source contributions look very good on a resume.
- **Selling services –** A number of open source companies have been founded on giving away the basic software and then selling services aimed at making it easier to use that software. Red Hat[57] is one of the more successful early examples. IBM[58] has positioned itself as offering corporate support for open source.

It is important to add a cautionary note about Linux. SCO[59] has sued IBM, claiming that IBM illegally caused code that belonged to SCO (or its predecessor companies) to be incorporated into Linux.[60] SCO has also sued users of Linux. Should SCO win, Linux would suffer a serious blow. In that case the future of open source would be under a serious cloud.

In the case of hardware, confident predictions can be made about future capabilities. With software, the future is much less clear. We do feel confident, however, in predicting that the software 'crisis' will continue. The online Wikipedia provides the following explanation:[61]

> The notion of a software crisis emerged at the end of the 1960s. An early use of the term is in Edsger Dijkstra's ACM Turing Award Lecture, "The Humble Programmer", given in 1972 and published in the Communications of the ACM. Dijkstra says, "[the major cause of the software crisis is] that the machines have become several orders of magnitude more powerful! To put it quite bluntly: as long as there were no machines, programming was no problem at all; when we had a few weak computers, programming became a mild problem, and now we have gigantic computers, programming has become an equally gigantic problem."

---

[54]See Lisa Vaas, "PeopleSoft, You Will Be Assimilated" *EWeek-Enterprise News and Reviews* (5 February 2004), online: <http://www.eweek.com/article2/0,4149,1517233,00.asp>.
[55]See Ragib Hasan, "History of Linux," online: <https://netfiles.uiuc.edu/rhasan/linux/> for an insider's view of the history of Linux.
[56]See "Hack, Hackers, and Hacking," online: Jesper / Laisen / DK <http://www.laisen.dk/Hack__Hackers__and_H.1233.0.html>.
[57]See, online: Red Hat, Inc. <http://www.redhat.com/>.
[58]See "Linux at IBM," online: IBM Corp. <http://www-1.ibm.com/linux/>.
[59]See, online: The SCO Group <http://www.sco.com>.
[60]See "Linux & Open Source," *EWeek-Enterprise News and Reviews*, online: < http://www.eweek.com/category2/0,4148,1237915,00.asp> for continuing coverage of the conflict in this area.
[61]See "Software Crisis," *Wikipedia, the free encyclopedia*, online: Wikipedia.org <http://en.wikipedia.org/wiki/Software_crisis>.

Even if all of the bright promises of fifth-generation programming languages are realized, we will still face a software 'crisis'. The problem is that successful business software must be built on a successful model for the business that software is to serve. If the author of the software doesn't understand the business problem, it's very unlikely that the resulting program will be successful. Acquiring the necessary domain knowledge[62] will remain labour intensive.

Beyond this 'prediction', we can only raise some questions.

> **Question**: Will Microsoft dominance of the desktop continue?
>
> Microsoft currently owns more than 95% of the desktop software market. Windows is the dominant operating system and Office is the dominant desktop application. Questions have been raised about the implications of this for our Information Infrastructure security.[63] The move towards Linux on the desktop can be viewed as a 'natural' market correction for the 'unnatural' current state of the desktop software market.
>
> **Question**: Will Microsoft desktop dominance be translated into dominance in other areas (e.g. servers, hand-held devices, and/or consumer products)?
>
> There is considerable evidence that Microsoft would like to dominate the market for operating systems in different markets – the company has introduced a number of related operating systems to run on several different platforms. But Microsoft's desktop dominance has not been repeated in other markets… yet. Microsoft has a history of eventually getting its products right.[64] Will the company figure out what is required for these other platforms?
>
> **Question**: Will the knowledge of how to 'engineer' software develop, flourish, and be widely applied?
>
> The term 'software engineering' was invented for NATO Science Committee Conferences held in 1968 and 1969, "the phrase 'software engineering' was deliberately chosen as being provocative, in implying the need for software manufacture to be used on the types of theoretical foundations and practical disciplines that are traditional in the established branches of engineering."[65] Within 30 years that 'provocative' title was being

---

[62]"WITHOUT EXPERT KNOWLEDGE of a particular problem, of course, Deep Computing algorithms can't be formed or a solution to a particular problem attempted. A computer's speed, power, software, or algorithms don't solve the problem by themselves. Without an understanding of the issue, "faster" is just another way to spin your wheels." See IBM Deep Computing Institute, online: IBM Corporation <http://www.research.ibm.com/dci/cat4_domain.shtml>.

[63]Dan Geer *et al*. "Cyber*In*security: The Cost of Monopoly – How the Dominance of Microsoft's Products Poses a Risk to Security"(27 September 2003), online: Computer & Communications Industry Association <http://www.ccianet.org/papers/cyberinsecurity.pdf>.

[64]It has been informally observed that by version 3 of a product, Microsoft figures out how to do it "right". This happened with Windows 3.0, and with Internet Explorer 3.0. Given enough time, Microsoft can often figure out what is required to be successful.

[65]J. M. Buxton, Peter Naur, & Brian Randell, eds., *Software Engineering: Concepts and Techniques*, (New York Petrocelli/Charter, 1976) at 6.

translated into what many called 'real' software engineering.[66] How long will it be before we can confidently expect that software will be engineered?

Question: Will any Canadian software fall within restricted areas of practice?

Canada is unusual in that many traditional areas of engineering fall within what are called restricted areas of practice. Given the way engineering is regulated in most Canadian provinces, it can be argued that a certain kind of software practice should only be performed by those holding an appropriate license. The 2001 Strategic Vision from the Professional Engineers of Ontario raises just this point.[67] If software can be engineered and if licensed engineers know how to do that kind of engineering, a strong argument can be mounted for licensing.[68]

3.3.3 Network Development

In the past, there were multiple network options available for use in Canada. Increasingly, IP (or Internet Protocol) networks are the dominant choice. This is certainly true for networks that are to be exclusively used to transport data. Voice networks have followed a different path, but even that is changing. Voice over Internet Protocol (VoIP) is today an attractive option for larger organizations,[69] and is being planned as an offer to consumers in 2005 by Rogers Communications Inc.[70] Increasingly, networks of all kinds will be following IP. Not all of the Canadian networks will interconnect, but they will be tracking development of IP networks. The Internet is the granddaddy of all IP networks (it's really a network of networks, or an inter-network).

There are a large number of trends that will shape the future of the Internet. In this section we identify some of the key trends. The rate at which changes happen will depend on many factors. Some of the key factors will apply outside Canada – the U.S. will have a massive impact on the future of the Internet as seen by Canadians and Canadian institutions. Many of those influencing

---

[66]The two largest IT professional societies in the U.S., ACM and IEEE-CS studied the question of whether software engineering had advanced to become a real profession. They disagreed, but have continued to work together on developments in the field. See "History of the Joint IEEE Computer Society and ACM Steering Committee for the Establishment of Software Engineering as a Profession," online: IEEE Computer Society <http://www.computer.org/tab/seprof/history.htm>.

[67]Does the engineering profession want "to take a proactive leadership role in additional restricted areas of practice in the area of applied science and technology, or simply wait and react to whatever proposals develop?" In supporting the motion, George Comrie noted that regulation to protect the public interest in such unregulated areas as software development is likely in the future. 'The question,' he said, 'is whether we want to be proactive or reactive. We can try to oppose after the fact or we can get in on the ground floor.' See Connie Mucklestone, "Strategic Plan Vision sparks lively discussion", March 26, 2001 meeting, online: Professional Engineers Ontario <http://www.peo.on.ca/publications/DIMENSIONS/mayjune2001/MJ01InCouncil.pdf>.

[68]There is little unanimity on this question within the software field. Robert Fabian presented the contra argument in *ComputerWorld Canada*, online: <http://www.fabian.ca/profper/pp9.html>.

[69]The organization with which the authors of this report are affiliated – Gowling Lafleur Henderson LLP – has rolled out VoIP technology for communications for use among its offices throughout Canada.

[70]"Ted Rogers, president and chief executive, told a UBS Warburg conference yesterday that the Toronto-based company will start a telephony service using Internet-based technology." See Mark Evans, "Rogers Edges Toward Telephony War v. BCE 'Prudent For Us': Will Start Service Using Internet By 2005, Says CEO" *National Post* (10 December 2003), online: <http://www.vonage.com/corporate/press_news.php?PR=2003_12_10_1>.

factors could interact in unpredictable ways, so while offering a single confident prediction of the Internet's future would be foolhardy, it is possible to sketch a range of possible futures.

3.3.3.1 Speed

There has been a steady increase in network speed. Back in 1968, the key network computers on the precursor of the Internet were interconnected using 50 kbps (thousands of bits per second) links. That was considered fast. Within a few years, individual users were connecting to those computers using 2.8 kbps modems. Ten years ago, a fast home connection used a 56 kbps dial-up modem. Today, a fast home connection uses a 1,000 kbps broadband link. We're moving rapidly to the place where high quality video can come down the connection into the home. There has been a parallel increase in speed in commercial interconnections.

As stated, Moore's Law for semi-conductors says that power doubles every 18 to 24 months. We've seen a steady increase in computing power because there is a steady stream of new chips. A similar trend can be observed in networks, but the jumps are in more discrete steps (e.g. from a 56 kbps dial-up modem to a 1,000 kbps DSL or cable modem). What shows a steady increase is the average connection speed. That average speed has kept pace with Moore's Law, and is likely to continue to keep pace with semi-conductor advances. This thinking would lead to a prediction that within 10 years a fast cell phone connection would be able to support high quality two-way video.

3.3.3.2 Wireless

More and more devices will be using a wireless network connection. Part of the trend can be seen in the growth of cell phone use. Part of it can be seen in your local coffee house, where a wireless Internet connection comes as a free or low-cost extra with your beverage of choice. Part of it can be seen in the new wireless help service that is provided, for a modest monthly fee, to many new car owners. It can also be seen in the design of new wireless offices where computers need to be plugged in to get electricity, but not to achieve a network connection. Wireless is growing rapidly, even in cottage country.

This move towards wireless changes the roles that can be discharged through a network connection. It will soon be common to locate things, and people, through their connection to the network. A raft of new questions is raised by this move towards wireless. Will people be allowed to have anonymous Internet connections, and specifically, wireless connections that cannot be used to locate them? And there are important issues around how service preference can be given in the public broadcast signals used by wireless devices – should a lonely teen's call to a friend be able to block the signal from an ambulance?

3.3.3.3 Connected Devices

Today, retailer Wal-Mart is experimenting with cartons that come with short-range radio frequency devices. Each carton in the warehouse can be located by its short-range wireless connection. The cost is low enough to do this with thousands of cartons a week, but still far too high for it to be universal. But wait for Moore's Law to kick in. Within a few years, the cost of this short-range connection will be only pennies. A few years after that, a full connection to the global network will fall down to the pennies range. At that point, it would be realistic to give 'everything' of importance a network connection.

3.3.3.4 Single Network

Currently, there are often separate networks used for voice, cable, data and Internet access. But services like voice over the Internet (VoIP) are growing rapidly. And more and more data connections are being made 'virtually' using the global Internet (with Virtual Private Network connections). Significantly, this is becoming an almost pure economic question. Carving out a virtual information 'pipe' between any two points on the Internet is steadily going down in price, and up in features. In the next 10 years, more and more of the separate networks will go sub-critical; they will shrink to the place where they can no longer provide competitive network services. As that happens, the global Internet will take on a more and more dominant role. It will be less and less practical to use alternative networks. The implications for how Critical Information Infrastructure services are maintained could be severe.

3.3.3.5 Spam

Today there is a growing problem with spam – unsolicited bulk email. It has been estimated that over half of the current email traffic on the global Internet is spam. For those with 'popular' email addresses, it's common to find that 90% of incoming email, or more, is spam. The economic forces are overpoweringly in favour of spam. It costs pennies to send hundreds of thousands of spam email messages. With a take-up rate as low as 0.001% it still makes very good economic sense to send spam. In our opinion, this can't be allowed to continue.[71] Something will have to be done, and many of the remedies will have serious implications for how Canada's Critical Information Infrastructure will be provisioned.

3.3.3.6 Protocols

The first pre-Internet research network was designed to accommodate up to 256 separate computer networks. Back then, no one expected there would ever be a need to connect millions and millions of computers. Very soon, however, the limit had to be increased. The current Internet Protocol (IPv4) was designed to allow four billion separate devices to have their own Internet addresses. That may seem like a large number of addresses, but various technical considerations sharply limit how many 'free' addresses are available for use by new devices that want to connect to the Internet. There was a serious concern that the Internet would run out of addresses for all of the devices that wanted to connect.

There has been a proposal on the table for a number of years to replace the current Internet Protocol (IPv4) with a new and improved version (IPv6). The new Internet Protocol (version 6)[72] would dramatically increase the number of available Internet addresses. But the conversion from version 4 to version 6 would be expensive and painful. A number of technical workarounds have been developed. Many of them were designed to allow multiple devices behind a network

---

[71] See Garrett Hardin, "The Tragedy of the Commons" *Science* 162 (1968): 1243-1248, online: <http://www.dieoff.com/page95.htm>.

[72] "This set of Web pages provides information of Internet Protocol Version 6 (IPv6). IPv6 is sometimes also called the Next Generation Internet Protocol or IPng. IPv6 was recommended by the IPng Area Directors of the Internet Engineering Task Force at the Toronto IETF meeting on 25 July 1994 in RFC 1752, *The Recommendation for the IP Next Generation Protocol*. The recommendation was approved by the Internet Engineering Steering Group and made a Proposed Standard on November 17, 1993." See online: Sun Microsystems, Inc. – Internet Engineering group of Solaris Software <http://playground.sun.com/pub/ipng/html/ipng-main.html>.

connection point (called a router) to share one address. We have been 'out of' new Internet addresses for several years, but the workarounds allow the Internet to continue to grow.

The primary motivation behind IPv6 was to increase the address space, but it would also provide some important additional benefits. Specifically in connection with Canada's Critical Information Infrastructure, the new IPv6 would allow priorities to be attached to message packets. The 'important' packets would be given more of the available network resources. Critical messages could make their way through the network, even if it was otherwise 'crowded' with unimportant traffic. Will IPv6 become the norm? Should Canada move to install IPv6, or a similar enhanced protocol, on key elements of its national Information Infrastructure?

3.3.4 IT Services Development

Since the very earliest days of the field, organizations have seen value in the use of computing. It's not surprising that this need would have inspired vendors to develop and offer *IT services* to the market. These services were based on what the vendor hoped would be an attractive and profitable combination of hardware, software, and connectivity (networks). In the 1950s and 1960s, it was common to find 'vendors' offering to rent time on their computers. Many university computer centres found this an attractive way to supplement their income.

By the 1970s there was a thriving computer service bureau business in Canada. This was back when mainframe computers were very expensive to purchase and operate. Economies of scale could be realized. Companies pooled their computing needs in order to be able to jointly purchase the largest mainframe computers. Several Canadian universities followed a similar approach. For a period, there were real savings to be achieved by shared use of the largest possible mainframe computers.

In the 1980s and into the 1990s, the IT services business shifted again. With the onset of personal computers and the growth in the power of minicomputers, the benefits of economies of scale for mainframe computers were reduced. Service bureaus shifted their focus to offer more specialized services. In 1985, the University of Toronto entered the supercomputer business, offering cycles on its Cray supercomputer.[73] A number of firms started to offer payroll processing services.[74] The market for general-purpose mainframe processing cycles continued to shrink. The IT service providers which remained focused on specialized services.

As we begin the 21st century, the market for IT services is shifting again. A growing range of IT services are being offered through the Internet or through more specialized communication facilities. Customer Relationship Management (CRM)[75] is currently a popular application. A wide range of software systems is available for a company to install on their own computers. There is also a growing market for CRM services provided through the Internet.[76] What's new is that these online services get woven into the fabric of the client organization – anyone who 'touches' a customer will use the online (remote) CRM service.

---

[73]See, online: University of Toronto Press <http://www.utppublishing.com/uoft_history/notes/notes_chapter39.pdf>.
[74]See, online: ADP Canada <http://www.adp.ca/en/index.html> for a current Canadian market leader.
[75]For general background information about CRM, see online: Customer Relationship Management Research Center <http://www.cio.com/research/crm>.
[76]Salesforce.com, online:<http://www.salesforce.com/> is one of the leaders in this field.

We are also seeing a dramatic growth in outsourcing.[77] In fact, outsourcing can take many forms. Of particular interest to the overall subject of this report is the trend to offshore outsourcing where the IT work is shipped to lower cost (or higher quality) foreign suppliers. One recent prediction is that this form of IT outsourcing will rise from $16 billion in 2004 to $46 billion in 2007 in the U.S.[78] Similar changes can be expected to occur in Canada, though we may enjoy the benefit of our lower dollar and be the destination of some U.S. IT outsourcing.

Organizations have always purchased some of the services they need in order to operate. What's new is that we are seeing an increasing real-time dependency on service providers that are outside of the organization. This trend looks as if it will continue. Questions of accountability and responsibility have barely begun to be addressed.

3.4 Projected Information Infrastructure Timeline

There have been a number of studies[79] undertaken which project the future for the Information Infrastructure in North America, Europe, and elsewhere. A report[80] prepared for the (U.S.) Institute for Information Infrastructure Protection[81] includes a useful timeline. It presents an Information Infrastructure projection, with predictions for 2006, 2010, and 2020. While this reported was prepared specifically for the U.S., most of its projections have significant applicability for Canada's Information Infrastructure. The remainder of this section includes our edited version of that timeline projection.

3.4.1 Near-Term (2006) Information Infrastructure Projected Characteristics

- The diverse components in the IT infrastructure (hand-held devices, laptop computer, desktop computers, mainframes, servers, and legacy applications) will continue to be challenging to integrate and will continue to have stability problems.
- Embedded sensors and microprocessors will begin to perform a wide variety of functions, specifically in process control. Smart cards will begin to be used.
- Enterprise specific networks will have boundaries that are increasingly ill-defined. Some of this will be due to the use of devices that can be anywhere (e.g. wireless communications, mobile computing, and mobile agent technologies). Some will be due to the dynamic collaborations between organizations
- Individuals will use increasing amounts of information technology. This will include use of personal digital assistants (PDAs) and position-based content delivery (via GPS

[77] See, online: <http://www.outsourcing.com/> for general information about outsourcing.
[78] See, online: CIO Web Site - Metrics <http://www2.cio.com/metrics/2004/metric667.html>.
[79] Anton, Silberglitt, & Schneider, *supra* note 28; Robert H. Anderson *et al*., *The Global Course of the Information Revolution: Technological Trends: Proceedings of an International Conference*, (Santa Monica: RAND, 2001); *Technology Timeline*, BTexact Technologies (a division of British Telecommunications) (November 2001), online: <http://www.btexact.com/docimages/42270/42270.pdf>.
[80] *National Information Infrastructure Protection Research and Development Agenda Initiative Report*, Institute for Information Infrastructure Protection, (9 September 2002), online: <http://www.thei3p.org/documents/analyses/I3P_Roadmap_Analysis_V1.0s.pdf> [*Initiative Report*].
[81] See, online: <http://www.thei3p.org/index.php>.

devices and cell-phones). There will also be increased use of digital media convergence, blending voice, data, still images, and video.

- The basic telecommunications infrastructure will continue to be wired and will increasingly be IP-based. Wireless adoption will increase significantly, with long-haul (satellite communications), local (Bluetooth and WiFi), and cellular (2.5G and 3G).

3.4.2 Mid-Term (2010) Information Infrastructure Projected Characteristics

- Embedded sensor use will be common for personal applications, often being transparent to users (e.g. personal wearable health status monitors included as an integral part of 'support' garments).
- Business will increasingly depend on location-finding technology (GPS or other) to track the physical entities of importance to the organization.
- The boundaries between networks, devices, and formats (voice, data, video, control, etc.) will blur, with reduced distinctions between providers, and between providers and users. Traditional regulatory controls will be less and less effective.
- Collaboration through the Information Infrastructure will become increasingly common and be built into the way social groups, work teams, and organizations operate. Connections will be dynamic, linking anyone and anywhere into communities.
- Network capabilities will be extended significantly. Wireless data flow rates will compare to today's desktop data flow rates (5+ Mbps). Video streaming and Voice over IP will be common. There will be real progress towards IPv6.

3.4.3 Long-Term (2020) Information Infrastructure Projected Characteristics

- In developed societies, almost anything and everything of importance will be able to be connected to the network. The distinction between important physical objects and cyber entities will begin to blur.
- Wireless technology will cover most of North America and will provide reliable terabit throughput for corporate use and full video capabilities for individual use.
- Nanotechnology will be commercially available and beginning to be used widely.
- Moore's Law will continue to hold, perhaps through the use of quantum computing, giving hand-held devices super-computing capabilities.

The report from which these projections have been developed[82] also includes projections for Information Security Characteristics in 2006, 2010, and 2020. Those security projections[83] are outside the scope of this section, but may be useful when considering different accountability models.

[82] *Initiative Report*, *supra* note 81.

[83] *Ibid*. page 46. This document projects that "there will be a mature body of information security law based on legislation and court cases" and "information security concerns will be a normal consideration …, just as are physical security concerns today". These security projections may be faulted for being too optimistic.

3.5 Critical Information Infrastructure Development

There has been a broad and pervasive trend in Canadian organizations to replace the traditional 'men, money, and material' with better information. The whole 'just in time' or 'lean manufacturing' movement can be viewed as doing nothing more than replacing the buffer stocks that formerly characterized manufacturing with better information. The obvious motivation is that the information costs less than the 'men, money, and material' that is being replaced.

The implications of this trend for Canada's Critical Information Infrastructure will be significant. Canada has already identified its Critical Infrastructure Sectors.[84] Aside from the Communications sector that includes the Information Infrastructure, there are 9 other Critical Sectors. In the case of all of these sectors, information has been used to replace 'men, money, and material'. The 10 sectors are outlined in Table 3.1.

Table 3.1 Canada's Critical Infrastructures

Sector	Sample Target Sub-Sectors
1. Energy and Utilities	Electrical power (generation, transmission, nuclear) Natural gas Oil production and transmission systems
2. Communications	Telecommunications (telephone, cable satellites) Broadcasting systems Networks (Internet)
3. Finance	Banking Securities Investment
4. Health Care	Hospitals Health-care facilities Blood-supply facilities Laboratories Pharmaceuticals
5. Food	Food safety Agriculture and food industry Food distribution
6. Water	Drinking water Wastewater management
7. Transportation	Air Rail Marine Surface

[84]Office of Critical Infrastructure Protection and Emergency Preparedness, *An Assessment of Canada's National Critical Infrastructure Sectors*, (July 2003), online: Public Safety and Emergency Preparedness Canada <http://www.psepc-sppcc.gc.ca>.

Sector	Sample Target Sub-Sectors
8. Safety	Chemical, biological, radiological, and nuclear safety Hazardous materials Search and rescue Emergency services (police, fire, ambulance and others) Dams
9. Government	Government facilities Government services (for example meteorological services) Government information networks Government assets Key national symbols (cultural institutions and national sites and monuments)
10. Manufacturing	Chemical industry Defence industrial base

Canada's Information Infrastructure plays a critical role in the continued smooth operation of all of these sectors. The impact of a failure in our Information Infrastructure would vary. Key national symbols could continue to be open and available to the public, but online screening of visitors to identify possible security threats would be eliminated, as would online processing for entrance fees. In the case of our electric power grid, Canada's Information Infrastructure is key to our ability to balance load across different sub-nets and generation sources. Rapid failure would be likely were our Information Infrastructure to fail.

Today, many of the Critical Infrastructure Sectors could continue limited operation even in the face of major failure in our Information Infrastructure. As technology advances, possible continued operations in the face of Information Infrastructure failures will become more and more limited. Our Information Infrastructure is fast becoming *the* critical enabler for the continued operation of all other Critical Infrastructure Sectors.

4.0 Introduction to Accountability

4.1 What is Accountability?

While this section of this report may seem somewhat legally technical, its importance will be become apparent in later sections.

In order to discuss the role accountability does or could play in the Critical Information Infrastructure, it is useful to understand more fully what is meant by accountability.

In the plain dictionary sense, "accountability" refers to being responsible for one's actions.[85] In turn "responsible" means being "liable to be called to account (to a person or thing).[86] From this, it can be inferred that any definition of 'accountability' must specify, at least, who is to be accountable to whom and for what.

The traditional approach argues that at least the following issues or elements should be addressed in subsequent analyses. Given the rate of change of the Information Infrastructure, there may also be additional dynamic elements, which need to be considered.

4.1.1 Accountable for What

It is our opinion that accountability works better when there are clear, unambiguous definitions of the obligations assumed by, or imposed upon, participants in the Critical Information Infrastructure for which a person or organization will be held accountable. Such obligations could be established by the usual sources, including some combination of contracts, tort law, and statutory duties. For example, in order to justify assigning liability to those participants who are service providers for their acts or omissions, such obligations should include clearly defined descriptions of the services to be delivered, and the levels at which those services must be delivered.

4.1.2 Who is Accountable

The principles used to assign liability to players in a network, such as the Internet, have been the subject of earlier discussion[87]. In citing the Varian-Anderson principle,[88] [89] Yahalom notes that liability should be assigned in a manner that ensures that "those who are best positioned to control the risks have appropriate incentives to do so", and in citing Anderson[90] notes that "where the party who is in a position to protect a system is not the party who would suffer the results of security failures, then problems may be expected."

---

[85]The Oxford Encyclopaedic English Dictionary, 2d ed., *s.v.* "accountability".
[86]*Ibid.*
[87]Raphael Yahalom, "Liability Transfers in Network Exchanges," a paper published for the Workshop on Economics and Information Security held at the University of California, Berkeley on 16–17 May 2002, online: UC Berkeley, <http://www.sims.berkeley.edu/resources/affiliates/workshops>.
[88]Ross Anderson, "Why Information Security is Hard – An Economic Perspective", (Proceedings of the 17th Computer Security Applications Conference, New Orleans, Louisiana, Dec. 2001), online: Annual Computer Security Applications Conference <http://www.acsac.org/2001/papers/110.pdf>.
[89]Hal R. Varian, "Managing On-Line Security Risks", Economic Science Column, *The New York Times*, (1 June 2000), online: The New York Times, <http://www.nytimes.com/library/financial/ columns/060100econscene.html>.
[90]Anderson, *supra* note 88.

Yahalom[91] argues that these principles can be extended to assign liability to parties who are well positioned, and have incentives, to maliciously perpetrate certain risk events.

In some cases, the allocation of liability among parties will be assumed by mutual agreement pursuant to a contract. In other cases, the allocation of liability could be imposed upon the parties in connection with duties set out in tort law or statute.

4.1.3 Accountable to Whom and Enforcement

When problems arise in the operation of the Critical Information Infrastructure because of failure by one or more participants to discharge their obligations, the source of the obligation will determine the potential plaintiffs. That is, both private and public parties could seek remedies for harm or losses suffered based on actions arising from breaches of contracts, or breaches of tortious or statutory duties.

4.1.4 Ability to Measure

In order to be able to assign accountability among parties in connection with problems that arise in the operation of the Critical Information Infrastructure, it is necessary to be able to monitor and measure, to an appropriate degree of precision, the acts or omissions of all relevant parties.

However, the structural complexity and interdependency of operation among the elements that comprise the Critical Information Infrastructure makes performing these tasks a non-trivial exercise. Similarly, adjudications of causality, remoteness, and other traditional means to assign, measure and assess damages, are also hampered by this complexity and interdependence.

4.1.5 Consequences of Breach

Along with the obligations themselves, there would also need to be a clear understanding of the consequences of the failure to discharge these obligations, including the remedies available to those who suffered the harm or losses brought about by such failure.

4.2 Need for Understanding of the Structure and Dynamics of the Critical Information Infrastructure

The goal of this paper is to assist in the efforts to understand the role that accountability does, can, and could play in the development and operation of the Critical Information Infrastructure. In order to do this, it is important to understand the overall accountability framework within which the Critical Information Infrastructure developed and operates, today and likely into the future. This would include an understanding of the public elements in Canada and internationally (e.g. the applicable laws, regulations, policies, and enforcement mechanisms), and private sector elements in Canada and internationally (e.g. the structure and dynamics of the markets for the goods and services that are produced for, and consumed by, participants in the Critical Information Infrastructure).

[91] Yahalom, *supra* note 87.

Without a solid understanding of the overall Critical Information Infrastructure and the dynamics of its development, decisions that are made in both the private sector and the public sector may not have the intended effects. Worse still, the effects of well-intentioned public and private sector acts may lead to undesirable outcomes. Extensive research is required to build that requisite solid understanding.

The following are some of the questions to be asked in order to gain a better understanding of the entire Critical Information Infrastructure, and the role of accountability within it:

1. How does the level, or allocation of accountability among participants in the Critical Information Infrastructure affect the development and operation of the Critical Information Infrastructure?
2. In what ways has accountability contributed to a desirable, or undesirable, state of the Critical Information Infrastructure?
3. What attributes are best used to describe the current and future Critical Information Infrastructure, and what are the corresponding metrics?
4. What current research is available about each such attribute; and what else should be known?
5. How and in what way is the desired future state of the Critical Information Infrastructure related to each such attribute?
6. What are the inter-relationships among the various relevant attributes of the Critical Information Infrastructure, and what are the trade-offs among them?
7. What are the inter-relationships, including trade-offs, between various attributes of the Critical Information Infrastructure and the policies that govern it?

5.0 Critical Information Infrastructure Accountability Objectives

Section 4 of this report provides a brief introduction to accountability. In this section we explore how accountability can be applied to the Critical Information Infrastructure. We think that the best starting point in this exercise is to consider our objectives. Clear objectives, established at the outset, provide a touchstone to help us to stay on track, and a basis for course corrections.

5.1 Objectives Are Perspective Dependent

Different stakeholders in the Critical Information Infrastructure have different objectives. There is broad agreement that we are becoming more dependent on the Critical Information Infrastructure, and that we must pay attention to ensuring that it continues to function. Beyond this point however, there seems to be little agreement on what, if anything, needs to be done.

It is best to start the exercise of objective identification from a baseline. First and foremost, it seems to us that Canadian society wishes to continue to function. It is our opinion that, in general, as a nation we also want to prosper and grow. At the same time, it is of paramount importance that we ensure the safety of all its members.

To meet these objectives, critical infrastructures (identified in Table 3.1) need to deliver reliable and expanding functionality. As stated in Section 3.5, these critical infrastructures rely ever more heavily on the Critical Information Infrastructure. Thus society requires that the Critical Information Infrastructure continue to deliver needed support to the other critical infrastructures. So far so good. But next comes the first tough question: How do we best ensure that the Critical Information Infrastructure delivers as desired?

5.2 Diversity and Accountability: The Two Leverage Points

In the course of our research, many key stakeholders mentioned two areas that they believed we can leverage to help us to ensure a robust and functional Critical Information Infrastructure: diversity and accountability. Many thought that in a perfect world, we would have a Critical Information Infrastructure that was composed of a number of diverse, but functionally equivalent components at each level. This was often coupled with the desire that we would have clear and meaningful accountability for all aspects. This would give us two separate failsafe mechanisms. In the real world, there are difficulties in achieving diversity and high levels of accountability. Not only that, but diversity and accountability are not easily separated; they interact with each other. In our opinion, we need to strive for the best reasonable situation in each of these areas.

5.2.1 Diversity

Canadians are no strangers to diversity. In fact, our country is built on diversity. We understand the challenges and the benefits better than any other country in the world. At a deep level we realize that social organizations are more robust when they have a high degree of internal diversity. This is because they can leverage this diversity to respond to any external threats.

Viewed from one perspective, the Critical Information Infrastructure is a collection of parties that communicate and work together for a joint purpose. Thus there are strong parallels between the Critical Information Infrastructure and a social organization. A Critical Information

Infrastructure that is composed of a diversity of components at each level has at least some level of redundancy. For example, consider the case where there are two separate backbone networks, and the key components of the Critical Information Infrastructure are connected to both. If one backbone fails, the other will absorb some of its traffic.

The idea of using diversity to build a reliable network informed the early network thinking that led to the Internet. Specifically Paul Baran's seminal paper of 1964 expressed this idea.[92]

Section 5.3 outlines how diversity interacts with accountability. Section 5.5 discusses ways in which the government can encourage diversity in the Critical Information Infrastructure.

5.2.2 Accountability: Process or Results

5.2.2.1 Accountability for Results

Many of our ideas about accountability originated at a time when things were simpler. You could only purchase your telephone service (local, long distance, and equipment) from one supplier. The same was true for your electricity. Computers, to the extent that they existed, were connected only to terminals in a single building. Under these scenarios, little thought was given to accountability, and indeed, it did not merit much thought. If your telephone service or electricity failed, it was very clear who was accountable. Levels of complexity, especially in information technology, have increased by orders of magnitude. Accountability models have not kept pace.

Accountability for the Critical Information Infrastructure can appear deceptively simple on first examination. The Critical Information Infrastructure is, by its nature, critical; it must function. Therefore, the thinking goes, if we hold the operators of the Critical Information Infrastructure accountable for making it function, we will have gone a long way to ensuring that it does function. Unfortunately here, as in many other situations, 'the devil is in the details'.

When we consider accountability this way, we are considering it in the traditional sense, as described above in connection with telephone service and electricity. This is holding people or organizations accountable for results. Aside from safety concerns, we were not overly concerned how the results were achieved. This made sense. The accountability/authority principle was maintained. (Simply put, this principle says that it is not reasonable to hold someone accountable for something unless they have authority over that thing.) Unfortunately, this type of accountability has limited applicability in the Critical Information Infrastructure.

It is important to realize that the Critical Information Infrastructure is not a thing. It is rather a partially defined group of devices, links, data, services and organizations that we have somewhat subjectively collected together into a single basket. There are many interdependencies. Critical services provided by the Information Infrastructure typically are dependent on a number of suppliers working in consort. There are both direct and indirect dependencies. Under these conditions, it rapidly becomes practically impossible to hold people accountable for delivering any sort of high-level functionality. There are too many things that they do not control.

---

[92]Paul Baran, "On Distributed Communications" The Rand Corporation (August 1964), online: Rand Corporation <http://www.rand.org/publications/RM/RM3420/index.html>.

Accountability for results does make sense at finer levels of granularity in the Critical Information Infrastructure. 'Results' can include not just the delivered functionality, but also other things, such as level of security. Standards can be developed. ISO 17799, discussed in Section 9.4.4, provides a good example.

5.2.2.2 Accountability for Process

Fortunately, there is an alternative type of accountability, and that is accountability for process. The professional disciplines provide us with excellent examples. Auditors are not accountable for the accuracy of a company's audited financial statements. They are accountable for conducting an audit according to generally accepted auditing standards, and rendering an opinion, based on their audit, about the accuracy of the statements.

In our opinion, process accountability may be highly applicable to the Critical Information Infrastructure. Proper practices around architecture and methodology allow us to build reliable systems from unreliable components. Process accountability can allow us to define how key nodes and links in the Critical Information Infrastructure are tested and certified. Finally, it can help specify code of conduct, levels of knowledge and areas of practice for the professionals working within the Critical Information Infrastructure.

5.3 The Interaction Between Diversity and Accountability

At the beginning of this section we pointed out that diversity and accountability are not easily separated. In fact, accountability can sometimes offer an alternative to diversity. For example, there are occasions where we, as a society, choose a regulated monopoly in preference to a competitive diversity. In this sense, there is a balance to be struck. There may not need to be high levels of accountability if there is sufficient diversity. There is, however, a potentially much more important interaction between accountability and diversity.

Accountability can work together with diversity to create a more robust Critical Information Infrastructure. By way of explanation, let's continue with our example from Section 5.2.1 where we had two independent backbone networks, with individual Critical Information Infrastructure components connected to both. Some critical traffic is carried over each backbone. IPv6, which was discussed in section 3.3.3.6, provides the ability to specify the quality of service for a packet in the header. If we define the individual Critical Information Infrastructure components, we can use IPv6 to give all traffic from and to these components the highest priority. Then, in the case of a failure of one of the backbones, all critical traffic from the failed backbone will claim priority on the operating one. The result is likely to be almost no interruption of the Critical Information Infrastructure; in other words, almost complete redundancy, without the usual requirement for idle capacity. This is an adaptation of a concept that has been proposed to govern the interaction between narrow band and ultra wide-band communications.[93]

[93]Kevin D. Werbach, "Supercommons: Toward a Unified Theory of Wireless Communication," online: Social Science Research Network Electronic Library <http://papers.ssrn.com/sol3/delivery.cfm/delivery.cfm/SSRN_ID456020_code031013670.pdf?abstractid=456020>.

5.4 Balances and Tradeoffs

In the real world, tradeoffs are inevitable. Success translates into achieving the right balance. Some important tradeoffs that impact on the Critical Information Infrastructure are:

- Cost vs. availability
- Cost vs. functionality
- Domestic concerns vs. international pressures
- Vendor agendas vs. user agendas
- Comprehensiveness vs. practicality
- Implementation time vs. useful life

6.0 Key Stakeholders

This section identifies the key stakeholder groups and discusses their functions within the Information Infrastructure.

6.1 Government

Public sector agencies have a major impact on shaping the Information Infrastructure. They also exert significant influence on accountability. The following subsections outline public sector groups that directly exert these influences. Government as a major user of the Critical Information Infrastructure is covered in section 6.3.

6.1.1 Regulators/Legislators

This group comprises government establishments primarily engaged in the administration, regulation, licensing and inspection of the Critical Information Infrastructure, as well as those who originate policy and legislation.

Examples of these stakeholders are the following federal departments, as well as any provincial or municipal counterparts:

- Parliament
- Department of Justice
- Privy Council Office
- Treasury Board
- Canadian Radio-television and Telecommunications Commission (CRTC)
- Standards Council of Canada

6.1.2 Safety and Security

This group is directly concerned with the security and integrity of the Critical Information Infrastructure. Examples of these stakeholders are the following federal departments, as well as any provincial or municipal counterparts:

- Public Safety and Emergency Preparedness Canada (PSEPC)
- Department of National Defence (DND)
- Communications Security Establishment (CSE)
- Industry Canada

6.1.3 Program Providers

One way that government influences the Information Infrastructure is through direct and indirect economic stimulation. Examples of these stakeholders are the following federal departments, as well as any provincial or municipal counterparts:

- Industry Canada
- Infrastructure Canada

6.2 Associations

Associations are important stakeholders in Canada's Critical Information Infrastructure because they often serve as aggregators for the opinions and concerns of their members.

6.2.1 Professional

The membership of professional associations comprises people who work within the other key stakeholder groups. The purpose of these associations is to advance the professions they represent, and to promote the professional interests of their members. These associations are classified under the NAICS code - 813920 Professional Organizations. NAICS is discussed in Section 6.4.1 below. Examples of Canadian professional associations include:

- Canadian Information Processing Society (CIPS) www.cips.ca
- Association of Internet Marketing and Sales (AIMS) www.aimscanada.com

6.2.2 Standards

Standards that are relevant to the Canadian Critical Information Infrastructure are established by both national and international organizations. Examples include:

- Institute of Electrical and Electronics Engineers (IEEE) www.ieee.org
- Canadian Internet Registration Authority (CIRA) www.cira.ca
- Internet Corporation For Assigned Names and Numbers (ICANN) www.icann.org
- Canadian Standards Association (CSA) www.csa.ca

6.2.3 Vendor

There are a number of associations representing the suppliers of products and services that make up the Critical Information Infrastructure in Canada. These include such organizations as:

- Information Technology Association of Canada (ITAC) www.itac.ca.
- Canadian Wireless Telecommunications Association (CWTA) www.cwta.ca

These associations are classified under the North American Industry Classification System (NAICS) code 813910 – Business Associations. NAICS is discussed in section 6.4.1. In addition to promoting the business interests of their members, these associations may "conduct research on new products and services, publish newsletters, develop market statistics, or sponsor quality and certification standards".[94]

[94]Statistics Canada, *North American Industry Classification (NAICS) 2002*, online: Statistics Canada, <http://stds.statcan.ca/english/naics/2002/naics02-class-search.asp?criteria=813910>.

6.3 Users

Canada's Critical Information Infrastructure is defined as the Information Infrastructure that supports the 10 critical infrastructures defined by PSEPC.[95] These were summarized in Table 3.1.

The users who are major stakeholders in the Critical Information Infrastructure are the organizations that comprise these critical sectors. In most cases, these organizations could be well represented by their Chief Information Officers (CIOs) with respect to their dependencies on the Critical Information Infrastructure.

6.4 Vendors

6.4.1 Overview

A large community of vendors supply and/or operate components of the Information Infrastructure. These vendors can be divided up into four groups based on economic activity: software, hardware, networking and services. Although many companies span categories, this is still a very useful segmentation because each category has distinct and recognizable concerns, products, and accountability mechanisms. Also, because most products are sold 'unbundled', companies that do span categories usually have distinct internal divisions to deal with individual categories.

In order to be more precise about which organizations are included in each of the four categories, we have elected to map the categories into the North American Industry Classification System (NAICS). This is a standard classification system that has superseded the 1980 Standard Industrial Classification (SIC) previously used. NAICS[96] was jointly developed by Statistics Canada, the Economic Classification Policy Committee (ECPC) of the United States, and Mexico's Instituto Nacional de Estadística, Geografía e Informática (INEGI). NAICS mappings could prove useful if sample frames are required for future research.

[95] *An Assessment of Canada's National Critical Infrastructure Sectors*, Office of Critical Infrastructure Protection and Emergency Preparedness, July 2003.

[96] More information on NAICS can be found at: http://www.statcan.ca/english/Subjects/Standard/naics/2002/naics02-index.htm.

Table 6.1 NAICS Mappings

Category	NAIC N^{o}	Description
Software	511210	Software Publishers
Hardware	334110	Computer and Peripheral Equipment Manufacturing
	334210	Telephone Apparatus Manufacturing
	334220	Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing
	334410	Semiconductor and Other Electronic Component Manufacturing
	335920	Communication and Energy Wire and Cable Manufacturing
Communications/ Network Services	517110	Wired Telecommunications Carriers
	517210	Wireless Telecommunications Carriers (except Satellite)
	517310	Telecommunications Resellers
	517410	Satellite Telecommunications
	517510	Cable and Other Program Distribution
	517910	Other Telecommunications
	518110	Internet Service Providers, Web Search Portals
	518210	Data Processing, Hosting, and Related Services
Consulting & Services	541510	Computer Systems Design and Related Services
	811210	Electronic and Precision Equipment Repair and Maintenance
	611420	Computer Training
	237130	Power and Communication Line and Related Structures Construction

6.4.2 Software

Software vendors are defined by Statistics Canada as those companies[97]

> primarily engaged in publishing computer software, usually for multiple clients and generally referred to as packaged software. Establishments in this industry carry out operations necessary for producing and distributing computer software, such as designing, providing documentation, assisting in installation and providing support services to software purchasers. These establishments may design and publish, or publish only.

These vendors provide the systems software that operates most of the Critical Information Infrastructure, as well as the applications software that delivers most of the Critical Information Infrastructure functionality.

6.4.3 Hardware

Hardware vendors are those companies that manufacture and sell the computer and communications hardware that is encompassed by the Critical Information Infrastructure. This includes such things as computers, peripherals, routers and switches.

6.4.4 Communications/Network Services

The primary function of this group is to operate the network that is the foundation of the Critical Information Infrastructure.

6.4.5 Consulting & Services

This category includes firms involved with the design, construction and maintenance of the Critical Information Infrastructure. Table 3.1 gives some indication of the types of firms encompassed.

Some examples include:

- Custom computer program development
- IT facilities management services
- Web site development
- Systems integration consulting

6.5 Industry Watchers

The Critical Information Infrastructure is important, complex and volatile. This has led to the development of a large number of firms whose activities involve tracking, analyzing and reporting on the industry. They help to keep all of the other stakeholders apprised of relevant developments, and their opinions often exert significant influence on industry directions and the fortunes of individual organizations.

---

[97] Statistics Canada, *North American Industry Classification (NAICS) 2002*, online: Statistics Canada, <http://stds.statcan.ca/english/naics/2002/naics02-class-search.asp?criteria=511210>.

Industry watchers include a broad range of firms, but the ones that have an important impact on the Critical Information Infrastructure can generally be divided into IT media organizations and researchers.

IT focussed media organizations activities encompass trade publications, consumer publications and trade shows. They can be both Canadian and international. Examples include:

- ComputerWorld, www.computerworld.com
- PC Magazine, www.pcmag.com
- eWeek, www.eweek.com
- Real World Linux Conference and Expo, www.realworldlinux.com

Researchers include specialized IT market research firms and academic researchers in universities and government. Some examples of IT market research firms:

- IDC Canada, www.idc.ca
- Gartner, www.gartner.com
- Meta Group, www.metagroup.com

7.0 Accountability in Other Environments

7.1 Introduction

The challenge of getting accountability for critical infrastructures 'right' is universal. It spans both other critical infrastructures and other jurisdictions. Many lessons have been learned (mostly by making mistakes). We believe that a number of these lessons from other environments have relevance to Critical Information Infrastructure accountability. This brings to mind a thought from Confucius: ''By three methods we may learn wisdom: First, by reflection, which is noblest; Second, by imitation, which is easiest; and third by experience, which is the bitterest.'' In this report, we are attempting the first two methods.

The subsections below present brief summaries of how accountability is handled in other environments. We selected these examples because we feel that the accountability lessons have particular relevance to the Critical Information Infrastructure. We discuss this relevance in the final subsection.

7.2 Health Care Professionals

7.2.1 Development of Accountability

Historically, modern health professions regulation commenced in the late 19th and early 20th centuries with the emergence of state regulation of medicine. In order to prevent the harm associated with 'dangerous medical practice,' governments enacted legislation to regulate health-care practitioners. Physicians were the first group to successfully obtain such state-sanctioned control. The subsequent evolution of regulatory regimes for health-care providers has been patterned upon a regulatory model designed to regulate medicine and grounded in a broad legal definition of medicine's scope of practice.[98]

The Constitution[99] grants the jurisdiction to regulate professions to the provinces and territories. The provincial and territorial governments have, in turn, enacted legislation that delegates the regulatory authority of various professions to organizations comprised of members of these professions. These professional regulatory bodies are generally self-governing within the confines of their statutory authority, and have been granted the right of self-governance in order to fulfill their mandate of protecting and promoting the public interest.[100]

As health care developed and matured in Canada, there was a steady increase in the number of self-regulating professions (self-governance for physicians and dentists dates back to the time of Confederation). Extremely rapid growth occurred in the number of health professions during the

---

[98]Douglas Alderson & Deanne Montesano, *Regulating, De-regulating and Changing Scopes of Practice in the Health Professions – A Jurisdictional Review* (a report prepared for the Health Professions Regulatory Advisor Council (HPRAC) (April 2003) at 3, online: Health Professions Regulatory Advisory Council <http://www.oaccpp.on.ca/news/appendix1-dp.pdf>.

[99]*Constitution Act, 1867* (U.K.), 30 & 31 Vict., c.3, reprinted in R.S.C. 1985, App. II, No. 5.

[100]James Casey & Frances Picherack, *The Regulation of Complementary and Alternative Health Care Practitioners: Policy Considerations*, Health Systems Division-Health Canada (December 2000), online: <http://www.hc-sc.gc.ca/hppb/healthcare/pubs/comp_alt/regs.html#t3>.

1960s and 1970s, owing to the emergence of various subspecialties. Currently, there are over 35 regulated health professions in Canada, with the predominant regulatory approach being that of self-regulation. Self-regulation has typically evolved historically through legislation, subsequent to acceptance or recognition by key players in the health care sector (both economic and political).[101]

An illustrative example is provided by the evolution of accountability in the health-care sector in Ontario. The *Regulated Health Professions Act, 1991*[102] (RHPA), which came into force on 31 December 1993, established a common framework for the regulation of health-care providers in the 23 regulated health professions in Ontario. In combination with a series of profession-specific acts, this legislation regulates both the practitioners themselves as well as the practice of the various professions.[103]

The basis for all health regulatory legislation that governs health care providers is protection of the public (i.e. protection for patients from health care practitioners that are incompetent, not fit to practise, etc.) This public protection rationale is grounded in the belief that regulated practitioners provide a better quality of health care than those who are unregulated. However, by the 1980s, governments throughout Canada and the U.S. were recognizing the drawbacks of regulation in various other sectors of the economy. Although the Ontario government recognized the social costs of regulating health-care providers, and realized that it might not be prudent or possible to deregulate the health professions, the RHPA was intended to diminish the adverse effects of regulation. Unlike its predecessor legislation, the RHPA was designed to avoid three detrimental aspects of the previous statutes:

1. Excessive limitation imposed upon the patients' freedom of choice;
2. Impediment to the evolution of the roles of the various health care professions; and
3. Limitations upon the creative utilization of health care professionals.

As was the case in the previous health regulatory system, the RHPA preserved the concept of self-regulation for the health professions. However, the governing bodies (the Health Regulatory Colleges) were required to function with more transparency and greater accountability to the public.

The *Regulated Health Professions Act, 1991* includes many rules that relate to accountability. The Health Regulatory Colleges, as well as their members, have legal obligations to serve and protect the public's interest and be accountable to individual patients as well as the public at large. Some of the more important provisions of the statute that deal with accountability include the sections on the structure of the College Councils, the responsibilities and powers of the Councils, Patient Relations programs, College Registers, the Complaints and Discipline process, public disclosure provisions, and the composition of the Advisors Council.[104]

---

[101] *Ibid.*
[102] S.O. 1991, c. 18.
[103] Linda S. Bohnen, *Regulated Health Professions Act- A Practical Guide* (Toronto: Canada Law Book, 1994) at 1.
[104] Ontario, Health Professions Regulatory Advisory Council, *Weighing the Balance – A Review of the Regulated Health Professions Act – Request for Submissions*, (Toronto: Publications Ontario, 1999) at 20, online: Health Professions Regulatory Advisory Council, <http://www.hprac.org/downloads//fyr/weighing.pdf>.

Under the Act, health professionals are required to be accountable to both their patients and to the public. The Health Regulatory Colleges are required to serve the public interest and are accountable to the public for this responsibility. The effectiveness of the Act in promoting and maintaining accountability among health care professionals requires that the RHPA establish sufficient provisions for accountability. It is the mandate of the Regulatory Colleges to ensure that such provisions are implemented optimally.[105]

Each Regulatory College has a Council that functions as a board of directors. All College Councils are required to have public members who are not regulated health professionals (although the professional members are always in the majority). To further ensure public accountability, the public has the right to attend Council meetings (except in limited and rare circumstances).

The primary responsibility of a College's Council is to govern the profession in the public interest by ensuring that its members comply with the RHPA and are accountable to the public. The Act ensures and maintains public accountability by having the Colleges report annually to the Minister of Health and Long-Term Care and by the previously mentioned requirement that College Councils include public members.

Duties of the College Council encompass the development and maintenance of standards relating to College membership requirements, quality assurance, scope of practice, and professional ethics. The Councils also have the authority to make Regulations, which carry the same force of law as does the RHPA. From the point of view of public accountability, some of the more important subject matter areas covered by Regulations include the definition of professional misconduct and conflict of interest, restrictions on advertising by health professionals, parameters and requirements for record keeping, and rules concerning delegation of controlled acts.

Another important feature of the RHPA to ensure and maintain public accountability is that the Act requires each College to establish a patient relations program to help prevent and/or deal with sexual abuse of patients, including funding for therapy and counselling. These programs function to educate College members and to inform the public about what is and is not appropriate professional conduct.

Every Health Regulatory College is required to maintain a Register that contains information about the College's members, including disciplinary action, information relating to incompetence or professional misconduct, whether any terms, conditions or limitations have been placed upon a member's certificate of registration, whether a member's certificate of registration has ever been suspended or revoked, etc. Since anybody, including members of the public, can obtain this information, accountability to the public is maintained and strengthened.

Public accountability is also an important feature of the complaints and disciplinary process. All formal complaints are investigated by a panel of the Complaints Committee. This panel must have at least one public member. After all submissions and evidence have been reviewed, the

[105] *Ibid*. at 24.

Complaints Committee may refer the matter to the Discipline Committee for possible disciplinary action. Each Health Regulatory College is required to include in its annual report a summary of the decisions of the Discipline Committee as well as the reasons for the decisions. Information about members found guilty of professional misconduct by a Discipline Committee is available to the public.

To ensure that overall accountability is maintained, the Health Professions Regulatory Advisory Council (Advisory Council) is vested with the responsibility for reviewing the impact and effectiveness of the RHPA. The Advisory Council is an impartial arm's length agency of the Ministry of Health and Long-Term Care. Its public members are appointed by the government and cannot be public servants, Crown employees, or former or present members of any Regulatory College or College Council.

7.2.2 Accountability Lessons

Various stakeholders in the sector felt that self-regulation is appropriate and functions well when the following criteria are satisfied:

1. There are clearly defined/delineated standards of practice (as in a profession) or industry standards. In the case of professions, the scope of practice must be well-defined and demarcated.
2. There must be a properly constituted body to oversee, coordinate and facilitate the self-regulatory process. In the case of the health professions in Canada, these entities are usually known as Regulatory Colleges.
3. There must be mechanisms built into the self-regulatory system to ensure optimal public accountability and transparency. In the case of health regulatory colleges, this has meant the inclusion of public members on College Councils and ensuring that Council meetings are accessible to the public (except in specific and limited cases when open meetings are not feasible).
4. The enabling statutes (and regulations) should clearly outline the powers and the duties of the self-regulatory entities.

It should be noted that there is an intrinsic tension in allowing professions to be self-regulatory. Although one can argue that the professionals are in the best position to evaluate standards and practices of their peers, a counterargument can be made that those who act to regulate entry into or the practise of a profession cannot do so fairly if they stand to benefit from their own regulatory actions (e.g., by reducing competition in the market by establishing unnecessarily high standards for entry into a profession).

7.3 The Financial Services Sector

7.3.1 Development of Accountability

In Canada, prior to Confederation (and as in many other countries), banking developed in order to satisfy the needs of trade and commerce. An early theory of the function of banks in the economy endeavoured to explain how money supply changes should be linked to the needs of trade. This theory, known as the 'Real Bills Doctrine,' stated that the growth of the money supply should be linked to output growth by way of the use of short-term credit (which historically meant private bank notes). By this mechanism, the money supply would always be backed by the existing production of the economy, thus ensuring a stable price level.[106]

The initial development of the financial sector in Canada was influenced by an accountability-based viewpoint that the welfare of society as a whole stipulates that the banking industry must be regulated to some extent. Thus, the early development and evolution of the financial sector in Canada was influenced by this view as well as by the conservative approach to banking taken in England. However, this conservatism was tempered by the free banking[107] experiments of the United States and Scotland in the period from 1800 to 1850. According to the free banking paradigm, individuals and businesses will tend to seek out institutional arrangements that minimize the costs of conducting business. Competition between banks is said to foster stability in the system, thereby negating the need for a central bank (a lender of last resort).

The opposing perspective on the evolution of a banking system is commonly known as the 'Legal Restrictions View.' This paradigm states that only regulation will force the public to hold non-interest bearing government debt (i.e. currency). Stability of the financial system will only be maintained through a certain level of governmental regulation and control.

During the 18th and early 19th centuries, a function of banking institutions that was equally important to that of accepting deposits and making loans was the issuance of bank notes. Because Great Britain was developing a tradition of careful conservative banking, banking charters were quite difficult to obtain in the British colonies such as Canada. After several failed banking ventures by groups of Montreal merchants in the late 18th and early 19th centuries, the Bank of Montreal obtained a charter to operate as a bank in 1822. The Bank of New Brunswick and the Bank of Upper Canada had been granted charters in 1820 and 1821, respectively. These early bank charters authorized a banking institution to issue notes, make loans for commercial purposes up to a stipulated amount, and usually open branches. A commonality present in all of these charters was that the financial institution had to be accountable to the government by reporting the status of its financial activities at regular intervals.[108]

Therefore, this conservative banking paradigm based upon the British model, characterized by regulation and accountability to the government, became the model for future evolution and development of banking in Canada.

---

[106] Pierre L. Siklos, *Money, Banking and Financial Institutions – Canada in the Global Environment*, 2d ed. (Toronto: McGraw Hill Ryerson Limited, 1997) at 390.

[107] 'Free Banking' denotes a financial system that is largely unregulated and has few governmental barriers to entry.

[108] *Ibid*. at 392.

In response to objections from populists that banking charters were primarily being issued to persons with the 'right' socio-political ties, mostly in urban areas, the legislature of Upper Canada introduced a free banking statute in 1850 that was based upon New York State banking laws of the period. However, a quantum of accountability was still present in the form of limited regulation. For example, there were regulations specifying the minimum start-up capital required, in addition to a requirement that bank notes be redeemable for cash on demand.

Upon Confederation, the *Constitution Act, 1867*, granted monopoly powers in all areas of banking and currency issue to the newly formed federal Government of Canada. The first *Bank Act* was enacted by Parliament in 1871, and would be the first in a series of statutes to regulate the activities of all chartered banks in Canada. Its highlights included the definition of a chartered bank, a gradual introduction of a government monopoly in the issue of currency, and a stipulation that the legislation be revised every 10 years.

The predominant themes in the series of *Bank Acts* were a concern for bank safety and a widening in the scope of chartered banking operations. The issue of bank safety was first explicitly addressed in 1891, when the Bank Circulation Redemption Fund was established to protect against the loss of funds in cases of bank failure. Evidence of steadily increasing financial accountability is apparent with the ever-increasing requirement for auditing of bank activities, which culminated in the creation of government supervision of the banking system. In addition, accountability to the public was increased further in 1967 with the establishment of the Canada Deposit Insurance Corporation (CDIC).

An important development in the evolution of accountability in the financial sector was the establishment of the Bank of Canada in 1935. The contraction of the money supply during and after the Great Depression was considered a failure of the pre-existing arrangement for monetary policy. In addition, the gold standard effectively terminated in the 1930s. Political forces also contributed to the need for a central bank, including the need for Canada to coordinate its international economic policies with those of the rest of the world.

The mandate of the Bank of Canada includes the maintenance of Canada's monetary policy and the facilitation of growth of economic activity combined with low levels of unemployment. The bank functions to create greater accountability in the financial system by controlling monetary policy through interest-rate adjustment and monetary base management. In addition, it conducts open market operations, acts as the federal government's fiscal agent, and functions as the lender of last resort.

The so-called 'modern period' (from the 1970s to the present) has been characterized by financial legislation designed to liberalize the regulations governing the behaviour of chartered banks. Similar to most governments in other countries, Canada has instituted deregulation in several aspects of the banking sector. This has allowed the chartered banks to offer a wider range of products and services, including residential mortgage services, financial leasing, and data processing services. Starting in the 1980s, chartered banks were permitted to acquire brokerage firms.

The *Bank Act* of 1991 introduced a regulatory environment that fostered the creation of near-equal competition throughout the financial sector in Canada. This virtually eliminated the

historical 'four pillars approach' to Canadian financial institutions, which included the chartered banks (commercial loans), trust companies and credit unions (personal loans), insurance companies, and investment dealers. This Act basically introduced a comprehensive set of reforms for all types of financial institutions, rather than the past system of legislating one branch of the financial sector in isolation from the others.

Canada's banks have enjoyed huge benefits, including tremendous asset growth, record annual profits, and market dominance resulting from decades of protection and privileges afforded to them by the Canadian government. Each of the Big Five banks' assets exceeds the federal government's annual revenues.[109] Although many critics have argued that the banks would not be as large or profitable as they are without these protections and privileges, and although many Canadians are dissatisfied with aspects of the banks' practices and policies, few will deny that banks are in a strong position of public trust with respect to the money they manage. In addition, consumers need to be protected with respect to the financial sector.

It is for these reasons that there is a continued need for regulations/legislation to ensure appropriate accountability in the financial sector.

The federal government recognizes the need for regulation of the financial services sector. As the discussion paper on the 1997 Review of Financial Sector Legislation stated:

> There is no question that regulations are required in the financial sector. Regulations not only protect the consumer, they set out the rules of the game so that the sector can operate smoothly.[110]

Furthermore, various stakeholder groups, representing consumers, small business and community interests have urged the federal government to amend/expand the current legislation and regulations so as to provide greater accountability and increased fairness.

7.3.2 Financial Audit

As can be seen in the previous subsection, the financial services sector represents a vital segment of the national economy. The main reason for this is that it is intimately associated with both monetary and fiscal policy. This sector largely controls the creation and flow of money through the economy.

Reliable and accurate measurement in the financial services sector is of paramount importance, owing to the need for quantification of monetary flows. Largely because the accounting for monetary flows is so crucial, a set of standards known as Generally Accepted Accounting Principles (GAAP) was developed and implemented. A comprehensive explanation and definition of GAAP (from the College of Commerce at the University of Saskatchewan) is reproduced as follows:

---

[109]Canadian Community Reinvestment Coalition, "An Accountability System For Financial Institutions in Canada: How To Ensure They Meet a High Standard of Performance," *CCRC Position Paper #5 Summary*, (December 1997), online: CCRC Web Site <http://www.cancrc.org/english/pp5sum.html>.
[110]*Ibid.*

> The term 'generally accepted accounting principles' in the auditor's report includes not only the narrow notion of specific principles associated with accounting (e.g., historical cost principle, matching principle, revenue realization principle) but also specific policies (methods), practices, procedures, and rules used to determine what is included in the statements, how amounts are determined (measurements made), how items are classified, and what disclosures are made (e.g., notes). Necessarily, the GAAP referred to incorporates all the requirements of recommendations in the CICA Handbook. Beyond this, the 'principles' applied reflect what is done by a substantial number of Canadian companies for similar items, or is supported by Canadian literature other than the CICA Handbook, or standards of the IASC or foreign countries (particularly the U.S.). When going outside the CICA Handbook, or when interpreting its contents when acceptable alternatives are permitted or a recommendation is somewhat general, professional judgement must be used to establish that a 'principle' used is justifiable and appropriate to a situation.
>
> Accounting theory (conceptual framework regarding objectives, relevant concepts, etc.) should be inferred in the GAAP referred to in audit reports. The CICA Handbook definition of GAAP incorporates the broad conceptual base for financial accounting. Prior to this definition being placed in the Handbook (March 1991), many had not viewed the theory as part of GAAP, but considered it always as a general basis for the development of GAAP. However, implicitly, the theory has probably played an important role when exercising professional judgement.
>
> Generally accepted accounting principles are those principles (regardless of whether or not their use is limited) that have substantial authoritative support. Whether a given principle has authoritative support is a question of fact and a matter of judgement. The accountant and auditor are both responsible for collecting the available evidence of authoritative support, and judging whether it is sufficient to bring the practice within the bounds of generally accepted accounting principles.
>
> The basic source of generally accepted accounting principles in Canada is the CICA Handbook. *The Canada Business Corporations Act* establishes this as the basic document setting the laws of the country with regard to financial accounting standards and disclosures for companies incorporated under it. While it is of primary importance, the CICA Handbook frequently leaves plenty of room for judgement regarding what the standards are and, therefore, other sources of authoritative support are significant.[111]

In order to ensure that GAAP was being properly applied, a third-party checking mechanism was developed, known as financial auditing. The auditors who conduct and implement the audit do not themselves control the reported financial measurements. Therefore, the financial services establishment realized that it could not hold auditors responsible for the accuracy of the financial statements. *Instead, the auditor is accountable for the process, not the results of the audit*, since they have no control over the behaviour of the corporation whose financial statements are being audited.

---

[111]College of Commerce-University of Saskatchewan, Commerce 321 Course, "Solution to Assignment #1" (2002), online: College of Commerce-University of Saskatchewan <http://www.google.ca/search?q=cache:OzP6wSXzfgYJ:www.commerce.usask.ca/faculty/kobussen/Comm_321/Solution_to_Assignment_1.doc+%22definition+of+GAAP%22&hl=en&ie=UTF-8>.

7.3.3 Accountability Lessons

Various stakeholders in the sector offered the following opinions regarding accountability lessons:

- Where it is determined that the supply of a critical good or service is best achieved by a restricted oligopoly, public sector regulation is often appropriate. This also applies to a monopoly supply situation.
- In cases where the Canadian operating environment is both volatile and globally connected, a formal process would be useful to review and update regulations and legislation on an ongoing basis. This is necessary to ensure that they remain relevant and effective.
- If we want to hold persons and entities accountable for their actions, it is essential to have dependable and reliable measurements tools in place – e.g. standards, benchmarks, and/or specific procedures (a good example is GAAP) – to facilitate the process.
- If an entity does not exercise total control over all aspects of a situation, the best outcome that can be anticipated is that this entity will be held accountable for its process, but not for its actual results (as is the case with respect to financial auditors).

7.4 Electric Utilities

7.4.1 Development of Accountability – The U.S. Experience

Unlike the Critical Information Infrastructure, the electric power sector is a mature and established industry. The California Electric Company of San Francisco, which started in 1879, was the first company started for the purpose of selling electricity. Electric power was sold to commercial enterprises and factories to provide power for electric arc lamps.[112] This was followed three years later by the opening of Thomas Edison's Pearl Street generating station in lower Manhattan, which provided direct current (DC) electric power for incandescent lighting to an area of approximately one-sixth square mile. Over the next 20 years, small electric generating plants were constructed in cities of all sizes. By the start of the 20th century, over 3000 generating stations were in operation in the United States.

Lucien Gaulard and John D. Gibbs patented the world's first alternating current (AC) power transmission system in England in 1881. The U.S. patents to the system were purchased in 1885 by George Westinghouse, and the first commercial transmission of alternating current in the U.S. occurred over a 3300-volt line from Willamette Falls to Portland, Oregon in 1890.

In the first few years of the electric power industry, accountability was virtually non-existent. Electric generating and distribution facilities were initially owned by individuals or small groups of investors. In some cases, people generated electric power for their own domestic use and sold the excess to their neighbours. Others established small generating plants and sold electricity to

[112]Luces M. Faulkenberry & Walter Coffer, *Electrical Power Distribution and Transmission*, (Englewood Cliffs: Prentice-Hall, Inc., 1996) at 7.

anyone who would purchase it. Some electric generating stations were opened and operated by entrepreneurs seeking a profitable venture.[113]

Since each generator had to be connected to each customer that it served, many localities had duplicate electric power distribution systems. Three main problems resulted from this situation:

1. The numerous, closely spaced, crisscrossing transmission lines created a potential danger to life and property;
2. There was unacceptable crowding of public right-of-ways resulting from the numerous distribution systems; and
3. The numerous duplicate distribution systems resulted in extremely high capital costs, which in turn produced high rates for electricity.

The first attempt at establishing accountability occurred when franchises were granted for a single geographical area to a single supplier of electric power. By 1900, some of the small, competing electric power companies had been consolidated into larger franchised enterprises owned by investors.

Although this step resolved the three aforementioned problems, it created a new one – the need for a method of controlling the rates charged for electric power, since competitive forces could no longer govern this. This problem was addressed via regulation. New York State established the first public utility regulatory commission in 1905, which signalled the start of the shift in the electric generating and distribution sector to state-regulated monopolies. Forty-two states had created electric utility regulatory commissions by 1924. The Federal Power Commission was established in 1920 to license the construction and operation of hydroelectric generating plants.

Early in the development of the electric utility industry (1914–1916), the rationale for electric utilities to be regulated monopolies was stated. These reasons are still considered valid today. First, the capital investment required for each unit of revenue received is substantially higher in the electric generation and distribution industry than it is in other sectors. Second, duplication of electric utility service in a geographical area is expensive and inefficient, and wasteful of both natural and human resources. However, in order to assure accountability to the public, monopolies must be regulated, since these utilities have no competition. The regulatory entities themselves must be accountable to the public, so as to ensure that suitable rate structures and business practices are being followed by the utilities. In addition, the electric utilities must be assured of adequate return on investment, so as to provide for the necessary capital improvements and to attract investors.

Another aspect of accountability in the electric utility sector is in the area of public safety. Utility companies are responsible for taking reasonable precautions to ensure the safety for both the public and their own employees. The utilities must ensure that no injuries to people or damage to property occurs due to inadequate or faulty equipment. This safety aspect is particularly vital when dealing with the single greatest threat to public safety in any critical infrastructure: nuclear generating plants.

[113] *Ibid*. at 7.

7.4.2 Development of Accountability – The Canadian Experience

In most countries outside the U.S., the government is the entity that generates and distributes electric power. The electric power transmission and distribution system in Canada is peculiarly structured, in a manner that reflects the historical idiosyncrasies of federal/provincial jurisdictions and competition between the provinces. Rather than developing a national grid system or even substantial regional grids to take advantage of efficiencies and low-cost producing abilities of some provinces, the squabbling between provinces prevented the development of a mechanism that could have regulated the transmission of electricity across provincial boundaries. Instead, each province developed an electrical grid for transmission and distribution within its borders. Rather than export electricity to other provinces, a province would export electricity to the U.S. owing to this unique grid morphology. As a result of this historical evolution, north-south ties are significantly more prevalent and developed than those between the provinces.[114]

With respect to the evolution of accountability, since the electric power industry developed predominantly within provincial boundaries, most of its regulation is under provincial control. Until recently, all provincial governments either directly owned the major electrical utilities or maintained strong regulatory control over private monopolies. The effect of this was that in most cases, the security of supply and stability of prices were firmly located in the public realm. The federal government regulated the export of electrical power to the U.S. and regulatory approval was needed from the National Energy Board (NEB) in order to enter into any export agreement.[115]

Such agreements were subject to public scrutiny and accountability through hearings to determine the effect on various stakeholder groups and the environment. This federal control and public scrutiny began to change, however, with the gradual opening of the market to comply with the U.S. Federal Energy Regulatory Commission (FERC) demands and with the signing of the Canada-U.S. Free Trade Agreement, and later the North American Free Trade Agreement (NAFTA).

Canadian electric utilities realized that if they wanted to increase exports to the U.S., they would need to begin the process of deregulating their markets. Overall accountability with respect to the export of electricity was diminished by changes to the law that altered the oversight functions of the Canada NEB. These changes included the removal of the necessity to consult with the public about the economic and social significance of proposed exports. Export permits are now permitted to proceed in a more routine manner without public hearings and in most cases without any federal scrutiny. In response to market changes, the rise of electric power trading, and the increase of Canadian utilities' actions on spot markets, blanket export permits are issued to exporting companies. As a result, accountability is reduced since virtually no control or oversight exists over Canadian exports of electricity.[116]

---

[114]Marjorie G. Cohen, "From public good to private exploitation: GATS and the restructuring of Canadian electrical utilities" *Canadian-American Public Policy* 48 (1 December 2001) 1, at 30.
[115]*Ibid*. at 33.
[116]*Ibid.*

In Ontario prior to 1998, Ontario Hydro, a vertically integrated, government-owned monopoly, was responsible for meeting the province's electricity generation and transmission needs. The power produced by Ontario Hydro was purchased and distributed to consumers by approximately 300 local, municipally-owned electric utility companies that were charged a fixed price per kilowatt hour (kWh). The bundled price included generation, transmission and distribution costs.[117]

Ontario Hydro had amassed a huge debt over the years, which resulted in a doubling in the prices of electricity in the late 1980s and early 1990s. This situation was often attributed to the organization's central planning methods and lack of 'serious accountability.'[118] Critics repeatedly cited Ontario Hydro's lack of accountability to the Ontario Legislature or any other entity. The Ministry of Energy, Science and Technology published a white paper in 1997 that stated that there was "an ambiguous relationship" between Ontario Hydro and the Ontario government.

The Ontario government dismantled the Ontario Hydro organization in 1998. At the time, municipal electrical utilities also distributed the electricity transmitted by Ontario Hydro. These municipal electrical utilities were regulated by Ontario Hydro. The aim of the government was to deregulate the electricity sector and create competition in the industry. As a result of this break-up, five distinct entities were created from the former Ontario Hydro. Ontario Power Generation Inc. (OPG) was made responsible for electricity generation and the sale of energy at the wholesale level. Hydro One Inc. assumed the transmission, rural distribution and retail energy services business. An Independent Electricity Market Operator (IMO) was created to be the market operator responsible for the dispatch of electrical power and control over the transmission grid. The Electrical Safety Authority was established to conduct inspections of electrical equipment and wiring installations. The Ontario Electricity Financial Corporation (OEFC) assumed the responsibility of managing the outstanding debt of the former Ontario Hydro.[119]

The restructuring of Ontario Hydro did not produce the desired results of reducing the province's debt in the electricity sector, lowering electricity prices, and encouraging private-sector investment in electricity generation facilities. Rather, it resulted in higher prices and new electricity-sector debt, while discouraging private sector investment in generation. The solution to Ontario's electricity problems may be related to a different facet of accountability (i.e. an economic form of accountability). Both producers and consumers of electricity must be subject to realistic prices that reflect the actual conditions of supply and demand. This type of regime is required to produce fiscal sustainability and long-run stability for the electricity system of Ontario. In addition, by exposing consumers to prices that reflect actual market conditions, the commensurate demand-side incentives to conserve energy and use energy-saving products will be created. Likewise, such a linking of pricing to market conditions would generate the supply-

[117]Michael J Trebilcock & Roy Hrab, "What will keep the lights on in Ontario: responses to a policy short-circuit?" *C.D. Howe Institute Commentary* 191 (1 December 2003) 1, at 3.
[118]David McFadden "Power to the people: The Opening of Ontario's electricity market is not just a get-rich scheme for a greedy few. It swill benefit the economy, the environment and consumers." *The Financial Post (National Post)* (2 May 2002) FP 15.
[119]Cohen, *supra* note 114 at 55 - 56.

side pressures required to stimulate investment in efficient generation and transmission equipment and facilities.[120]

With respect to nuclear power plants, a high level of accountability has been imposed by legislation. Section 3 of the *Nuclear Liability Act*[121] (NLA) states in part:

> Duty of Operator
>
> 3. Subject to this Act, an operator is under a duty to secure that no injury to any other person or damage to any property of any other person is occasioned as a result of the fissionable or radioactive properties, or a combination of any of those properties with toxic, explosive or other hazardous properties, of (a) nuclear material that is in the nuclear installation of which he is the operator

Section 4 imposes maximum accountability when it states:

> Absolute Liability of Operator
>
> 4. Subject to this Act, an operator is, without proof of fault or negligence, absolutely liable for a breach of the duty imposed on him by this Act.

The *Nuclear Liability Act* has two main purposes:

1. To ensure that funds are available to provide financial compensation to third parties for injuries or damage suffered as a result of a nuclear incident and to impose upon the operator the obligation of strict liability regardless of fault; and
2. To establish a regime of nuclear liability that encourages nuclear development by channelling all third-party liabilities to the operator and by limiting the operator's liability.[122]

The liability regime established in the NLA is similar to that found in the domestic legislation of most nuclear countries, as well as in the two main international conventions on third-party liability, the Paris and the Vienna Conventions. The Paris Convention (basically a Western European convention) was adopted under the auspices of the Organization for Economic Cooperation and Development (OECD) in 1960. The Vienna Convention, which has wider membership, is an International Atomic Energy Agency (IAEA) convention that was adopted in May 1963.

The *Nuclear Safety and Control Act*[123] (NSCA) received Royal Assent on 20 March 1997 and came into force on 31 May 2000. The NSCA replaced the *Atomic Energy Control Act* of 1946 with new, more effective and explicit legislation to regulate the activities of the Canadian Nuclear industry. The NSCA also provided for the establishment of the Canadian Nuclear Safety Commission (CNSC), which replaced the Atomic Energy Control Board (AECB).

---

[120]Trebilcock & Hrab, *supra* note 117 at 19.
[121]*Nuclear Liability Act*, R.S., c. 29 (1st Supp.), ss. 3 – 4.
[122]Natural Resources Canada Electricity Resources Branch, *Nuclear Legislation Web Page*, (6 March 2003), online: Natural Resources Canada – Nuclear Energy, <http://www2.nrcan.gc.ca/es/erb/erb/english/View.asp?x=453>.
[123]*Nuclear Safety and Control Act* (1997, c. 9).

7.4.3 Accountability Lessons

Various stakeholders in the sector offered the following opinions regarding accountability lessons:

- The producers as well as the consumers of the products or services of a regulated monopoly must be held accountable to economic conditions and market forces that reflect the actual conditions of supply and demand in the sector. This is important if the industry is to remain fiscally stable and economically viable.
- Such a regime of 'economic accountability' will also help promote efficient use of products or services as well as attract new capital and investment to the construction of efficient production or delivery capacity.

7.5 Legal Services

7.5.1 Introduction

The practice of law in Canada, as is the case in most commonwealth countries, is a self-governing profession. Absent governmental intervention, lawyers (with some exceptions), elected by other lawyers, are charged with overseeing the admission, competence, regulation and discipline of lawyers within each province. In the United States, by contrast, the legal profession is governed by judicial regulation. Each province has its own individual law society charged with regulating the legal profession within the province. We will examine Ontario's governing body, the Law Society of Upper Canada (the Law Society), as being representative.

In order to practice law within Ontario, a lawyer must be a member of the Law Society. The Law Society's mandate is to:

> govern the legal profession in the public interest by:
>
> - ensuring that the people of Ontario are served by lawyers who meet high standards of learning, competence and professional conduct; and
> - upholding the independence, integrity and honour of the legal profession;
> - for the purpose of advancing the cause of justice and the rule of law.[124]

Forty elected lawyers and eight appointed non-lawyers form the Law Society's governing group, known as benchers. Benchers meet once each month (called Convocation) to deal with governance issues and make policy decisions. Benchers also form panels to hear cases with respect to conduct and competence of lawyers.

[124]Role Statement of the Law Society of Upper Canada, adopted by Convocation on October 27, 1994.

7.5.2 Background

Until 1792, an Ontario lawyer was whomever the British governors in Quebec City decreed to be a lawyer. Courts were given the authority to call lawyers to the bar and to set standards. There was no formal training requirement for lawyers in Ontario until 1785. With the passing of the *Judicature Act* in 1794, colonial courts were replaced with the more institutionalized procedures and structure of the British system. Since there was a dearth of trained lawyers in Upper Canada (now Ontario) at that time, a bill was passed authorizing the Lieutenant Governor to license up to 16 persons as lawyers within two years. After the two-year period, the right to call lawyers to the bar reverted back to the Courts.

In July of 1797, an act titled *An Act for the Better Regulating the Practice of Law* was passed. The Act gave birth to the Law Society:

> …it shall and may be lawful for the persons now admitted to practice in the law, and practicing at the bar of any of his Majesty's courts in this Province, to form themselves into a society, to be called the Law Society of Upper Canada, as well as for the establishing of order amongst themselves as for the purpose of securing to the Province and the profession a learned and honourable body…

The Act gave the newly formed Law Society the right to make rules and regulations with respect to governing the legal profession within Upper Canada. This ability to self-govern and self-regulate did not derive from either the British or the United States systems of governing the legal profession. Both of these jurisdictions were regulated through the courts. The reasons behind the decision to create and allow the Law Society to govern the legal profession appear to be lost since government records from that time were burned during the American occupation of York (now Toronto) in 1813.

Unlike the United States and other Canadian provinces that granted universities the right to educate aspiring lawyers, the Law Society controlled legal education. In 1949, the Dean, along with most of the Law Society's law school faculty, defected to the University of Toronto to form that university's law school. In 1957, the Law Society and provincial universities agreed that any university within the province could open a law school. Admission would require the completion of two years in an undergraduate program. After completion of a three-year law degree, students would be required to article for one year followed by up to six months of practical instruction at the Law Society. This method of training students to become lawyers in Ontario remains more or less unchanged to this day.

In the early days of the Law Society, benchers appointed others to their body as they perceived a need. This method of appointing new benchers led to a profession tightly controlled by insiders. In 1871, the government passed legislation ending life-appointments and giving all members of the Law Society in good standing the right to vote for the 30 benchers who would serve five-year terms (with the exception of certain benchers holding their position by way of political office). The legislation did not, however, change the bencher's right to appoint whomever they selected to fill vacancies in their numbers that occurred during the five-year appointment term. 1912 saw the creation of life benchers. Life benchers were benchers given permanent appointments once elected a number of times. Life benchers retained the right to vote but were not counted as part of the 30 elected benchers.

The *Law Society Act* (the LSA) was passed in 1970. The number of benchers increased to 40. The traditional five-year term was reduced to four years. Regional representation was implemented. Vacancies during the five-year term would be filled by defeated candidates based on the number of votes received. Provisions with respect to investigating and disciplining members were added. For the first time, four non-lawyer government appointed bencher positions were created (currently, this number stands at eight). The LSA mandated an annual general meeting. The LSA was revised in 1998 with regional representation altered to better reflect provincial representation.

7.5.3 Governance Today

In order to fulfill its mandate, the Law Society implements a number of programs that educate and inform its members. The Law Society conducts spot audits in order to measure the integrity of law firm financial filings and ensure law practitioners are meeting their record keeping requirements. The goal of spot audits is to identify and correct small problems early before serious non-compliance or misconduct problems arise.

The Law Society governs the legal community in Ontario partially through its Rules of Professional Conduct (the Rules). The Rules set out the professional and ethical obligations of all members of the Law Society. The first 'Rules' appeared in 1964. Coming into force on 1 November 2000, the new Rules have been continually amended in order to better serve both lawyers and the public. For example, the Law Society is currently considering an amendment to include a new rule concerning conflict of interest in the context of a sexual relationship between a solicitor and his or her client. The Law Society issues practice advisories in order to assist members to better understand the Rules and practice management. At present, the Rules are grouped into six categories dealing with different areas or aspects of practice such as the lawyer's relationship to clients, avoidance of conflicts of interest, and the lawyer's relationship to the administration of justice.

Additionally, there are other divisions within the Law Society as well as other organizations that serve to assist lawyers and guard the integrity of the legal profession:

Lawyers Fund for Compensation
The fund gives assistance to clients that have lost money due to a lawyer's dishonest conduct. The fund is financed solely by lawyers and from their personal resources. Since inception, the fund has paid out millions of dollars. The majority of client losses stem from lawyers misappropriating trust funds.

Lawyer's Professional Indemnity Company (LawPro)
Headquartered in Toronto and incorporated by the Law Society in 1990, LawPro is an independent insurance company licensed to provide liability insurance and title insurance in jurisdictions across Canada.

Legal Aid Ontario
The *Legal Aid Services Act* established Legal Aid Ontario (LAO) in 1998. The principal mandate of LAO is to "promote access to justice throughout Ontario for low-income individuals by means

of providing consistently high quality legal aid services in a cost-effective and efficient manner."[125]

7.5.4 The Discipline Process

The Law Society's process for dealing with complaints is similar to the process adopted by other professional governing bodies such as doctors and dentists. The process is set out in the Law Society Act and involves various stages with respect to review of complaints, hearings, appeals and review by courts.

Members can be suspended by certain elected benchers for administrative violations such as failure to pay annual dues or make annual filings. A lawyer is forbidden to practice as long as the suspension is in place. Grounds for a complaint made against a lawyer include: professional misconduct; conduct unbecoming of a barrister or solicitor; incapacity; incompetence; failure to pay dues; failure to make filings; and good character hearing for admission of members.

The Law Society receives complaints against lawyers from a number of sources including clients, other lawyers, the courts, police, or from the general public. Once a complaint is received, the Law Society generally informs the member and allows the member the opportunity to respond. Lawyers have a duty to respond promptly. A failure to respond promptly is grounds for discipline. A minor breach moves to the Complaints Resolution division of the Law Society. A more serious breach is channelled to the Investigation division. Both divisions are part of the Law Society's Professional Regulation Department.

A Complaints Resolution Commissioner reviews and attempts to resolve complaints of persons dissatisfied with the Law Society's initial resolution of complaints. If the complaint is still not satisfactorily resolved, the complaint may be referred to the Proceedings Authorization Committee. The Proceedings Authorization Committee may authorize a hearing to be held in front of a three-member panel of benchers. The Hearing Panel has authority to issue any order pursuant to the LSA such as reprimand, disbarment, suspension or fine. The hearing is much like that of a court, but somewhat less formal. For example, hearsay evidence may be admitted.

Decisions of the Hearing Panel may be appealed to a seven-bencher Appeal Panel. An appeal from an Appeal Panel decision may be made to the Divisional Court. Appeals from the Divisional Court are to the Ontario Court of Appeal or the Supreme Court of Canada.

7.5.5 Other Governance Rules and Acts

In addition to the Rules and various regulations and by-laws under the LSA, the Law Society has adopted Rules of Practice and Procedure for Discipline Hearings. These rules govern the conduct of hearings before a Hearing Panel or Appeals Panel and serve as a supplement to the *Statutory Powers Procedure Act* that governs administrative tribunals in Ontario. The *Solicitors Act* deals with such issues as the unauthorized practice of law in Ontario and the assessment of costs of a solicitor.

[125] *Legal Aid Services Act, 1998*, S.O. 1998, c. 26, section 1.

7.5.6 The Results

Being a self-regulating and self-governing profession, mechanisms to ensure that the legal profession maintain a high level of service and ethics are absolutely necessary. Law societies across the country have responded by implementing programs, rules, accountability systems and avenues that, taken together, assure high standards are maintained. When a standard is breached, a number of systems are in place to address and effectively resolve the breach. Current accountability structures are fair, responsive and expeditious. Law societies have long demonstrated a willingness to adapt and be responsive to changing times in order to make certain that society's legal needs are not simply met, but exceeded.

7.5.7 Accountability Lessons

Various stakeholders in the sector offered the following opinions regarding accountability lessons:

- In order for self-governing entities to have credibility in the eyes of the public, they must provide accountability that is transparent, effective, meaningful and responsive;
- Public trust and confidence in the self-governing entity is paramount;
- Instilling public trust and confidence in the self-regulating body and system is best promoted by putting in place well-defined and enforceable accountability mechanisms;
- Implementing systems (such as the Lawyers Fund For Compensation) that provide additional layers of support and relief when things go wrong assists in inspiring trust and confidence in the self-governing entity; and
- Self-governing entities must diligently update and adapt accountability standards as accountability environments evolve.

7.6 Accountability Lessons for the Critical Information Infrastructure

Sector stakeholders' opinions about accountability lessons are presented in some of the previous subsections. In this subsection, we present ways in which these lessons *may* apply to the Critical Information Infrastructure. These might prove valuable.

7.6.1 Healthcare and Legal

Professions are in the best position to define standards and certification for their members, and enforce adherence to these. The constant threat of regulation ensures integrity. Professional standards and certifications may be necessary if we are to achieve meaningful accountability in the Critical Information Infrastructure.

7.6.2 Financial Services

Dynamic environments require adaptable accountability models with a built-in evolution process to ensure that they stay relevant and effective. There are few environments more dynamic than the Information Infrastructure.

Effective accountability depends on clear standards of measurement. The Critical Information Infrastructure lacks many of the standards needed to enforce accountability. Many feel that they should be developed.

In situations where organizations do not control the complete environment, holding them accountable for following well-defined processes makes sense. The Critical Information Infrastructure is a collection of interdependent parts with no centralized control. Process accountability as opposed to results accountability may, in general, be more applicable.

7.6.3 Electric Utilities

Accountability for results at interfaces between private systems and the rest of a system makes sense. The interfaces provide a defined point of measurement. The Critical Information Infrastructure is composed of many private systems interfaced to a vast shared system. Operators of the private systems can be held accountable for not ‘exporting grief’ to the shared system.

8.0 Accountability Initiatives

In Section 7 we discuss the evolution of accountability in other environments and some of the lessons learned. As we conducted our research on these environments, we came across a number of interesting, specific accountability initiatives. Each of these initiatives also has some lessons to offer. They can provide inspiration for addressing accountability for the Critical Information Infrastructure. In this section, we present brief summaries of these initiatives and conclude by discussing their relevance to the Critical Information Infrastructure.

8.1 Y2K

8.1.1 The Problem

Computer systems faced a potentially serious problem in connection with the year 2000 (Y2K) – the famous Y2K Problem[126]. The problem arose from the fact that two digits were seen as adequate to represent the year of any date, thus "03/21/39" was universally accepted as a shorthand for "21 March 1939". Almost all computer programs built in the 1960s and 1970s, and many built in the 1980s, used this abbreviation[127] for dates. When computers performed arithmetic on such abbreviated dates everything worked, provided the dates fell between 1 January 1900 and 31 December 1999.

The authors of many of the programs written in the 1960s, 1970s and 1980s believed that the life span of their programs would be less than 10 years. There might be problems in 2000, but the confident expectation that all the early programs would be replaced well before 1 January 2000. It didn't happen quite that way. Many of the computer programs still in active use in 1995 were not able to correctly process dates after 1 January 2000. There was a clear Y2K technical problem with many computer systems. If we failed to remediate the problem, many of those computer systems were at risk of failure.

8.1.2 The Response

By 1990 a number of people recognized that we would be facing a Y2K computer problem. There were several early articles and speeches on the subject. There was very little early action to even understand the problem – we didn't really know which computer systems were most vulnerable, nor did we know the likely consequences of Y2K computer failures. This section of the report provides an anecdotal history[128] of the Y2K Problem and suggests how some of the

---

[126] A considerable amount of information about the Y2K Problem was available on the Internet. Many of the most popular Y2K sites have gone off-line, there being no continuing reason to maintain their presence. Some of the sites have been maintained, most often as a part of the Internet presence of a continuing organization. The UK IEE has such a site – see, online: <http://www.iee.org/Policy/Areas/Y2K/index.cfm>. The Oregon State University Extension Service maintains an extensive archival Y2K Web site at <http://extension.oregonstate.edu/archives/y2k/index.html>.

[127] In North America it was common to internally represent, for example, 21 March 1930 as a string of six digits – 032139. There were standard programs to compute the number of days, weeks, months and years between two such dates (e.g. 032140 was computed to be 365 days after 032139).

[128] We were fortunate to have been able to conduct a telephone interview with Peter de Jaeger on 2 March 2004. Mr. de Jaeger was one of the most visible champions of the Y2K Problem in the English-speaking world. His Year 2000 Web site, <http://www.year2000.com/>, was one of the most active in providing a broad range of information on the subject. His current Web site (<http://www.technobility.com/>) provides full information about his current

insights gained may apply or may not apply to efforts to maintain our Critical Information Infrastructure.

Eventually everyone connected with the computer field recognized that we did face a problem over Y2K. Disagreement was only over the extent and severity of the problem. But few IT managers stepped forward to take responsibility or accept accountability. On one level, this was a natural human reaction to a problem that was not urgent. In the early 1990s it would be many years before the Y2K problems surfaced. There were more immediate problems that demanded attention.

Very little progress was made in talking to IT managers, but there was a steady build-up of public pressure about the issue. The Y2K problem was ripe for treatment in the popular and business press. The problem was relatively easy to describe and disaster scenarios had the ring of high plausibility. By the middle of the 1990s, the pressure to do something was building.

When the issue came to a head, it was largely inspired by CYA[129] sentiments. Managers, especially senior executives, did not want to be seen as doing nothing about a problem that was clear and obvious to business and government. By 1997-98, most major institutions, especially major financial institutions, were well on their way to addressing their Y2K problems. The focus had shifted from "What are we going to do about Y2K?" to "What have you done about the Y2K problem?" There was also a growing concern about the problem that expressed itself in statements about fiduciary duties of directors, senior officers and professional advisers.

Major banks were concerned about whether their business customers had taken appropriate steps to address their Y2K problems. Auditors recognized a professional responsibility to raise Y2K preparedness questions. Lawyers began to advise clients that they could be under serious legal threat under negligence and corporate law principles if appropriate steps were not taken to address Y2K concerns. The demand for Y2K compliance statements from vendors grew. Business 'partners' required Y2K compliance statements from each other. Banks demanded Y2K compliance statements from many of their business customers. In the end, there was a land-office business connected with Y2K.[130]

The Y2K problem was a good example of a 'simple' accountability issue:

- The problem was *easy to understand*;
- There was a *fixed deadline*; and
- Technical *solutions* were known.

---

activities. The material in this section draws heavily on that the conversation with Peter de Jaeger. It is also based, in part, on the first-hand experience of both Mark Stirling and Robert Fabian, two of the contributors to this report.

[129]Often politely translated as "Cover Your Assets."

[130]Members of the public were apprehensive. The sale of electric generators grew. People stocked up on bottled water and canned foods. The popular press offered all kind of advice about what to do when the Y2K disaster struck. It was a frantic time.

8.1.3 The Results

The social pressure to address the problem was strong enough that society spent what was required to solve the Y2K problem.[131] There were relatively few Y2K failures. In most cases there were easy workarounds that were deployed (e.g. a letter asking customers to ignore the incorrect printing of '1900' on a statement when it should have been '2000'). Collectively, we did solve the Y2K problem.

Central to the solution, however, was the application of social force from boards of directors, business 'partners' and professional advisors. Accountability was not easily embraced by those with the knowledge and skill required to solve the problem.

8.2 The Treadway Commission

8.2.1 The Problem

The National Commission on Fraudulent Financial Reporting was formed in the United States in 1985. It was more commonly known as the Treadway Commission (the TC) after its chair, James C. Treadway Jr. The TC enjoyed private sector joint sponsorship of Financial Executives International, the American Accounting Association, the American Institute of Certified Public Accountants, the Institute of Internal Auditors and the Institute of Management Accountants. It had a mandate to inspect, analyze and make recommendations in fraudulent public company financial reporting. After two years of studying the financial information reporting system, the TC issued a report (the Report). The TC's stated purpose was "to identify causal factors that can lead to fraudulent financial reporting and steps to reduce its incidence."[132]

The introduction to the Report states:

> Fraudulent financial reporting is indeed a serious problem. Infrequent though its occurrence arguably may be, its consequences can be widespread and significant. Although fraud in any form can be difficult to deter, fraudulent financial reporting can be reduced, perhaps substantially, if each party for whom we made recommendations takes the steps we recommend.[133]

8.2.2 The Response

The TC had three major objectives:

> (1) Consider the extent to which acts of fraudulent financial reporting undermine the integrity of financial reporting; the forces and the opportunities, environmental, institutional, or individual, that may contribute to these acts; the extent to which fraudulent financial reporting can be prevented or deterred and to which it can be detected sooner after occurrence; the extent, if any, to which incidents of this type of fraud may be the product of a decline in professionalism of corporate financial officers and internal auditors; and the extent, if any, to which the regulatory and law enforcement

[131] It could be argued that as a society we over-spent on solutions. Certainly, there was a massive flurry of Y2K compliance statements requested and issued as 1 January 2000 approached.
[132] "Treadway Commission Report on Fraudulent Financial Reporting" [The Report].
[133] *Ibid*. at 2.

environment unwittingly may have tolerated or contributed to the occurrence of this type of fraud.

(2) Examine the role of the independent public accountant in detecting fraud, focussing particularly on whether the detection of fraudulent financial reporting has been neglected or insufficiently focused on and whether the ability of the independent public accountant to detect such fraud can be enhanced and consider whether changes in auditing standards or procedures – internal and external – would reduce the extent of fraudulent financial reporting.

(3) Identify attributes of corporate structure that may contribute to acts of fraudulent financial reporting or to the failure to detect such acts properly.[134]

The Report is divided into five chapters:

1. Overview of the Financial Reporting System and Fraudulent Financial Reporting;
2. Recommendations for the Public Company;
3. Recommendations for the Independent Public Accountant;
4. Recommendations for the SEC and Others to Improve the Regulatory and Legal Environment; and
5. Recommendations for Education.

The TC observed that since "financial reporting by public companies is the most critical component of the full and fair disclosure that ensures the effective functioning of the capital and credit markets in the United States…our examination caused us to conclude that steps need to be taken to improve our financial reporting system, despite its present excellence".[135] The TC concluded that:

- "No company, regardless of size or business, is immune from the possibility that fraudulent financial reporting will occur. That possibility is inherent in doing business;[136]
- "The problem's multidimensional nature becomes clear when we merely consider the many participants who shape the financial reporting process…Each one has the potential to influence the outcome…;[137]
- "The responsibility for reliable financial reporting resides first and foremost at the corporate level…[R]educing the risk of fraudulent financial reporting must start within the reporting company.[138]
- "One key practice [to help all public companies meet their responsibilities and reduce the incidence of fraudulent financial reporting] is the board of directors' establishment of an informed, vigilant and effective audit committee to oversee the company's financial reporting process. Another is establishing and maintaining an internal audit function.[139]
- "Independent public accountants play a crucial, but secondary role. They are not guarantors of the accuracy or reliability of financial statements.[140]

[134] *Ibid*. at 2.
[135] *Ibid*. at 5.
[136] *Ibid*. at 6.
[137] *Ibid.*
[138] *Ibid*.
[139] *Ibid*.
[140] *Ibid*.

- "Regulatory and law enforcement agencies provide the deterrence that is critical to reducing the incidence of fraudulent financial reporting…But improvements can and should be made, both at the state and the federal level.[141]
- "Education can prepare business and accounting students to recognize the factors that can contribute to this type of fraud and the ethical values and good business practices necessary to guard against it."

8.2.3 The Results

Although the Report was well-received, a cynical person might sum up the impact of the TC with one word: Enron. On the positive side, it was extremely helpful in identifying the various stakeholders involved in the financial reporting 'food chain'. It also made significant recommendations that could play a considerable role in minimizing the opportunity for fraudulent financial reporting. However, it must be underlined that the TC's mandate was to make recommendations. Without implementation, even the best recommendation is left to languish on the dust heap of good intentions. During the intervening years, numerous studies and research groups have been struck in order to build upon the work undertaken by the TC. With the arrival of the *Sarbanes-Oxley Act of 2002*, some 14 years after the release of the Report, many of the TC's recommendations were finally implemented.

8.3 The Sarbanes-Oxley Act of 2002

8.3.1 The Problem

Enron collapsed due to corporate fraud. Arthur Andersen was convicted on charges of obstruction of justice in the Enron investigation. Faced with accusations that its stock research misled investors, Merrill Lynch agreed to pay a US$100 million fine in exchange for charges being dropped. The fallout continues as investigations widen in scope. WorldCom imploded due to a US$11 billion accounting fraud. With an onslaught of scandals, legislative intervention aimed at defining corporate standards and holding those responsible for breaching those standards accountable was not far behind. Senator Paul Sarbanes (D-Maryland) stated that "Something needs to be done to restore confidence in the world's greatest marketplace". That 'something' came in the form of the *Sarbanes-Oxley Act of 2002* (the SOA).

8.3.2 The Response

The SOA was named for its bi-partisan congressional sponsors, Senator Paul Sarbanes and Representative Michael Oxley (R-Ohio). The SOA was introduced in the United States on 30 July 2002 and states its purpose as "An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws and for other purposes."[142] On signing the SOA into law, U.S. President George W. Bush voiced a warning to corporate America stating that, "Every corporate official who has chosen to commit a crime can expect to face the consequences."

[141] *Ibid*.
[142] *Sarbanes-Oxley Act of 2002*.

The SOA is made up of 11 titles that together:

- Toughen corporate accountability and governance of public companies,
- Impact directors and officers,
- Make auditors more independent and subject to quality control and integrity standards,
- Empower audit committees,
- Create protection for whistleblowers,
- Speak to conflicts of interest by securities analysts, and
- Offer protections to employees, pension holders and investors from fraud.

The SOA creates the independent Public Company Accounting Oversight Board (the Board) to act as the body that oversees the audit of public companies that are subject to securities laws. The Board protects the interests of investors in the preparation of accurate and independent audit reports and supervises the accounting industry, subject to the direction of the Securities and Exchange Commission (the SEC), which governs trading in securities. Auditors are granted more independence from their public company clients by prohibiting them from providing certain non-audit services. Audit firms must now rotate lead audit partners and the audit partner responsible for reviewing the audit so that neither performs the same audit role for more than five consecutive years.

Every public company must have an audit committee. Each audit committee member must be a member of the board of directors of the company, is not allowed to accept any other compensation other than compensation as an audit committee member and cannot be otherwise affiliated with the company. Auditors report only to the audit committee and not to management.

The SOA mandates that public companies create reporting systems for employees to report misconduct (i.e. 'blow the whistle'). Audit committees must implement procedures for receiving, retaining and responding to complaints including the confidential, anonymous submission of questionable accounting, internal accounting controls and auditing matters. Whistleblowers whose employers retaliate against them are now able to seek relief through the U.S. Department of Labor and the district courts. The SOA makes retaliation a federal offence punishable by up to 10-years imprisonment.

The SOA puts accountability for a public company's financial statements and other disclosures squarely on the shoulders of officers by requiring both the CEO and CFO to personally certify disclosures made in periodic reports. The SOA creates a felony punishable by up to 20 years in prison if a violation of this section was knowing and wilful.

Officers and directors of public companies must report their personal trades of the company's securities within two business days, down from the previous reporting period of up to 40 days. Their trading must be posted on the company Web site. Insiders who violate this section may be subject to suit by the company to have their profits repaid to the company. If a company is required to restate its financial statement as a result of misconduct, the CEO and CFO must reimburse the company for bonuses or other forms of compensation received during the 12-month period following the first public issuance or filing with the SEC of the financial document.

Public companies must disclose whether a code of ethics for senior financial officers has been adopted and, if one has not been adopted, it must explain why not. The SOA bans personal loans from public companies to their executive officers and directors that are not made in the ordinary course of business. Timelines with respect to the reporting of possible negative information are improved. The SOA provides guidelines for securities analysts that ensure unbiased advice. Attorney-client privilege is redefined for lawyers representing public company clients. Outside attorneys representing public companies must take appropriate action when they come across evidence of wrongdoing, despite the old rule that communications between an attorney and a client are privileged. For example, they must disclose their findings to the company's CEO or general counsel and they must ensure that their disclosures are properly addressed by these company representatives. If not dealt with properly, attorneys are obligated to report to a company's audit committee, independent directors, or board of directors. If appropriate action is still not taken, the attorney must inform the SEC.

The SOA creates a number of civil and criminal penalties that provide compliance incentive. For example, the destruction, alteration or falsification of records or documents with the intent to impede, obstruct, or influence a federal investigation is punishable by a fine and/or up to 20-years imprisonment.

8.3.3 The Results

At its core, the SOA is meant to provide securities regulators and law enforcement with the tools necessary to arrest white-collar crime perpetrated by the very people charged with running corporate America. The SOA accomplishes this by setting standards of behaviour and by providing mechanisms to hold individuals that violate those standards accountable. Since the SOA is less than two-years old, it is perhaps too early to accurately gauge its impact. Additionally, having the tools available to combat a problem and using those tools are two separate things – just as having policies and enforcing them are two separate things. However, creating wealth and a growing and stable economy through investment in public companies is perceived to be one of the pillars of the American economic system. The investment system is threatened with collapse if those that traditionally have used the system feel that they can no longer trust it. Restoring public confidence in that system by persuading a jaded public that appropriate legislative safeguards are in place, that authorities are willing to use the tools new legislation provides, and that there are real consequences for those convicted of corporate fraud is, perhaps, the only way of ensuring that the way of life of Americans will continue to thrive.

8.4 European Union's Directive on Personal Data Protection

8.4.1 The Problem

The formation of the European Union (EU) greatly increased the need to transfer personal data within the union. At the same time, there was a growing public sensitivity to the need to preserve the privacy of this data. Demands for accountability respecting the collection, use, retention and disclosure of personal data grew with the burgeoning of massive computerized databases.

8.4.2 The Response

The EU's directive on personal data protection[143] was promulgated in an attempt to provide a regulatory framework that would allow the free transfer of personal information between EU member countries. Also, it would ensure a minimum level of security for the information, whenever it was stored, transmitted, or processed.

The Directive applies to the 'processing' of 'personal data.' Personal data is any information relating to an identified or identifiable natural person (data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity.[144] The processing of data is "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction."[145]

In order for the processing of personal data to be legitimate under the Directive, the collector of personal data must disclose, at the time of collection, its identity, the specific purposes for the data collection and any recipients of the collected data. The collection must be limited to data that is necessary for the identified purposes. The data can only be retained for the period of time that is necessary for those purposes.

Personal data may only be processed for the identified purposes if the data subject has 'unambiguously' consented. He or she must also be informed of, and given the right to opt-out of, disclosure of personal data to third parties. Individuals are guaranteed a right of access and the right to request amendments to incorrect data. The collector of the data is required to monitor correctness of data and correct it as required. More stringent rules apply to the processing of sensitive data (e.g., health or sex life).[146]

Third parties may carry out data processing but must be governed by a contract stipulating that the processor will act only on instructions from the controller. Obligations binding upon the

[143]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] O.J. L. 281/31, ["Directive"].
[144]Directive, Article 2(a).
[145]Directive, Article 2(b).
[146]Directive, Article 8.

controller must be binding on the processor.[147] A data controller must ensure that the data it collects is properly secured with appropriate technology and business methods.[148] In turn, if a third party is conducting data processing on a controller's behalf, the controller must obtain sufficient guarantees that the third-party has protections in place and must ensure compliance with those measures.[149] The Directive does not require that a data subject provide a separate consent to the use of a third-party data processor.

8.4.3 The Results

There is general agreement that the Directive has been successful. It has been instrumental in the implementation of baseline protection for the personal information of individuals that is collected and processed in the course of commercial activities.

Its effects have not been limited to the EU. The transfer of data to a third-party processor situated in a country outside the EU is permissible when such a country ensures an "adequate level of protection" for the data. On 20 December 2001 the Commission decided that Canada is considered as providing an adequate level of protection for personal data transferred from the Community to recipients subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[150]

Indeed, PIPEDA was implemented, in part, to address the requirements of the Directive. Other countries have also acted in a similar fashion so that the legitimate transfer of personal data can continue with EU members.

8.5 The Personal Information Protection And Electronic Documents Act

8.5.1 The Problem

The experience in Canada reflected the experience in the EU. Personal information has become an extremely lucrative asset that is constantly being transferred as people complete daily and routine transactions. The Government of Canada has attempted to address public concerns about the collection, use, retention and disclosure of personal information through the implementation of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[151]

8.5.2 The Response

PIPEDA's rules regarding personal information attempt to balance the right of privacy of individuals with the need of organizations to collect, use, or disclose personal information for a

[147]Directive, Article 17(3).
[148]Directive, Article 17(1).
[149]Directive, Article 17(2).
[150]Commission Decision of 20 December 2001, pursuant to Directive 95/46/EC of the European Parliament and the Council on adequate protection of personal data provided by the Canadian *Personal Information Protection and Electronic Documents Act* (notified under document number C(2001) 4539), O.J. L. 002, 04/01/2002 P. 0013-0016.
[151]S.C. 2000, c. 5 ["PIPEDA"].

reasonable purpose.[152] It was designed to operate in an era in which technology increasingly facilitates the circulation and exchange of information.

PIPEDA now applies to all non-government organizations that collect, use or disclose personal information in the course of commercial activities (subject to provincial legislation, as discussed below). 'Commercial activities' are defined to mean "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character" and includes the selling, bartering or leasing of donor, membership or other fundraising lists.[153] PIPEDA will not apply to provincial undertakings in those provinces that have enacted legislation that, in the view of the federal government, is substantially similar.[154] To date, only Quebec, Alberta and British Columbia have enacted legislation and, as of the date of this writing, the federal government has not officially declared that Alberta and British Columbia legislation is 'substantially similar'.[155]

PIPEDA is intended to protect *personal information* which is "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."[156] This is broad enough to include information such as:

- Race
- Ethnic origin
- Colour
- Age
- Marital status
- Religion
- Education
- Medical
- Criminal
- Employment history
- Financial history
- Address
- Telephone number
- Numerical identifiers such as the Social Insurance Number
- Fingerprints
- Blood type
- Tissue or biological sample
- Views or personal opinions

The restrictions placed on the collection, use and disclosure of personal information under PIPEDA are found in Schedule 1 of the Act (the Schedule). The Schedule is actually an unmodified re-statement of the Standard Council of Canada's *Model Code for the Protection of*

[152]PIPEDA, s. 3.
[153]PIPEDA, s. s.2(1).
[154]PIPEDA, ss. 30(2), 26(2)(b).
[155]*An Act Respecting the Protection of Personal Information in the Private Sector*, S.Q. 1993, c.17.
[156]PIPEDA, s. 2(1).

Personal Information (the Model Code).[157] The Model Code is comprised of 10 principles of accountability with respect to personal information. These principles in turn contain substantive obligations. Pursuant to s.5(1), every organization governed by PIPEDA must comply with the obligations set out in the Schedule.

PIPEDA sets out a series of accountability principles to which those who collect personal information must adhere. At the centre of these principles is the concept of informed consent. The principles seek to ensure that an individual is made aware of the purposes for which personal information is being collected and that the individual is given the opportunity to consent to such specific uses. The principles further seek to ensure that personal information is not used for any other purpose to which an individual has not consented.

A detailed examination of these substantive principles is beyond the scope of this paper.[158] Instead, we wish to draw attention to the accountability mechanism found in the Schedule. The first principle stated in the Schedule – all of which is servient to the principle of accountability – is the most important for our purposes as it is titled "Accountability." It states that an "organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the [principles contained in the Schedule]." While these identified individuals may delegate some of their tasks, they bear the ultimate responsibility for their organization's dealings with personal information. In addition, the identity of these individuals must be made known upon request.

These designated individuals are also responsible for developing procedures to protect personal information while it is in the custody of their organization. They must also establish procedures: to receive and respond to complaints and inquiries, for training staff and communicating to staff information about the organization's policies and for developing information to explain the organization's policies and procedures.

If an individual has a complaint about an organization's practices surrounding personal information, they must first contact these designated individuals. If this does not provide satisfactory results, the individual may complain to the federal Privacy Commissioner, who has the power to conduct an audit of an organization's privacy practices. The Commissioner will issue a report with his or her findings and any recommendations that he or she may have. If an individual is still unsatisfied, he or she may request a hearing in the Federal Court.

8.5.3 The Results

Given that PIPEDA has only been fully implemented for such a short time, its effectiveness as an accountability mechanism remains to be seen. There are those such as University of Toronto professor Richard Owens who believe that PIPEDA will do very little to ensure privacy, while at the same time creating an environment of uncertainty for business. He contends that PIPEDA contains "inconsistencies and errors" that make it "maddeningly difficult for even a trained

[157]CAN/CSA-Q830-96 (Etobicoke, Ontario: Canadian Standards Association, 1996).
[158]For a detailed explanation of PIPEDA and its background, see C.H.H. *McNairn and A.K. Scott, A Guide to the Personal Information Protection and Electronic Documents Act*, 2004 Edition, (Markham, Ontario: LexisNexis Canada Inc., 2003).

lawyer to interpret."[159] University of Ottawa professor and renowned cyber-law expert Michael Geist, however, believes that PIPEDA imposes "a national privacy standard that provides businesses with greater certainty and individuals with guaranteed minimum protections."[160] It will be impossible to determine which, if either, of these views is correct until we have the opportunity to witness the application of PIPEDA over time.

8.6 Health Insurance Portability and Accountability Act

8.6.1 The Problem

Healthcare in the United States is delivered through a system that combines government programs and private enterprise. The many and varied entities involved in this system increasingly use electronic means to share information about medical patients in the course of delivering medical services to those individuals. Such exchanges were traditionally regulated by a patchwork of state laws. This lack of uniform legal standards left significant gaps in the protection of patients' confidential information. In 1996, the U.S. federal government passed legislation aimed at providing a nationwide standard for the protection of such information.

8.6.2 The Accountability Response

The *Health Insurance Portability and Accountability Act* (HIPAA),[161] among other things,[162] attempts to secure the privacy of patients' confidential health information. HIPAA refers to this confidential health information as Protected Health Information (PHI). Much of the substance of HIPAA's protection is found in the final privacy rule (the Final Rule) published by the Department of Health and Human Services pursuant to HIPAA.[163]

The Final Rule applies to 'covered entities' which include health plans, healthcare clearinghouses and healthcare providers.[164] A complete review of all the statutory obligations imposed upon covered entities is beyond our present scope. What follows is a summary of the principles of accountability embodied in the Final Rule.[165]

The Final Rule gives an individual a right to adequate *notice* of the uses and disclosures of PHI that may be made by the covered entity and of the individual's rights and the covered entity's legal duties with respect to PHI.[166] The Final Rule mandates certain content for such notices.

---

[159]Richard Owens, "Federal privacy law is a dog's breakfast," Online: The Toronto Star: <http://www.torontostar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1075677008521&call_pageid=968350072197&col=969048863851>.
[160]Michael Geist, "Canada badly needs a national standard," Online: The Toronto Star: <http://www.thestar.ca/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1075677008515&call_pageid=968350072197&col=Columnist1036500183695>.
[161]Public Law 104-191.
[162]Another key aspect of HIPAA is to secure access to health coverage by limiting pre-existing condition exclusions.
[163]45 C.F.R. pt. 160 ["Final Rule"].
[164]Final Rule, §§ 160.103, 103.
[165]The Final Rule does not refer to "principles of accountability" *per se*. The phrase is used here to refer to the broad types of requirements contained in the Final Rule.
[166]Final Rule, § 164.520.

In general, a covered healthcare provider must obtain an individual's consent, in the manner prescribed by the Final Rule, prior to using or disclosing PHI to carry out treatment, payment, or health care operations.[167] Should an organization wish to use PHI for a purpose not covered by consent, it needs to obtain an authorization from the individual for such a use.

When using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.[168]

In addition, the Final Rule imposes baseline organizational standards that must be implemented by covered entities. These include:

- physical and organizational systems to ensure the safety and security of PHI;
- a process by which internal privacy policies are to be created, implemented and amended;
- a process whereby individuals can complain about the entity's PHI practices; and
- the designation of a privacy officer charged with ensuring the entity's compliance with the Final Rule and that employees are properly educated about the entity's privacy practices.

8.6.3 The Results

Complying with the substantive requirements of the Final Regulation has proved challenging to many of the organizations covered by it. As a result, the deadline for compliance has been extended. It will therefore be sometime before we will be able to ascertain the practical effects of a fully implemented HIPAA.

[167] *Ibid*. at § 164.506.
[168] *Ibid*. at § 164.502.

8.7 Accountability Lessons for the Critical Information Infrastructure

Sector stakeholders' offered opinions about accountability lessons that were associated with the initiatives described previously. We merged these opinions with our own to suggest ways in which these lessons *may* apply to the Critical Information Infrastructure. These might prove valuable.

8.7.1 Y2K

There are a number of significant differences between the Y2K problem and the challenge of increasing the reliability, availability and security of the Critical Information Infrastructure. The implications for what will be required to maintain our Critical Information Infrastructure are serious:

- We do not yet understand what is required to maintain[169] our Critical Information Infrastructure;
- What is required to maintain the Critical Information Infrastructure will change[170] over time;
- There is no deadline for establishing measures to protect our Critical Information Infrastructure;
- In many cases, we do not have the required technical solutions[171]; and
- Maintaining Canada's Critical Information Infrastructure will critically depend on foreigners.[172]

Our collective success with Y2K can be a source of some pride, but we should resist the temptation to assume that the same approach would be successful if used to protect Canada's Critical Information Infrastructure.

Although the approaches that succeeded in dealing with Y2K may not be particularly applicable to the Critical Information Infrastructure, Y2K provides an excellent example of how a serious perceived threat can galvanize both the public and private sector to effective action.

[169]There is a two-fold challenge. We have yet to identify the services that must be provided by our Critical Information Infrastructure. And we have yet to determine what is required to maintain those yet to be identified services.
[170]The Y2K problem could be localized to existing computer programs. The services require by our Critical Information Infrastructure will change over time and the technology deployed to provide those services will change.
[171]We cannot even agree about the technical and social means that should be employed to solve the problem of Spam (unsolicited bulk commercial email). Yet Spam is a clear and immediate irritant to all Internet email users.
[172]Our Information Infrastructure has connections and interdependencies across the globe. We have little option but to conform to established standards and conventions. Many of these "rules" will be set by bodies and within social groups where Canada has only a minor role to play.

8.7.2 Treadway Commission/Sarbanes-Oxley

The Treadway Commission teaches us that understanding a serious potential problem is not enough. Even identifying a solution does not, in itself, do any good. The solution must be implemented. This takes resources and will, neither of which is easy to generate in the absence of a disaster. When a disaster happened in the form of a series of major financial scandals that included Enron and WorldCom, the resources and will were quickly forthcoming. Sarbanes-Oxley was the result.

There is general agreement that major disasters are likely in the Critical Information Infrastructure. If or when they occur, significant will and resources to increase the reliability of the Critical Information Infrastructure may become available. Those parties with ideas for or interest in specific actions to increase the reliability of the CII may be wise to lay the groundwork for their initiatives in preparation for opportunities to present them. In addition, efforts that quantify and demonstrate the potential for disaster in the hope of stimulating proactive action, as was done for Y2K, might be useful.

8.7.3 EU Directive/PIPEDA

Initiatives in one jurisdiction can not only improve things in that jurisdiction, but also can spawn corresponding positive initiatives in other jurisdictions. Canada's Critical Information Infrastructure is interconnected with and dependent on, the global Information Infrastructure. This does not mean that Canada cannot unilaterally initiate positive changes within our own portion of the Information Infrastructure. These changes may ripple outward to other jurisdictions to everyone's benefit.

8.7.4 HIPAA

Many make the argument that economics must drive all significant change. HIPAA proves that this is not true. Initiatives that are unpopular and expensive with corporations can still succeed if they have enough popular support. Changes to the accountability framework for Critical Information Infrastructure may add more costs than profits, but the HIPAA experience indicates that this may only be one factor in deciding on action, and not the decisive factor.

9.0 Current Common Accountability Mechanisms

Although the Information Infrastructure is a single system, it can be viewed as being composed of five types of components:

1. Software Products
2. Custom Software
3. Systems
4. IT Services
5. Hardware

In this section we present accountability mechanisms that apply to all five types of components.

9.1 Indemnification

"Indemnity" may be defined in the following manner:

> An indemnity is a specific type of contractual risk allocation mechanism whereby one party to a contract agrees to hold the other (and presumably innocent) party harmless if a third party brings a claim against the innocent party.[173]

An alternate definition is as follows: "An agreement whereby one party agrees to secure another against an anticipated loss or damage".[174]

Indemnification may be used to describe a variety of legal obligations. Although an indemnity has been compared to a contractual insurance policy, this description is not technically accurate from a legal or practical standpoint. Indemnification is primarily concerned with risk management. Certain indemnities are based upon the aforementioned 'innocent party' description, while others are based upon the occurrence of an event. With respect to the 'innocent party' variety of indemnity, somebody is being sued – not because he or she knowingly committed any wrongdoing, but rather on the basis that he or she used, licensed and paid for something that another party alleges should be licensed from them.[175]

The other type of indemnification, sometimes known as an 'event indemnity,' is more closely related to the pure allocation of risk. In other words, if I cannot perform a service, I will arrange to have somebody else perform this service and I will pay any incremental amounts you incur due to my non-performance. In addition, I agree to hold you harmless from any damages you may have to pay to another party in order to obtain the same service. Most indemnification clauses offered by licensors in their standard forms agreements are of the 'innocent infringer' variety.

---

[173]Joseph Rosenbaum, "Protect Thyself 101: A primer on indemnification," *ZD Net Tech Update*, (18 February 2004), online: ZD Net Tech Update. <http://techupdate.zdnet.com/techupdate/stories/main/indemnification_primer.html>.

[174]*The 'Lectric Law Library Lexicon, s.v.* "indemnity," online: The Lectric Law Library <http://www.lectlaw.com/def/i027.htm>.

[175]Rosenbaum, *supra* note 173.

There are other factors that should be considered before one accepts a provider's offer for indemnification:[176]

1. Is the indemnity restricted to certain kinds of claims, such as patent or trademark infringement only? Or does it extend to copyright infringement, which enjoys worldwide protection?
2. Are there geographic/territorial limitations to the indemnity (e.g. is the indemnification limited to claims brought in Canada only)?
3. Is the indemnification clause comprehensive, (i.e. will it defend you, indemnify you and hold you completely harmless from any and all damages and losses, including legal fees) or does it limit you to a set dollar amount?
4. Does the indemnity clause limit damages to those "actually and finally awarded by a court", or does it also cover all ancillary expenses associated with the litigation?
5. If the contract in question contains a limitation of liability clause (a clause that says, in effect, no matter what happens, the maximum we will pay is "X" dollars), is the indemnification capped by that limit?
6. If a claim is covered by insurance, does this coverage overlap or conflict with the indemnification clause?

The aforementioned discussion illustrates that the subject of indemnification is quite complex. Ideally, indemnification provisions should be customized depending on the situation under consideration.

In the businesses supporting the Critical Information Infrastructure, indemnification is used to transfer risk between customers and vendors. Risk and accountability are interchangeable here for purposes of this discussion. Indemnification clauses occur in licenses or contracts for software products, custom software, systems and IT services.

A current high-profile example of indemnification in the software realm is the Linux community's response to SCO's claims that Linux infringes on certain copyrights held by SCO in respect of the UNIX operating system. In order to ease customer concerns about potential liability, including legal defence costs, several Linux vendors, either singly or in concert, are proactively offering to indemnify customers against these costs. While indemnification clauses have had a high profile in the news media recently owing to the Linux/SCO disputes, indemnification has had a function in almost all IT and technology contracts for many years.[177]

For illustrative purposes, an indemnification clause (from RealNetworks Inc., for its RealOne Player software) is reproduced here:[178]

---

[176] *Ibid*.
[177] *Ibid*.
[178] RealNetworks Inc. *End User License Agreement* (2004), online: Network Computing News <http://www.ncns.com/RealNetworksLicense.html>.

> 11. INDEMNIFICATION. This Software and the Services are intended for use only with properly licensed media, content and content creation tools. It is your responsibility to ascertain whether any copyright, patent or other licenses are necessary and to obtain any such licenses to serve and/or create, compress or download such media and content. You agree to record, play back and download only those materials for which you have the necessary patent, copyright and other permissions, licenses and/or clearances. You agree to hold harmless, indemnify and defend RN [RealNetworks], its officers, directors and employees, from and against any losses, damages, fines and expenses (including attorneys' fees and costs) arising out of or relating to any claims that you have (i) viewed, downloaded, encoded, compressed, copied or transmitted any materials (other than materials provided by RN) in connection with the Software in violation of another party's rights or in violation of any law, or (ii) violated any terms of this License Agreement. If you are importing the Software from the United States, you shall indemnify and hold RN harmless from and against any import and export duties or other claims arising from such importation.

9.2 Tort Law

9.2.1 Introduction to Tort Law

Tort is derived from the Latin word *tortus*, which means crooked or twisted. The word was introduced into early English as a synonym for the word 'wrong'.[179] In French, the word "tort" also means a "wrong". Tort law refers to that facet of the law, which will allow an injured person to obtain compensation from the person who caused the injury.[180]

A tort is a wrongful act (other than a breach of contract) for which relief may be acquired in the form of damages or an injunction. The function of the law of tort is to discourage wrongful conduct and to compensate those who are harmed by such conduct.[181] Whereas the law of contract is based largely upon obligations imposed by bargain or negotiation, the law of tort derives from duties of care imposed by law. Perhaps the best overall definition of tort law offered to date is the following: "A tort is a civil wrong, other than a breach of contract, which the law will redress by an award of damages."[182]

Every individual is expected to behave in a manner that does not injure others. When one does cause injury to others, either intentionally or by negligence, he or she can be required by a court to pay money to the injured party (damages) so that, ultimately, he or she will be accountable for the pain caused by the tortious action. Compensation is probably the most important social role of tort law.[183]

---

[179]Allen M. Linden, *Canadian Tort Law*, 5th ed. (Toronto: Butterworths, 1993) at 1.
[180]Lloyd Duhaime, "Tort Law in Canada-An Introduction," *Duhaime's Law Dictionary*, (2004), online: Tort & Personal Injury <http://www.duhaime.org/Tort/ca-negl.htm#general>[Duhaime "Tort Introduction"].
[181]Cynthia A. Patterson & Stewart D. Personick, eds., *Critical Information Infrastructure Protection and the Law*, (Washington, D.C.: The National Academies Press, 2003) at 45, online: The National Academies Press <http://books.nap.edu/catalog/10685.html>[Patterson & Personick, Critical Information Infrastructure Protection and the Law].
[182]Linden, *supra* note 179 at 1-2.
[183]Duhaime "Tort Introduction", *supra* note 179.

9.2.2 Negligence

The law of negligence is an important element of the law of tort. As was stated almost 150 years ago in an English case:

> Negligence is the omission to do something which a reasonable man, guided upon those considerations which ordinarily regulate the conduct of human affairs, would do, or doing something, which a prudent and reasonable man would not do. The defendants might have been liable for negligence, if, unintentionally, they omitted to do that which a reasonable person would have done, or did that which a person taking reasonable precautions would not have done.[184]

The fundamental principle of negligence law is known as the 'neighbour principle'. It was first espoused by Lord Atkin in the seminal United Kingdom decision of *Donoghue v. Stevenson*,[185] in order to outline a "general conception of relations giving rise to a duty of care, of which the particular cases found in the books are but instances."

Lord Atkin stated:

> The rule that you are to love your neighbour becomes in law, you must not injure your neighbour; and the lawyer's question, Who is thy neighbour receives a restricted reply. You must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour. Who, then, in law, is my neighbour? The answer seems to be—persons who are so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question.[186]

This idea has provided guidance for later court decisions, which have generally stated that a duty arises wherever some harm is reasonably foreseeable, unless valid policy reasons are present from denying such a duty.

The Supreme Court of Canada refined the test of duty into a two-step approach in the case of *Kamloops* v. *Nielsen*,[187] where the Court distilled the test into two branches:

> (1) Is there a sufficiently close relationship between the parties... so that, in the reasonable contemplation of the defendant, carelessness on its part might cause damage to that person. If so,
>
> (2) are there any considerations which ought to negate or limit
>
> (a) the scope of the duty and
> (b) the class of persons to whom it is owed or
> (c) the damages to which a breach of it may give rise?

This two-stage approach has been consistently followed in other Supreme Court of Canada decisions.[188]

---

[184] *Blyth v. Birmingham Water Works* (1856), 11 Ex. 781.
[185] *Donoghue v. Stevenson* [1932] A.C. 562 (H.L.).
[186] *Ibid*. at 580.
[187] [1984] 2 S.C.R. 2, at 10.

The law of negligence states that a person who causes harm (the defendant) to another individual (the plaintiff) for failing to conform to a reasonable standard of care will be liable to the plaintiff for the damages caused to the plaintiff – assuming that it is determined that the defendant owed the plaintiff a duty of care. Generally, in order to recover damages in tort, the plaintiff must demonstrate that the defendant was negligent.

9.2.3 Criteria to Establish Negligence

In order to establish a cause of action for negligence, there are several elements that must be present.[189] In his text, *Canadian Tort Law*, the Honourable Mr. Justice Allen M. Linden mentions six criteria that must be present to establish a cause of action for negligence:

1. The claimant must have suffered some damage;
2. The damage suffered must be caused by the conduct of the defendant;
3. The conduct of the defendant must be negligent (i.e. in breach of the standard of care as established by the law);
4. There must be a duty recognized by the law to avoid this damage;
5. The conduct of the defendant must be a proximate cause of the loss (in other words, the damage should not be too remote a result of the defendant's conduct); and
6. The conduct of the plaintiff should not be such as to bar recovery, i.e. the plaintiff must not be guilty of contributory negligence and must not voluntarily assume the risk[190]

In general, before liability in negligence can be established, a plaintiff must substantiate all the necessary elements to support its claim.[191]

The courts generally determine what the reasonable standard of care is for any given fact situation. If this standard has not been satisfied, the court will then ascertain who is entitled to be compensated for the defendant's failure to comply with the standard. A primary goal of

---

[188]These decisions include *B.D.C. Ltd.* v. *Hofstrand Farms Ltd*., [1986] 1 S.C.R. 228, at p. 243 (per Estey J.); *Just* v. *British Columbia* (1989), 64 D.L.R. (4th) 689 (S.C.C.); *Rothfield* v. *Manolakos* (1989), 63 D.L.R. (4th) 449 (S.C.C.) (per Cory J.), etc.

[189]There is a modicum of disagreement over the actual number of the required elements. The traditional British approach to negligence liability, also known as the "A.B.C. rule", requires the plaintiff to establish three things as part of a negligence action to the satisfaction of the court: (a) a duty of care exists; (b) there has been a breach of that duty; and (c) damage has resulted from that breach. However, this simple approach does not adequately deal with the issue of the extent of liability.

American scholars [*Prosser and Keeton on the Law of Torts*, 5th ed. (1984)] have suggested that four elements are necessary to establish a cause of action for negligence:

(a) duty; (b) failure to conform to the required standard; (c) a reasonably close causal connection between the conduct and the resulting injury (sometimes referred to as "proximate cause"); and (d) actual damage or loss resulting to the interest of another individual. However, this scheme can also result in difficulties. A court may sometimes interpret the proximate cause issue in terms of duty or remoteness, which results in a blending of the first and third elements. In addition, courts sometimes confuse duty with failure to conform to the standard required. Furthermore, this approach disregards the consideration of the plaintiff's conduct as an element to be considered in establishing the cause of action.

[190]Linden, *supra* note 179 at 93.

[191]Patterson & Personick, *supra* note 181 at 45-46.

negligence law is to encourage more prudent behaviour through the adoption of cost-effective measures so as to avoid scenarios that result in damage.

9.2.4 Tort Law and the Critical Information Infrastructure

The operation of the Information Infrastructure can give rise to a number of issues within the sphere of the law of negligence. There are questions that relate to negligence with respect to the manufacture of computer and information-based products, especially in the light of the ever-shortening product cycles. Other negligence-related questions may arise in relation to the fact that error-free software remains an unattainable goal (at least for the foreseeable future).[192] In addition, the utilization itself of computers and information-based products can result in negligence.

In reality, there have been few reported cases related to negligence claims brought against the manufacturers and developers of elements of the Critical Information Infrastructure, such as computers, software and other information-related products. One of the reasons for this is that for the most part, any harm caused by malfunctions in these products has been largely restricted to economic loss, rather than injury to persons or physical property damage. Therefore, most claims against vendors have been brought in contract (a branch of the law that is more amenable to compensating for pure economic loss).[193]

Another factor that makes it difficult to apply negligence principles to the Critical Information Infrastructure is the problem of determining what standard of care to apply to the development of a computer system or software program. First, there are no uniform licensing or certification requirements for software engineers or developers. Second, there are no general standards in place for software programming, design or testing (e.g. there is nothing analogous to the CICA Handbook used by the accounting profession). As a result, there are no widely accepted standards among software professionals with respect to how much testing a new product should undergo or how many errors can exist per line of code before a product is released for commercial distribution.[194]

With respect to deliberate attacks against the Critical Information Infrastructure, such as distributed denial-of-service attacks, it is evident that the hacker responsible for the harm should be held liable in tort. However, the more difficult question is whether negligence liability should also be applicable to those entities, such as companies, vendors, service providers, universities, individuals, and so on, whose systems or products were accessed or utilized in the attack and who neglected to take reasonable steps to protect against misuse of their networks prior to the attack.[195] There have been no cases of this type in Canada, and to date no U.S. court has addressed the question of liability for failure to secure a computer network adequately. It is conceivable that if tort law is found to apply to issues of computer security with respect to the Critical Information Infrastructure, then the potential for lawsuits with their commensurate

[192]George S. Takach, *Computer Law*, 2d ed. (Toronto: Irwin Law, 2003) at 457.
[193]*Ibid*. at 459.
[194]*Ibid*.
[195]Patterson & Personick, *supra* note 181 at 45.

damages awards could encourage investment in greater Information Infrastructure security measures.

Another area of uncertainty with respect to the applicability of tort law is whether recovery of damages should be allowed from a company whose networks were improperly secured and were subsequently utilized by a third party to cause harm. As previously stated, to recover damages in tort, a plaintiff must demonstrate that the defendant was negligent. However, with respect to the aforementioned required elements necessary to establish a cause of action for negligence, the plaintiff would have some difficulty satisfying all these requirements in the network security fact scenario mentioned above. This is because there is currently no legal duty that exists between a service provider and other unrelated (or 'downstream') parties on the Internet. If such a duty were to be acknowledged in the future, it would have to be based upon a public policy decision that such victims require legal redress, the foreseeability of risk of harm to the victim, an ability on the part of the defendant to lessen or control the risk of harm and a finding that the defendant was the party best suited to protect against the harm.[196]

There have been some cases in the U.S.[197] that have considered the issue of foreseeability of harm to third parties in the context of computer networks. Decisions in these cases turn on the question of whether or not the defendant *knew or should have known* that certain wrongful conduct was occurring on its networks (as opposed to 'likely to occur'). Although these cases were decided in different contexts – mainly copyright infringement and defamation law – the legal principles are transferable and applicable. The decisions suggest that holding defendants liable for harm resulting from known, yet unaddressed, network security vulnerabilities would be a rational and logical extension of current legal doctrine. Following this line of reasoning, if a service provider knows or should have known that its networks are being utilized to cause harm (and has the capability to prevent such harm from occurring), the organization may be required to take steps to stop such harm from occurring. Supporters of the application of tort liability to the Critical Information Infrastructure state that the organizations that control the computer networks are in the best position to initiate and apply appropriate security measures and can implement these measures at the lowest cost.

Tort law could also function as a motivating factor and important accompaniment to the setting of industry-wide standards and best practices, since compliance with such standards normally demonstrates that due care has been exercised.[198] If negligence liability were to be recognized as being applicable to this area, then an organization could minimize its liability through the implementation of security standards. At the moment, however, there is no apparent duty of care nor is there a uniformly recognized standard of care in the area of computer/network security. Furthermore, the selection of such a standard would entail much complexity owing to the evolving nature of security vulnerabilities, as well as the huge diversity of entities that make up the Critical Information Infrastructure.

---

[196]*Ibid*. at 46.
[197]*Cubby* v. *CompuServe*, 776 F. Supp. 135 (S.D.N.Y. 1991); *Stratton Oakmont* v. *Prodigy*, 1995 WL 323710 (N.Y.Sup.Ct.); *RTC* v. *Netcom* , 907 F. Supp. 1361 (N.D.Cal. 11/21/95); *A&M Records, Inc*. v. *Napster, Inc*., 239 F.3d 1004 (9th Cir. 2001); *Cyber Promotions* v. *Apex Global Information Services*, 61997 WL 634384 (E.D. Pa. 1997).
[198]Patterson & Personick, *supra* note 181 at 51.

For example, a ‘reasonable care’ standard might include the practice of promptly installing and applying security patches. However, it would be difficult to decide the frequency with which such patches should be applied to meet such a standard. In addition, although a patch might close one vulnerability in a system, it could result in a new vulnerability surfacing. With respect to tort law, should an organization that installs a patch that leaves its system more vulnerable be deemed to be negligent? Also, patches sometimes lead to other errors in the system by creating other vulnerabilities. Might it not sometimes be more prudent to delay installing a patch until it can be shown that it is ‘safe’ to install?

Another unanswered question is whether all entities within the Critical Information Infrastructure should be held to the same standard of care with respect to computer network security. In tort law, the determination of negligence liability often depends on which parties are in the best position to prevent the harmful events from occurring. In the case of distributed denial-of-service (DDoS) attacks, Internet service providers (ISPs) occupy a unique position in preventing or mitigating harm resulting from DDoS attacks. This is because they can isolate certain network attacks as these attacks enter their system. Although ISPs could deter and cut off attacks, they currently have little incentive to do so. The implementation of better network security protocols would raise expenses and could degrade overall network performance, resulting in disgruntled customers. On the other hand, DDoS attacks result in disgruntled customers. Because ISPs are largely unregulated, there are no formal standards for security or reliability of service to which they must adhere. Thus, their responses to incidents such as network attacks are variable and depend largely upon the ISPs’ own discretion and competitive market forces.[199]

Some legal commentators have argued that that ISPs should face substantial negligence liability for insecure systems and networks, owing to the fact that ISPs know (or should know) about the inherent risks and possess the capability to mitigate or stop DDoS attacks. On the other hand, some ISPs argue that they should be immune from liability for hostile traffic running through their networks on the ground that they are merely common carriers of signals.

[199] *Ibid*. at 53.

9.3 Criminal Law

Criminal law is one of the clearest mechanisms for accountability assignment and enforcement. The true nature and quantum of computer crime are not precisely delineated. With respect to the level of such crimes, precise and dependable statistics are difficult to obtain. There are two main reasons for this. First, a certain proportion of nefarious computer-related activity is difficult to detect. Second, many victims, even when they become aware of a crime, are reluctant to report it because of potential negative impacts on their reputation with customers and investors. However, it is a well-established fact that computer crime represents a significant and increasing problem.

One definition of computer crime is "any illegal, unethical, or unauthorized behaviour involving automatic data processing and/or transmission of data."[200] An alternate definition of computer crime, used by the RCMP, is "any illegal act which involves a computer system whether the computer is the object of the crime, an instrument used to commit a crime or a repository of evidence related to a crime".[201] From these definitions (as well as from others), it can be seen that computer crime covers a very broad area.

Within the purview of the criminal law (as it relates to current accountability mechanisms), we have identified three major players:

1. The Lawmakers
2. The Enforcers
3. The Criminals

Each group will be discussed in the context of accountability.

9.3.1 The Lawmakers

Criminal law in Canada is primarily under the purview of the Canadian *Criminal Code*. In essence, the *Criminal Code* defines the behaviour that society, acting through Parliament, has deemed to be socially unacceptable.[202] The sections of the *Criminal Code* that are most relevant in charging and prosecuting individuals who utilize computer technology for unauthorized gain, destruction, manipulation, intrusion, or attempt to distribute socially unacceptable images or speech include the following: theft, fraud, computer abuse, data abuse, obscenity/child pornography, hate propaganda and interception of communications. In addition, depending upon the nature of the crime and the extent to which the Information Infrastructure played a role in the commission of the particular offence, other offences in the *Criminal Code* may be applicable from time to time.

It is useful to note that customarily, criminal law in general has dealt with the protection of tangible property and the safety of the individual. However, because the Information Infrastructure is characterized by rapid technological change, combined with the ephemeral and

[200]Ulrich Sieber, *The International Emergence of Criminal Information Law* (Koln: Heymanns, 1994) at 5, cited in Takach, *supra* note 192 at 209.
[201]Takach, *supra* note 192 at 209.
[202]See Kent Roach, *Criminal Law* (Toronto: Irwin Law, 1996), at 2: "Criminal laws are primarily designed to denounce and to punish inherently wrongful behaviour and to deter people from committing crimes or engaging in behaviour that presents a serious risk of harm."

elusive qualities of information, lawmakers have faced a substantial challenge in updating and revising the *Criminal Code*, so as to be able to effectively deal with the novel mischiefs possible resulting from the utilization of computers and networks.[203] Several amendments to the *Criminal Code* in recent years have computer-related provisions. However, the increasing use of computers and the Internet, along with the increased dependence upon the Information Infrastructure, has and will likely continue to raise difficult questions and present challenges under both the new and older clauses of the *Criminal Code*. To maintain an adequate level of accountability, lawmakers will likely have to review relevant sections of the *Criminal Code* on a regular, ongoing basis in order to keep pace with technological changes.

We should also note that lawmakers can be heavily influenced by political pressures. In addition, notwithstanding what new laws are passed relating to the Information Infrastructure, judges are free to apply and interpret these laws on a case-by-case basis, depending on the facts of each individual case, and the decisions of courts in other jurisdictions.[204]

9.3.2 The Enforcers

In the total scheme of enforcement of all crimes, the importance of cyber crimes depends upon the type and severity of the actual criminal offence under consideration. With respect to many of these types of offences, especially those that involve the use of the Internet, a major factor is the availability of resources to properly conduct the investigation. In addition, the quantum of resources expended upon the enforcement of a particular type of cyber-criminal offence tends to be commensurate with society's perception of the importance of deterring the particular offence.[205]

For example, the protection of children has been deemed by our courts and government to be a paramount consideration in allocating funds and services for deterring criminal activity for crimes against children. Child pornography, for instance, can now be easily transmitted throughout the world via the Internet. This accessibility has had an impact upon the amount of resources allocated to fighting such crimes. As a result, it is not uncommon for police departments to have task forces set up to monitor and investigate the possession and distribution of child pornography throughout the Internet, and to work hand-in-hand with other jurisdictions within Canada and internationally in fighting this type of crime.

Due to limited resources, our police departments also rely on the public and corporate community to assist in fighting cyber crimes. The fight against credit card fraud, for instance, is a joint effort between the credit card companies, the community and the police departments. At the top of this chain are the internal auditing departments of the credit card companies that detect and monitor fraudulent activity. Conversely, when police departments become aware of credit card scams they will contact the credit card companies and credit card owners. Finally, all credit card holders have an obligation to monitor their own credit card activity and report any fraudulent activity as soon as they become aware of it.

---

[203] Takach, *supra* note 192 at 228.
[204] Interview of Keith L. Geurts, Associate, Gowlings Lafleur Henderson (26 February 2004) [Geurts interview].
[205] *Ibid*.

Under the *Criminal Code*,[206] certain offences have minimum sentences that must be imposed. For such offences, such as driving while impaired, society has made it a mandatory condition that a convicted first offender will be given a criminal record, driving suspension and a fine. The presiding judge does not have the discretion to impose a lower sentence. However, there are no minimum sentences with respect to fraud. As with all crimes that do not require a minimum sentence, much variation exists between different judges and different jurisdictions with respect to sentencing for fraud offences. This can lead to a general attitude of leniency on the part of certain judges when hearing computer-related crimes. For example, with respect to offences involving 'script kiddies', judges will often impose extremely lenient sentences, such as conditional or absolute discharges, community service, and so on. The rationale usually given to support this leniency is that the accused did not realize the harm that the malicious code would cause, or the judge will cite a lack of true malicious intent. In addition, the perpetrator's young age, as well as a desire to not burden such an individual with the stigma of a criminal record, may represent additional factors favouring leniency.[207]

9.3.3 The Criminal

There are several significant differences between cyber criminals and criminals not involved in offences related to computers or the Information Infrastructure. First, cyber criminals do not have direct contact with their victims. They typically commit their crime at home through the screen of a computer.[208]

Second, many cyber criminals, especially the inexperienced or novice variety, do not comprehend the severity of their criminal act, or that they can actually be caught. The fact that the act itself is illegal will have little or no deterrent effect on them. What does have a deterrent effect, however, is when similar persons are caught doing similar acts, and there is a large amount of media attention surrounding that person.

A good example is provided by the recent lawsuits in the U.S. against persons who were illegally downloading copyrighted songs via peer-to-peer file sharing services. Once the Recording Industry Association of America (RIAA) cases got underway, the volume of illegal file sharing and downloading of copyrighted works plummeted.[209]

Third, the more experienced or 'professional' cyber criminals understand that it is possible to trace criminal activity done through computer networks. As a result, these criminals (who are usually highly educated and technologically sophisticated) take numerous precautions that lessen the chances of apprehension. In fact, they seem to feel, with considerable justification, that their chances of being caught and brought to justice are minimal.[210] Stricter laws with higher penalties will not likely serve as much of a deterrent to this group.

---

[206] *Criminal Code*, R.S., c. C-34, s. 1.
[207] Geurts interview, *supra* note 204.
[208] *Ibid*.
[209] *Ibid*.
[210] *Ibid*.

9.4 Insurance

Insurance was a subject that recurred many times in the course of the interviews and secondary research. It is clear to us that people expect insurance to have a major impact on the operation of accountability for the Critical Information Infrastructure. Richard Clarke, the former chairman of the President's Critical Information Infrastructure Protection Board in the United States said, "The insurance industry can play a pivotal role in securing cyberspace by creating risk-transfer mechanisms, working with the government to increase corporate awareness of cyber risks and collaborating with leaders in the technology industry to promote best practices for network security."[211]

When we spoke with insurance executives, there seemed to be significant gaps between the perspectives of the insurers, Critical Information Infrastructure users and vendors, and industry pundits. At the risk of oversimplifying the situation, we would like to offer the following thoughts:

- Many analysts seem to feel that insurance companies will be very proactive in such areas as establishing standards, product certification and user certification.
- Insurance companies on the other had, seem inclined to move very slowly and cautiously in offering insurance. This prudence is justified. "According to some, these insurance companies [that offer cyber risk insurance] are making suicidal choices. "It's a crazy move," says Catherine Hajnal, Assistant Professor of Information Systems at Carleton University's Sprott School of Business."[212] It is very difficult, if not impossible to quantify many of the risks. Also, insurers do not possess the expertise to do certifications or standards development. Nor do they have the inclination or incentive to develop this expertise.
- Users are largely uninsured against cyber risk and moreover are unaware of this gap in coverage. "Unfortunately, most companies are operating in a 21st century threat environment with 20th century insurance coverage," stated John Spagnuolo, cyber expert for the Insurance Information Institute (I.I.I.). "The dynamics of risk management have changed with technology."[213]
- Vendors are somewhat more sensitive to their risks, but are under tremendous economic pressure to minimize their insurance premiums.

Although the scope of this project does not allow us to explore this issue in depth, we felt compelled to include the following brief analysis (section 9.4.1). Also, we recommend that further work be undertaken with a view to fostering consensus about the evolution of insurance

[211]Information Insurance Institute, News Release, "Most Companies Have Cyber-Risk Gaps in Their Insurance Coverage, States The I.I.I. -- Traditional Insurance Policies Not Adequate For Cyber Exposures", (13 August 2003), online: Insurance Information Institute <http://www.iii.org/media/updates/press.731722/>.
[212]Scott Foster, "Virus victims weigh cyber-insurance options: insurance providers offer policies to cover corporate damage caused by worms such as Blaster" *Computing Canada* (3 October 2003), online: looksmart <http://www.findarticles.com/cf_dls/m0CGC/19_29/108992880/p1/article.jhtml>.
[213]John Spagnuolo, as quoted in Information Insurance Institute, News Release, "Most Companies Have Cyber-Risk Gaps in Their Insurance Coverage, States The I.I.I. -- Traditional Insurance Policies Not Adequate For Cyber Exposures", (13 August 2003), online: Insurance Information Institute <http://www.iii.org/media/updates/press.731722/ >.

with respect to the Information Infrastructure. This work would harmonize with market forces to encourage smoother, quicker development of appropriate insurance products.

9.4.1 Insurance Market Overview

Cyber insurance constitutes a very minor part of the total insurance industry. Because of this, the current state and evolution of cyber insurance is best understood within the context of the overall insurance industry. The following excellent overview of the insurance market is provided by Gaston & Associates:[214]

> Businesses will need to prepare for major changes in insurance availability and pricing. We expect that most, if not all, insurance companies will be increasing premiums during the coming year, as well as restricting certain classes of business or certain types of coverage. These are industry wide changes and not restricted to any one particular insurance company or any one particular geographic region.
>
> While the events of September 11th most definitely had an effect on insurance availability and pricing, there were changes taking place even before this event. Our economy was changing and the insurance industry was already experiencing an economic downturn.
>
> Insurance companies rely on investment income to make a profit, since premium alone is typically not adequate to pay claims. Investment income is used in calculating the rates necessary to meet claims obligations. Since the late 1980s, too much capital in the insurance industry resulted in what is known as a 'soft market', as evidenced by highly competitive pricing for commercial insurance policies. By the mid-1990s, outstanding performance in the investment market created even more competition for premium dollars among insurance companies, driving the premiums down to even lower levels. After 12 years of 'soft market' conditions, in 2001 the industry began to show signs of strain and there seemed to be pockets of activity within the marketplace that indicated that a change in the cycle might be near. As the investment market began to change, resulting in a lower rate of return for investors, insurance companies were beginning to increase rates and be more selective in the types of risks they were willing to underwrite. This condition is termed a 'hard market'.
>
> Insurance companies also purchase their own type of insurance, called re-insurance, which allows them to insure large risks and to spread the risk on smaller accounts. Re-insurance costs to insurance companies were already rising prior to September 11th, resulting in increased premiums passed on to consumers. The World Trade Center catastrophe is the largest insurance claim event in history, with estimated claims totalling in excess of $40 billion. This event sent shock waves through the entire insurance industry, including the reinsurance market and hastily sped up what was already happening in terms of rising prices. While all legitimate World Trade Center claims are expected to be paid by the insurance industry, the financial consequences of this event are enormous.
>
> Starting in 2002, re-insurance companies have sharply increased their costs to insurance companies and are refusing in certain cases to provide coverage at all on certain perils, such as terrorism. All of this is eventually passed on in some form to the insurance

[214]Gaston & Associates, Inc., "Insurance Market Hardening", online: Gaston & Associates, Inc. <http://www.gastonassoc.com/html/market_hardening.asp>.

> company's customers, across all lines of coverage. It's a simple matter of supply and demand, in this case the demand surpassing the supply.

9.4.2 The Evolution of Cyber Insurance

In the upcoming new edition of his book *Secrets and Lies*, cyber security expert Bruce Schneier says, "It's clear to me that computer security is not a problem that technology can solve. Security solutions have a technological component, but security is fundamentally a people problem. Businesses approach security [and liability] as they do any other business uncertainty: in terms of risk management." [215]

Dr. Schneier, along with many others, believes that risks will rise for businesses, because they will be held increasingly liable for the security (or lack thereof) of their products and services. This liability will fundamentally impact the way vendors and users behave.

"Business owners don't like unknowns," says Daniel Egger, President of Open Source Risk Management, "if business risks can be managed for a cost, the known cost can be factored into the cost of running the business or the total cost of ownership (TCO) of the information technology. Depending on what that cost is, everything from the budget to the price of goods or services can reflect the additional costs to manage risk."[216]

Insurance will be the principal way that organizations manage the cost of cyber risk. Bruce Schneier goes on to say:

> This [insurance] will happen automatically, because CEOs turn to insurance companies to help them manage risk and liability transfer is what insurance companies do. From the CEOs' perspective, insurance turns variable-cost risks into fixed-cost expenses and CEOs like fixed-cost expenses because they can be budgeted. Once CEOs start caring about security – and it will take liability enforcement to make them really care – they're going to look to the insurance industry to help them out. Insurance companies are not stupid; they're going to move into cyber-insurance in a big way. And when they do, they're going to drive the computer security industry... just as they drive the security industry in the brick-and-mortar world.[217]

There is abundant evidence to support the expectation of dramatic growth in cyber insurance. The Ernst & Young 2003 Global Information Security Survey[218] covered 1,400 companies. Only 7% of the respondents knew that they had specific insurance coverage for network and Internet risks. Almost one-third of the respondents thought they were covered for these risks, but actually were not. Another 34% knew that they lacked coverage and 22% admitted that they were unaware of their coverage. Ernst and Young commented that the fact that only 7% of the

---

[215]Bruce Schneier, *Secrets and Lies, Digital Security in a Networked World* 2nd ed. (Hoboken, NJ: John Wiley & Sons, forthcoming 2004).

[216]Interview of Daniel Egger by David Berlind "Instead of indemnification, consider 'open source insurance'" *Tech Update Software Infrastructure* (18 February 2004), online: ZDNet <http://techupdate.zdnet.com/techupdate/stories/main/open_source_insurance.html>.

[217]Schneier, *supra* note 215.

[218]Ernst & Young, Global Information Security Survey 2003 (New York: Ernst & Young), online: Ernst & Young <http://www.ey.com/global/download.nsf/US/TSRS_Global_Information_Security_Survey_2003/$file/TSRS_-_Global_Information_Security_Survey_2003.pdf >.

respondents had cyber insurance was "… astonishingly low, given the risk environment and the fact that general policies do not provide such coverage."

This low saturation rate, combined with increasing liabilities, makes cyber insurance growth almost certain. There are a number of barriers to cyber insurance growing as an industry: lack of actuarial data, precedent (nobody insured you for Y2K failures), and others. Perhaps the market demand will drive the innovation needed to overcome these obstacles, but definitely, that innovation will be a prerequisite to this industry taking off.

And just as there is evidence of low coverage rates, there is also evidence of increasing risk and liabilities. The CERT® Centers at Carnegie Mellon University's Software Engineering Institute track security breaches, or incidents. They report that the number of incidents grew from 21,756 in 2000 to 82,094 in 2002, a 377 percent increase.[219] Not surprisingly, 2003 and early 2004 have seen this trend continue. The damages, both direct and indirect, sustained by organizations have grown proportionately. Although there are no definitive measures, it is certain that damages run into the many billions of dollars annually worldwide.

In summary, cyber insurance can and will provide:

- Risk transfer
- Definition of best practices for risk reduction
- Incentives for the adoption of these best practices
- Improved education

The result of these four things will be improved cyber risk management and this could translate directly into a more robust Critical Information Infrastructure.

9.4.3 Cyber Risks and Cyber Insurance Overview

There are cyber insurance products available to deal with a variety of Information Infrastructure risks. For the most part, there do not seem to be standard types of policies among various companies (Errors and Omissions being a notable exception). Each company offers a selection of policies that cover one or more cyber risks. These risks/policy types include: professional errors and omissions; network security; copyright, trademark or patent infringement; destruction or corruption of data; public relations costs; criminal reward fund reimbursement; and cyber extortion.

9.4.3.1 Professional Errors and Omissions

Errors and Omissions (E&O) Insurance is the most common type of cyber insurance. An E&O policy covers the holder for negligent acts and omissions that may harm its clients. This policy typically relates to custom software and systems work and to a lesser extent IT services. It is concerned with things such as programming errors, or failure of the software or systems to perform as promised in the contract. Coverage includes both legal defence costs and judgements awarded against the vendor.

[219]CMU CERT® Coordination Center, Software Engineering Institute, Carnegie Mellon University, News Release (August 2003).

9.4.3.2 Network Security

Network security breaches are increasingly common. These allow attackers to:

- Transmit and/or install malicious code such as viruses and trojans;
- Gain unauthorized access to data that can result in breaches of privacy;
- Interrupt service causing breaches of contract; and
- Steal sensitive data.

Cyber insurance can mitigate both first-party damage and third-party damage.

9.4.3.3 Copyright, Trademark or Patent Infringement

As explained in section 9.1, vendors are increasingly being required to indemnify their customers against copyright, trade mark or patent infringement. The reason for this trend is that over the last few years, there has been an alarming increase in the number of lawsuits in this area. This increase has been especially evident in the United States. There has also been a significant increase in the value of the judgements being awarded. As in other types of cyber insurance, policies typically cover both the costs of defence and judgements, up to specified limits.

More recently, there is a second type of cyber insurance being offered in this area. It is referred to as a pursuit policy and it helps to pay legal expenses of suing an alleged infringer.

9.4.3.4 Destruction or Corruption of Data

Data is arguably the most valuable asset in the Critical Information Infrastructure. Systems can usually be replaced, albeit with some pain. Data is often much less replaceable. Cyber insurance can mitigate the financial loss resulting from the loss or corruption of data arising from either malicious activity or accident.

9.4.3.5 Public Relations Costs

Many cyber crimes and accidents associated with the Information Infrastructure go unreported by the victims. One of the main reasons for this is victims' concern over loss of reputation with customers, investors, employees and regulators. The financial consequences can be far greater than the direct losses from the incident. Post-incident public relations initiatives are both necessary and expensive.

9.4.3.6 Criminal Reward Fund Reimbursement

If an organization is the victim of a malicious incident, it is occasionally desirable to post a reward for information leading to the arrest and conviction of the individual or individuals responsible. Such a reward may form part of a public relations initiative, as well as acting as a deterrent against future incidents. For example, the SCO Group recently offered a reward in connection with the Mydoom virus.[220] It is possible to obtain cyber insurance that will mitigate the cost of such a reward under certain circumstances.

---

[220]Ken Mingis, "SCO Offers $250,000 Reward for Arrest of Mydoom Worm Author" *ComputerWorld* (27 January 2004), online: ComputerWorld <http://www.computerworld.com/securitytopics/security/virus/story/0,10801,89470,00.html>.

9.4.3.7 Cyber Extortion

Cyber extortion is growing quickly. The most common form is a threatened Distributed Denial of Service (DDoS) attack that will bring down a victim's Web site. The most popular targets are sites where there is a high loss per minute of downtime. Internet gambling sites are among those most threatened.[221] These attacks are almost impossible to defend against if they are well executed. There was a recent DDoS attack on the Web site of the SCO Group. The details of the attack were known in advance, including the precise time the attack would occur. In spite of this foreknowledge, the attack was successful in disabling the site.

9.4.4 ISO 17799

In Section 9.4.2, we mentioned that one of the main things that will be driven by insurance is the definition of best practices. This is already happening. One of the leading examples is the evolution of the Code of Practice for Information Security Management established by the International Organization for Standardization (ISO), referred to as the ISO 17799 Standard. This extensive security standard directly addresses cyber security practices. It forms the basis of online and onsite security assessments conducted by insurance companies such as American International Group (AIG). AIG writes 70% of the cyber insurance policies in the United States, as well as a large number in Canada. We felt that it would be useful to provide a brief overview of ISO 17799 to give a taste of the many other standards that we feel will evolve in the future. The description below comes from Risk Associates:[222]

> ISO17799 is a detailed security standard. It is organized into 10 major sections, each covering a different topic or area:
>
> 1. Business Continuity Planning
> The objectives of this section are: To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.
>
> 2. System Access Control
> The objectives of this section are: 1) To control access to information 2) To prevent unauthorised access to information systems 3) To ensure the protection of networked services 4) To prevent unauthorized computer access 5) To detect unauthorised activities. 6) To ensure information security when using mobile computing and tele-networking facilities
>
> 3. System Development and Maintenance
> The objectives of this section are: 1) To ensure security is built into operational systems; 2) To prevent loss, modification or misuse of user data in application systems; 3) To protect the confidentiality, authenticity and integrity of information; 4) To ensure IT projects and support activities are conducted in a secure manner; 5) To maintain the security of application system software and data.
>
> 4. Physical and Environmental Security
> The objectives of this section are: To prevent unauthorised access, damage and interference to business premises and information; to prevent loss, damage or

---

[221] Paul Roberts, "Super Bowl fuels gambling sites' extortion fears" *InfoWorld* (29 January 2004), online: InfoWorld <http://www.infoworld.com/article/04/01/29/HNsuperbowl_1.html>.

[222] Risk Associates, cited in *The ISO 17799 Service & Software Directory*, ISO 17799: What Is It?, (2004), online: ISO 17799: What Is It? <http://www.iso17799software.com/what.htm>.

compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities.

5. Compliance
The objectives of this section are: 1) To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements; 2) To ensure compliance of systems with organizational security policies and standards; and 3) To maximize the effectiveness of and to minimize interference to/from the system audit process.

6. Personnel Security
The objectives of this section are: To reduce risks of human error, theft, fraud or misuse of facilities; to ensure that users are aware of information security threats and concerns and are equipped to support the corporate security policy in the course of their normal work; to minimise the damage from security incidents and malfunctions and learn from such incidents.

7. Security Organisation
The objectives of this section are: 1) To manage information security within the Company; 2) To maintain the security of organizational information processing facilities and information assets accessed by third parties; and 3) To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

8. Computer & Operations Management
The objectives of this section are: 1) To ensure the correct and secure operation of information processing facilities; 2) To minimise the risk of systems failures; 3) To protect the integrity of software and information; 4) To maintain the integrity and availability of information processing and communication; 5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure; 6) To prevent damage to assets and interruptions to business activities; and 7) To prevent loss, modification or misuse of information exchanged between organizations.

9. Asset Classification and Control
The objectives of this section are: To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

10. Security Policy
The objectives of this section are: To provide management direction and support for information security.

Within each section are the detailed statements that comprise the standard.

10.0 Current Focused Accountability Mechanisms

In the previous section we discussed accountability mechanisms that apply to all the types of components (software products, custom software, systems, IT services and hardware) that make up the Information Infrastructure. In this section we discuss accountability mechanisms that apply to predominantly one type of component. These are discussed under the subsections dedicated to the components to which they best apply.

In sections 10.1, 10.2, and 10.3 we have somewhat arbitrarily chosen three points on the software spectrum involving increasing levels of accountability complexity: products, custom programs and systems. The differences between these points are significant enough that there is a change in the feel of the accountability from one to the next.

10.1 Software Products

The business of selling software is fundamentally different from other endeavours in several significant ways, some of which have accountability and legal consequences. First, software is characterized by short product cycles (as are other components of the Critical Information Infrastructure). Partially as a result of this fact, 'perfect' software cannot be produced (i.e. it will always include some 'bugs' or errors). Second, as is true for other computer-related products, the channels of distribution for software are complicated and multifaceted.[223] Third, software is not sold. Rather, it is licensed.

The majority of software products have relatively short shelf lives (i.e. for any specific version of the product). Unlike many other industry sectors, advances and innovations in the software industry tend to occur in weeks or months, instead of in years. In addition, the software industry is characterized by a high level of competition, with many new products constantly being introduced to the market. When combined with the short product cycles, this situation frequently results in unreasonably excessive expectations on the part of the end user. The software vendors, who are under continual pressure to stay ahead of the competition, often assert that users purchase new products and upgrades for enhanced features, rather than for improved quality and reliability.[224]

Software creation typically consists of several distinct stages, starting with the original high-level planning and design, progressing through the writing of code for the instructions and statements and ending with final testing to discover and correct as many errors as possible prior to delivery to the end user.[225] Although most software undergoes a substantial amount of testing, it is an accepted fact among programmers and developers that it is effectively impossible to discover and eradicate all the errors prior to shipment. Despite good intentions, defective code is still the bugbear of the software industry. According to the Standish Group (a market research firm), bad

[223]Takach, *supra* note 192 at 423.
[224]Aaron Ricadela, "The State of Software Quality," *Information Week.com News*, (21 May 2001), online: Information Week Web Site http://www.informationweek.com/shared/printHTMLArticle.jhtml?article=/838/quality.htm> [Ricadela, "Software Quality"].
[225]Takach, *supra* note 192 at 425.

code accounted for as much as 45% of computer system downtime and cost U.S. companies over $100 billion in lost productivity and repairs (year 2000 figures).[226] It should be noted that this $100 billion does not include the cost of losing disgruntled customers. In the words of Alan Willett, a software process engineer at Xerox Corp., "Absolutely, the commercial off-the-shelf software products we purchase don't have the quality we need."[227]

Even if it were possible to design bug-free software,[228] it would be so prohibitively expensive and time-consuming so as to make it commercially unfeasible in the light of the current commercial environment. Thus, one of the current accountability mechanisms in place is that of support programs offered by software vendors to the user. A major constituent of these programs involves correction of errors that manifest themselves after the customer has started using the software product. Another aspect of a typical end-user software support program is the furnishing of future versions or upgrades of the software. Although the principal *raison d'être* for the existence of such ensuing versions is to provide the consumer with additional and/or enhanced features, these upgrades are also utilized as a vehicle to distribute new copies of the previous software with some of the bugs removed.[229]

10.1.1 Limitations of Liability and Warranty Disclaimers

Software that is created for mass-market distribution (as contrasted with custom-designed software) typically contains license terms, together with various warranty disclaimers and limitations on liability (invariably in favour of the software vendor). For illustrative purposes, relevant portions of End User License Agreements ('EULAs') from Apple Computer, Inc.[230] and Microsoft[231] are reproduced below:

> **SINGLE USE LICENSE AGREEMENT FOR APPLE COMPUTER, INC.**
>
> PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") BEFORE USING THE SOFTWARE. BY USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE.
>
> 6. Disclaimer of Warranties. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE APPLE SOFTWARE IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU. EXCEPT FOR THE LIMITED WARRANTY ON MEDIA SET FORTH ABOVE AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE APPLE SOFTWARE IS PROVIDED "AS

[226]Ricadela, "Software Quality," *supra* note 223.
[227]*Ibid*.
[228]Definitions of bad software vary, but it is generally accepted that it only requires three to four defects per 1000 lines of code to result in a poorly performing program. For every 10 lines of code written, the average programmer injects one error. When one considers that many commercial software applications contain millions or tens of millions of lines of code and that it costs software vendors at least 50% of their development budgets to fix errors during the testing phase, the huge scope of the problem becomes apparent.
[229]Takach, *supra* note 192 at 426.
[230]Apple Computer, Inc. Software License Agreement (3 December 2003), online: Apple Computer, Inc. Support - Software License Agreement <http://docs.info.apple.com/article.html?artnum=26275>.
[231]Microsoft, Inc., END-USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE - TrueType core fonts for the Web EULA (28 December 2001), online: Microsoft Typography <http://www.microsoft.com/typography/fontpack/eula.htm>.

IS", WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND APPLE AND APPLE'S LICENSORS (COLLECTIVELY REFERRED TO AS "APPLE" FOR THE PURPOSES OF SECTIONS 6 AND 7) HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE APPLE SOFTWARE, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF ACCURACY, OF QUIET ENJOYMENT, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. APPLE DOES NOT WARRANT AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE APPLE SOFTWARE, THAT THE FUNCTIONS CONTAINED IN THE APPLE SOFTWARE WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE APPLE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE APPLE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY APPLE OR AN APPLE AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE APPLE SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, SO THE ABOVE EXCLUSION AND LIMITATIONS MAY NOT APPLY TO YOU.

7. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL APPLE BE LIABLE FOR PERSONAL INJURY, OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR USE OR INABILITY TO USE THE APPLE SOFTWARE, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF LIABILITY FOR PERSONAL INJURY, OR OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Apple's total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of fifty dollars ($50.00). The foregoing limitations will apply even if the above stated remedy fails of its essential purpose.

END-USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE

IMPORTANT-READ CAREFULLY: This Microsoft End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Microsoft Corporation for the Microsoft software accompanying this EULA, which includes computer software and may include associated media, printed materials and "on-line" or electronic documentation ("SOFTWARE PRODUCT" or "SOFTWARE"). By exercising your rights to make and use copies of the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, you may not use the SOFTWARE PRODUCT.

> LIMITED WARRANTY
>
> NO WARRANTIES. Microsoft expressly disclaims any warranty for the SOFTWARE PRODUCT. The SOFTWARE PRODUCT and any related documentation is provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties or merchantability, fitness for a particular purpose, or noninfringement. The entire risk arising out of use or performance of the SOFTWARE PRODUCT remains with you.
>
> NO LIABILITY FOR CONSEQUENTIAL DAMAGES. In no event shall Microsoft or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this Microsoft product, even if Microsoft has been advised of the possibility of such damages. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

The paragraphs reproduced above are representative of almost all commercial off-the-shelf software. As can be seen, accountability with respect to product liability is virtually nonexistent. Statutes that relate to the sale of goods are approximately 100-years old. The sales statutes in the Canadian common law provinces are modelled upon the original English *Sale of Goods Act*, which was intended to codify sales laws applying to goods being produced in English factories of the late 1800s. Thus, it is not illogical that these sale of goods statutes are not compatible with the problems raised by computer software sales. To all intents and purposes, these statutes relate to the sale of tangible goods and thus do not often effectively address issues surrounding intangible software and other information-based products, particularly where the software is not 'sold', but rather licensed. Because of this, most software vendors expressly disclaim all implied warranties and conditions in their licence agreements.

Many software vendors contend that the end users cause many of their own problems by heavily customizing their software application products.[232] Since vendors realize that software can be utilized in so many different ways by the purchaser, they provide a general limitation of liability in the contract of sales with the user. These limitations usually restrict their liability to a fixed dollar amount for direct damages and exclude all other damages, such as lost profits and consequential damages. Furthermore, courts in a broad range of situations have not been willing to impose unlimited liability on the vendors of information-based goods and services, including software, especially for pure economic loss.[233]

It is instructive to note that most software is produced by teams of diverse individuals, rather than by single programmers working alone. This is significant, in that the task of assigning accountability for problems inherent in the software becomes exacerbated and obscured. Accountability for faults, which is traditionally implicit in a single individual, is not easily extrapolated to collective groups.[234] Although this problem of collective responsibility (also known as 'the problem of many hands') is not unique to software itself, it is highly relevant, as

[232]Ricadela, *supra* note 224.
[233]Takach, *supra* note 192 at 477-480.
[234]Helen Nissenbaum, "Computing and Accountability," (1994) 37 *Communications of the ACM 72*.

most software is produced in institutional settings. (Collective responsibility is a problem that afflicts other technologies, as well as large corporations, governments and the military.)

Another aspect of this accountability problem is related to the fact that software is frequently assembled out of modules or segments. It may include code from previous versions, or utilize code from entirely different software. With respect to software that has evolved to a high level of complexity, no single individual who grasps the entire program may exist, let alone one who can keep track of all those who have contributed to its various components. Thus, responsibility and/or liability of errors or malfunctions is further obscured.[235] (For example, the initial release of Microsoft Windows 2000 contained approximately 40 million lines of code. Since the industry standard for software produced by companies such as Microsoft is one known bug or defect for every 1500 lines of code, one could expect approximately 600,000 bugs in the program.) [236]

10.1.2 Some Divergent Views on Software Liability Allocation

The issue as to whether the prevailing allocation of liability is appropriate, as between the manufacturers and the consumers of software, continues to be the subject of considerable debate.[237] The lack of consensus and significantly differing positions taken by various commentators on this issue cogently illustrates the need for a systematic framework for discussion, including reliable empirical data to inform that discussion. Arguments about whether this allocation can or should be changed using private or public sector mechanisms, or some combination of the two, become relevant in a number of circumstances. These include when the discussion of the allocation of liability arising from security breaches surfaces; and when such breaches involve questions of software reliability.

For example, one author[238] argues that it is not practical for consumers to create their own security software. He further contends that it is reasonable for manufacturers to be liable for the reliability of their products.

Other authors[239] have argued that imposing liability is not the appropriate tool for reducing the number and severity of adverse security events caused by software problems. According to this line of reasoning, software should be treated differently than other products (for example, automobiles). Among the reasons cited, are:

1. The relatively short expected useful life of many software products compared to the time required to dispose of a dispute in the courts (i.e. the software would be obsolete before the case was finally decided);

---

[235] *Ibid*.
[236] "Changes in the Customer Support Industry" *Computer News* (January 1999), online: Help Desk Solutions, Inc. <http://www.helpdesksolutions.com/Publications/change_support.htm >.
[237] See, for example, Nancy R. Mead, *International Liability Issues for Software Quality*, Special Report, CERT Research Center, CMU/SEI-2003-SR-001, (July 2003) at 19, online: Carnegie Mellon Software Engineering Institute <http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03sr001.pdf>.
[238] Daniel J. Ryan, "Two Views on Security Software Liability: Let the Legal System Decide." IEEE Security & Privacy 1, 1 (2003): 70-72.
[239] See, for example, Carey Heckman, "Two Views on Security Software Liability: Using the Right Legal Tools." IEEE Security &Privacy 1, 1 (2003): 70-72, online: <http://csdl2.computer.org/dl/mags/sp/2003/01/j1073.htm>.

2. The purposes for which software will be used cannot, in many cases, be reasonably predicted by the manufacturer; and

3. If liability were to be imposed upon software manufacturers, many of them would exit the market and thus we would see a reduction in the degree and pace of innovation.

Both sides of this debate are invoking, at least implicitly, standard examples of economic reasoning. They are making assumptions about the state of the market, or about the likely outcome of changes, that, to some degree, are empirically testable.

In any case, this debate about the appropriate allocation of liability to software manufacturers, for damages arising from adverse security-related incidents caused by software inadequacies, is a subset of the following problem. The more general issue concerns the appropriate allocation of liability of both software and hardware manufacturers for damages that arise in connection with various kinds of events, whether or not they are adverse security-related events.

We think that this debate would benefit from the rigorous application of standard economic reasoning. Although this analysis is outside the scope of this report, in performing it, we feel it may be prudent and efficacious to incorporate data that is collected from various further research endeavours that are suggested throughout this paper.

10.2 Custom Software

10.2.1 Custom Software Defined

Custom software, also sometimes called custom programming, is based on an organization's specific requirements. Today, almost no custom software is completely original. Elements from previous efforts are re-used to increase productivity. In general, there is a higher level of expectation that custom software will better meet the purchasers' requirements than software products. Custom software forms a substantial part of the Information Infrastructure.

10.2.2 Software Development Contracts

We have confined ourselves to examining accountability mechanisms that operate where custom software is developed for an organization that will use it (the purchaser), by an arms-length party (the vendor). Some custom software is still developed in-house by employees of the organization that will subsequently use the software. We have not considered the accountability mechanisms governing such custom software. They are highly variable and frequently ill-defined.

A software development contract documents an agreement between a purchaser and a vendor to build and develop an application or system required by the purchaser in accordance with some mutually acceptable specifications. The accountability mechanisms for custom software are enshrined in the contract.

Key contract provisions relating to accountability include:

- Scope of work, including functional and technical specifications
- Indemnification against IP infringement
- Milestones, timelines and associated penalty clauses
- Acceptance criteria
- Acceptance testing procedures
- Pre- and post-implementation services

Most contracts for custom software have a services component. It often includes implementation, integration, training and support. We discuss these services in section 10.4.

10.2.3 How Accountability Fails

A massive amount of effort has been expended on drafting custom software contracts. These contracts governed the thousands of custom software development initiatives that have been undertaken. As a result, we have a large body of knowledge about what works (and what doesn't) in assigning and enforcing accountabilities. Many problems can be traced back to a common source: the failure of both the vendor and the purchaser to put enough effort and resources into the pre-development contract phase of the relationship.

One of most frequent problems occurs when both parties do not have a clear and common understanding of what is required by the purchaser. This understanding is only likely to occur if requirements are spelled out in detail in the contract at the time of signing. Often in the desire to get projects started, contracts are signed with Schedules 'to be developed'. These schedules can encompass key contract elements such as technical specifications and project schedules. This is a recipe for disaster. Perhaps surprisingly, the development of detailed functional and technical specifications is extremely difficult, as evidenced by how often it is not done.

Another common accountability problem arises when acceptance testing procedures for modules, the overall system, and final acceptance are not adequately specified in the contract. Disputes are frequent when agreements on these procedures are absent.

Schedule slippage also often causes the failure of custom software development projects. Vendors and purchasers often succumb to the pressure to agree to predefined deadlines, even though these deadlines are neither necessary nor realistic. The resulting stress can cause corners to be cut and eventually lead to chaos.

Payment methods can create major problems. If vendors are paid on a time and materials basis, there is an inherent misalignment of goals between the vendor and the purchaser.

A final situation worth mentioning is that vendors occasionally find that they simply cannot deliver on the contract requirements. Vendors frequently go out of business, or do not have assets or ability to remediate deficiencies. Problems that are identified some time after the contract is complete are often very difficult to rectify because of poor documentation and/or access to original talent that may no longer be available.

10.3 Systems

10.3.1 Systems Defined

The Information Infrastructure is composed of many layers of interconnected systems. These systems may be standard or custom components, or groups of components. The process of building systems is referred to as systems integration.

Systems integration includes designing system architectures, identifying the hardware and software products that will be incorporated into the system, identifying the interface points between elements of the system and specifying them in detail, building the custom code that connects the system elements and whole system testing to ensure that the system meets specifications.

In the beginning, systems integration was a highly manual and custom process. Components were not designed to work together. Getting them to do so was difficult. In response to market demand, integration software was developed to aid the effort of combining components into a working system. This traditional integration software, or middleware, was used to connect packaged or custom applications. Despite being expensive and difficult to use, middleware was a considerable improvement over fully manual integration.

We are now witnessing the emergence of a new class of products that make systems integration much easier by leveraging emerging cross platform standards such as Web services, extensible markup language (XML), and Java Connector Architecture. Gartner calls these products Enterprise Service Buses (ESBs). They define ESBs as "a new architecture that exploits Web Services, messaging middleware, intelligent routing and transformation. ESBs act as a lightweight, ubiquitous integration backbone through which software services and application components flow."[240]

As systems integration becomes easier and more affordable, the demand continues to grow. Organizations want and need their systems to be connected in real-time into the overall Information Infrastructure.

10.3.2 Key Integration Enabling Standards

Key standards are accelerating the pace of systems integration and at the same time allowing users to develop integration strategies that do not rely on a single vendor. Some of these standards are:

1. The Java Connector Architecture – addresses the first problem of getting information out of or into applications. This provides a single standard that complements the mix of existing standards such as JDBC (Java Database Connectivity) or RMI (Remote Method Invocation) and a wide-range of vendor supplied APIs (Application Program Interfaces) that provide a good starting point.

[240]Roy Schulte, Gartner Inc., as quoted by Ronan Bradley, "The Universal Enterprise Service Bus", PolarLake JIntegrator White Paper (3 January 2004), online: PolarLake <http://www.polarlake.com/products/jintegrator/whitepaper/>.

2. XML addresses the biggest problem of any integration project: how do I get the message into the right format for its next destination? While XML doesn't remove the need to transform messages, it has significantly reduced the complexity associated with it.
3. Web services offer standardized interfaces between applications and also the possibility of standardized orchestration.
4. The Java Messaging Service (JMS) provides the asynchronous communication protocol, with the added advantage of guaranteed delivery of publish/subscribe capabilities typically provided by JMS-supported messaging products such as IBM's WebSphere-MQ.[241]

10.3.3 Systems Integration Contracts

Systems integration efforts are usually governed by contracts containing provisions very similar to those for custom software development. However, there are some differences.

Systems integration projects often result in systems with very broad scope and impact on the purchaser's organization. Consequently, the vendor is frequently held partially accountable for delivering business results and not just functionality. Performance clauses can talk to such things as cost savings and revenue increases.

Because of the complexity of systems integration efforts, clarity in requirement definition assumes a much larger importance. Requirements are much more encompassing. Vendors cannot be knowingly blind to business requirements.

Hardware and software products are frequently encompassed in system integration projects. Contracts must contemplate who owns (and who pays for) these products in the event that the contract is terminated early and the system is never completed.

10.3.4 How Projects Fail

Here again, there are many similarities between how systems integration efforts fail and how custom software development projects fail. Also as with contracts, there are some differences.

Vendors frequently exhibit resistance to assuming the accountability associated with giving representations and warranties on the performance of the overall system. Such performance is difficult to predict in advance because of the complexity of interaction between the components. Also, it may not be possible to remedy performance shortfalls using the chosen components and architecture. Because there is often no clear accountability, the resulting system may fail to deliver the benefits desired by the purchaser.

Many of the components in typical systems are standard products. New versions of these products are constantly being released. This happens both during the development and implementation phases and post implementation. It is virtually impossible to predict the impact of installing new versions of components. Systems integration vendors frequently are forced to

[241] *Ibid*.

adopt workarounds to cope with undocumented component features encountered during projects. These features may change in subsequent versions and may impact negatively on the system. In the case of custom software development, the vendor can exert significant control over the development environment and these types of problems are much rarer.

10.4 IT Services

Many internal service providers deliver as much as they can with the resources available to them. A budget is struck for the service and then the service group works out what it has the resources to deliver. That's what happens with most internal services in organizations. That's also what happens with most internal IT service groups. It's a 'best effort' kind of accountability – comfortable and under increasing challenge.

10.4.1 ITIL

There is an emerging international standard for IT service management. It's based on the Information Technology Infrastructure Library, or ITIL.[242] This began as a 1989 effort by the UK government to assemble a useful collection of best practices for supporting and delivering IT services, hence the Library part of its name. Their goal was to provide a tool the help governments improve the way IT services were obtained.

Today, ITIL is supported by an international user forum – the IT Service Management Forum or itSMF.[243] There is an active itSMF branch[244] in Canada with chapters across the country. Several units of the Canadian federal government have joined itSMF Canada as have several provincial governments.[245] ITIL is in the process of becoming an international standard. BS 15000[246] is the related British standard – "BS 15000 is the world's first standard for IT service management … and is based heavily upon the ITIL (IT Infrastructure Library) framework."[247]

ITIL has set the standard for IT service accountability. Its adoption is far from universal, but it has been used widely enough that we know it works in Canada. This section provides an introduction to IT service accountability as seen through the ITIL framework. Fundamental to effective accountability is having a standard against which to measure and assess performance. Under the ITIL framework, Service Level Agreements (SLAs) provide that referent.

10.4.2 Service Level Agreements

ITIL assumes that there are two parties involved with an IT service. There is an IT service provider and an IT service client. Both provider and client may be in the same organization, but it's useful to treat them as separate parties. The SLA for an IT service is the contractual

---

[242]There is a large and growing literature about ITIL. See, online: <http://www.ogc.gov.uk/index.asp?id=2261> as a useful initial pointer into the literature.
[243]See, online: IT Service Management Forum <http://www.itsmf.com/>.
[244]See, online: itSMF Canada <http://www.itsmf.ca>.
[245]See, online: <http://www.itsmf.ca/corporate.asp> for a recent list of corporate members of itSMF Canada.
[246]See, online: BS15000 – The BS 15000 IT Service Management Standard <http://www.bs15000.org.uk/>.
[247]*Ibid.*

understanding between provider and client of exactly what is to be delivered, how, where, when, under what conditions and based on what assumptions.

A full table of contents for an SLA should include:[248]

- Description of the services to be provided
- Performance commitment, with tracking and reporting
- Procedures to follow for problem management
- Full description of fees and allowed expenses
- Client duties and responsibilities
- Security, backup, recovery and continuity
- Warranties offered and available remedies
- Intellectual property rights and confidentiality
- Contractual compliance and resolution of disputes
- Procedures to follow upon termination

When both parties are in the same organization (typical for an internal IT service department) many of these items can be covered by standard agreements. The goal is not to produce a fat SLA document that exhaustively covers each IT service. Rather, the goal is to establish clear accountabilities between provider and client. An internal SLA need be little more than a one-page memo of agreement which lays out what is to be provided and who has what responsibilities.

There are several points that can be made about how this approach works in practice.[249] The first critical point is that if an aspect of an IT service isn't being measured, then it's not really all that important. People pay attention to what's being measured, and it's common to find providers who optimize their performance in order to achieve the best possible score on what's being measured. Those service aspects which are not being measured, however important they may be in theory, will be ignored under the regular pressures of service delivery.

Clients are often attracted to the idea that providers should be held responsible for the full cost of any failure to meet contractual terms and conditions. In the presence of a significant failure, the provider could find itself facing a guaranteed loss on the service. Because of stringent contractual terms, there may be nothing that can be done by the person in charge can turn around or reduce the loss. That becomes a powerful de-motivator. Remedies should be structured so that the provider always has an incentive to try harder.

We have the knowledge required to establish effective SLAs for IT services. ITIL does provide useful guidance. There are many outsourcing[250] IT service contracts that claim to follow the ITIL

---

[248]Developed from the "Service Level Agreement Toolkit", EasyTec Solutions, 2002.

[249]Two of the contributors to this document, Mark Stirling and Robert Fabian, have significant practical experience with IT service delivery and with SLAs. The points to be raised are largely drawn from that Canadian and international experience.

[250]"Purchasing a significant percentage of intermediate components from outside suppliers". This definition appears in *Campbell R. Harvey's Hypertextual Finance Glossary*, online: <http://www.duke.edu/~charvey/Classes/wpg/bfgloso.htm>.

framework. Notwithstanding the existence of ITIL and similar best practices, "a Gartner study says half of this year's [2003] outsourcing projects will be labelled as losers by top decision makers."[251] There are many factors that contribute to this high expected failure rate. One of the key challenges is that the IT service required will change, but we don't have effective ways to modify accountabilities to track the service changes. We may want to consider how IT service accountabilities can be effectively changed to track changes in the IT services to be provided.

10.5 Hardware

10.5.1 Hardware Defined

The Information Infrastructure is composed of computer system components and communications systems components. All the critical infrastructures that depend upon the Critical Information Infrastructure (e.g. the electric power grid, the financial services sector, etc.) depend upon telecommunications – the public telecom network, the Internet and satellite as well as land-based wireless networks. The hardware assets include the computers and peripheral equipment, routers, switches, etc. The communications-related hardware components include the transmission lines of various types, comprised primarily of traditional wire and cable, as well as fibre-optic lines. In addition, there are the communications satellites and their associated uplink and downlink equipment.

10.5.2 Hardware Accountability Mechanisms

10.5.2.1 Implied Warranties and Conditions

Unlike software, which is typically licensed, computer hardware may be sold outright pursuant to an agreement of purchase under which the purchaser obtains title to the equipment. Alternatively, computer hardware may be rented or leased, pursuant to an agreement that permits the user to utilize the equipment for a certain time period in return for a periodic fee.

All the common law provinces have sale of goods statutes that include several warranties and conditions. These are normally implied into all sale of goods contracts. However, they may be expressly disclaimed, except when sales to consumers are involved.[252] In such cases (e.g., where PCs are sold for home use), most provincial consumer protection laws often contain specific rules with respect to consumer warranties and may disallow the disclaiming of implied warranties and conditions as contained in the Sale of Goods statutes.[253] Although personal computers and associated equipment are contained in the greater Information Infrastructure, for the purposes of this report, the Critical Information Infrastructure will be deemed not to include computer hardware and associated products purchased for home (non-business) use. However, home computers may represent a risk (so far unquantified) of being hijacked for purposes of DDoS, penetration redirection, spam serving, etc. Thus, while not part of the Critical Information Infrastructure, home computers can impact on the Critical Information Infrastructure.

---

[251] Gregg Keizer, "Outsourcing: A 50-50 Proposition" *InformationWeek* (26 March 2003), online: Information Week <http://www.informationweek.com/story/IWK20030326S0006>.

[252] Note: In certain jurisdictions, the implied warranties and conditions contained in the Sale of Goods statutes cannot be disclaimed when sales to 'consumers' (i.e., non-business entities) are involved).

[253] Takach, *supra* note 192 at 473.

With respect to hardware sales (in contrast to software), there is no confusion as to whether or not this involves a sale of a good. For example, the Ontario *Sale of Goods Act*[254] contains the following definition for "goods":

> "[G]oods" means all chattels personal, other than things in action and money and includes emblements, industrial growing crops and things attached to or forming part of the land that are agreed to be severed before sale or under the contract of sale;

It is quite obvious that an item of computer hardware or related communications equipment falls clearly within the purview of this *chattels personal* definition of goods. Thus, since the Sale of Goods legislation applies to the hardware under consideration, several implied warranties and conditions will apply to the hardware sale unless there is a specific agreement to the contrary. First, if the vendor is a merchant and the goods are purchased from a description provided by the vendor who deals in goods meeting the description, then the products supplied must be of 'merchantable quality' (i.e., suitable for their intended purposes).[255]

The second significant implied warranty and condition states that where:

1. the buyer relies upon the skill and the knowledge of the vendor,
2. and the vendor has specific knowledge of the purpose for which the goods will be used at the purchaser's premises,

then the vendor must deliver goods that are fit for their purpose.[256] For this second implied warranty and condition to apply, the vendor must be informed to the user's specific requirements. As an example of the above, in the case *Saskatoon Gold Brokers* v. *Datatec Computer Systems Ltd*.,[257] the Court held that the vendor of a computer system was not liable for the system's failure to perform a crucial function. This was because the vendor was never informed of the need for such a function by the purchaser – the vendor was not told that the inventory management aspect of the business included a manufacturing component – something that the computer system did not support.
In an Ontario decision, *Classified Directory Publishers* v. *Image Management Technologies Inc*.,[258] a vendor was found not liable under section 15(1) of the Ontario *Sale of Goods Act* (the fitness for purpose warranty and condition section). The supplier had sold an optical disk drive storage device that failed to work properly with the buyer's existing computer hardware.

---

[254]R.S.O. 1990, Chapter S.1.

[255]For example, the Ontario *Sale of Goods Act* states in section 15(2),

> Where goods are bought by description from a seller who deals in goods of that description (whether the seller is the manufacturer or not), there is an implied condition that the goods will be of merchantable quality, but if the buyer has examined the goods, there is no implied condition as regards defects that such examination ought to have revealed.

[256]For example, see section 15(1) of the Ontario *Sale of Goods Act*, which reads:

> Where the buyer, expressly or by implication, makes known to the seller the particular purpose for which the goods are required so as to show that the buyer relies on the seller's skill or judgment and the goods are of a description that it is in the course of the seller's business to supply (whether the seller is the manufacturer or not), there is an implied condition that the goods will be reasonably fit for such purpose, but in the case of a contract for the sale of a specified article under its patent or other trade name there is no implied condition as to its fitness for any particular purpose.

[257]*Saskatoon Gold Brokers* v. *Datatec Computer Systems Ltd*.. (1986), 55 Sask. R. 241 (Q.B.).

[258][1995] O.J. No. 36 (Gen. Div.).

However, the purchaser had failed to inform the vendor as to for what purpose that it required the disk drive. The vendor's drive was designed for secondary online storage, whereas the purchaser required primary online storage. The Court ruled that the vendor was not liable for or responsible for this disparity. In justifying its decision, the Court stated:

> The plaintiff chose the defendant's equipment without fully informing the defendant of the purpose to which it would be put and without sufficient expertise on its own part and without relying upon consultants which were available to it for that purpose. It has not been established that the failure of the system can be ascribed to the equipment supplied by the defendant. There is no evidence that it would be impossible to determine the reason for such a failure. The essential elements needed to invoke the warranty protection under section 15 have therefore not been established.

On the other hand, in cases where the purchaser informs the vendor for what purpose the product is required and the supplier indicates that the product can meet this specific need, then a court will uphold the implied warranties and conditions as to fitness of purpose, as stated in the statute.

The Sale of Goods statutes include a further accountability mechanism that can apply to hardware. Specifically, these sales statutes consider the question of when the purchaser is deemed to have accepted the goods from the vendor (assuming that this is not specifically addressed in a written contract). The significance of this is that once the product is accepted, the purchaser is typically limited to monetary damages in the event of a subsequent hardware malfunction. In contrast, before the product has been deemed to be accepted by the buyer, the purchaser is entitled to the remedy of rescinding the sale and receiving a full refund.[259]

10.5.2.2 Limitations on Liability

Although generally done in the case of software, vendors of hardware may sometimes disclaim all implied warranties and conditions in the contract of sales. A more likely scenario in the case of hardware is where the vendor will provide a general limitation of its liability in the sales contract. For example, the hardware vendor may restrict its responsibility for direct damages to a fixed dollar amount. Other damages, such as lost profits or consequential damages, may be excluded. The rationale for this is typically that a purchaser may use the computer hardware for a wide variety of tasks or functions. Some of these uses may never have been anticipated by the vendor and other uses may entail a high degree of risk.

10.5.2.3 Express Warranties

In contrast with warranties that are implied by common law or convention, express warranties are spoken or written promises by a vendor about what will happen if the product is defective.[260] Some sales contracts will include express warranties. This is often prudent, in the light of the custom in the computer industry to disclaim implied warranties and conditions. These express warranties often run in conjunction with acceptance testing provisions. If the acceptance test requirements are not satisfied by the vendor, the purchaser is often entitled to explicit remedies.

---

[259]Takach, *supra* note 192 at 474.

[260]Crawford, C. Merle, C. Anthony Di Benedetto and Roger J. Calantone. *New products Management*. New York: Irwin McGraw-Hill, 2000.

10.5.3 Wireless Hardware

Wireless communications hardware presents some unique accountability problems and challenges in the broader context of the Critical Information Infrastructure. This equipment includes the communications satellites and associated devices, the hardware that comprises wireless data networks (e.g. wireless modems, wireless routers, base station transmitters, etc.), as well as microwave relay systems (transmitters, receivers and associated hardware).

All wireless hardware devices share a major attribute that impacts upon accountability – that is, they are subject to uncontrollable and frequently unpredictable potentially detrimental influences. These 'Acts of God' include solar storms and flares, other electromagnetic (EM) disturbances of cosmic origin, extreme adverse meteorological events, etc. Communications satellites themselves are subject to additional unpredictable hazards, such as meteor strikes or collision with space debris.

Owing to these factors, wireless hardware suffers from an inherent lack of predictability of bandwidth availability. This makes it virtually impossible to guarantee a specified level of uptime and reliability. This is not the usual case for wired devices, for which specific uptime levels can generally be assured (or at least predicted). In addition, although one can design various redundancies into wired systems, this is not possible with respect to a totally wireless piece of hardware, since it will always be susceptible to the above-mentioned EM disruptions.

In the light of the rapid growth and importance of wireless technology, it is essential that appropriate accountability mechanisms be established and implemented for wireless hardware devices. However, a detailed investigation of such accountability mechanisms is outside the scope of this report, but could be a topic for future research and investigation.

10.5.4 Standards

The ability to establish, refine and enforce accountability requirements depends upon and requires the capacity to quantify and assess the requirements against a benchmark or standard. Standards facilitate these requisite measurements. A number of different standards have evolved with respect to wireless equipment. These include standards established by the Canadian Standards Association (CSA), Industry Canada and Health Canada.

Some of the CSA standards that wireless hardware is subject to include the following:

- CAN/CSA-CEI/IEC CISPR 22-02: Information Technology Equipment – Radio Disturbance Characteristics – Limits and Methods of Measurement
- C22.2 NO. 98-1954 (R2002) – Construction and Test of Power-Operated Radio Transmitters
- C108.8-M1983 (R2000) – Limits and Methods of Measurement of Electromagnetic Emissions From Data Processing Equipment and Electronic Office Machines

- C22.1 SB-02 – Canadian Electrical Code, Part I (19th Edition), Safety Standard for Electrical Installations[261]

Wireless hardware is also affected by Industry Canada standards, including the revised Radio Standards Specifications (RSS). Such equipment is required to meet certain minimum radio frequency standards such as out-of-block emission limits and frequency drift tolerance. As stated in the Industry Canada publication, Spectrum Management and Telecommunications Policy:

> These standards will be developed in consultation with industry and the appropriate Radio Standard Specification (RSS) will be revised accordingly. Vendors will be required to certify compliance to the revised RSS specifications for equipment under Industry Canada's technical acceptance certification process.[262]

Some of the Industry Canada standards that apply to wireless hardware include the following:

- (RSS) Radio Standards Specification for Local Multipoint Communications Systems in the 28 GHz Band and Point-to-Point and Point-to-Multipoint Broadband Communication Systems in the 24 GHz and 38 GHz Bands (Provisional RSS-191)
- RSS-195 – Wireless Communications Service Equipment Operating in the Bands 2305–2320 MHz and 2345–2360 MHz
- RSS-192 – Fixed Wireless Access Equipment Operating in the Band 3450–3650 MHz
- RSS-210 – Low Power Licence-Exempt Radiocommunication Devices (All Frequency Bands)
- ICES-003 – Digital Apparatus (This Interference-Causing Equipment Standard sets out the technical requirements relative to the radiated and conducted radio noise emissions from digital apparatus.)

Finally, wireless hardware is subject to Health Canada standards, such as *Limits of Human Exposure to Radiofrequency Electromagnetic Fields in the Frequency Range from 3 kHz to 300 GHz – Safety Code 6.*[263] The aim of this standard or Code is to set out safety requirements for the installation and use of radio frequency (RF) and microwave devices that operate in the frequency range from 3 kHz to 300. This frequency range includes many of the wireless hardware devices that form part of the Critical Information Infrastructure.

---

[261]Canadian Standards Association, Endorsed Standards (2004), online: Canadian Standards Association-Electrical/Electronics Standards and Communications Standards Web Pages <http://www.csa.ca/standards/electrical/Default.asp?language=English> and <http://www.csa.ca/standards/communications/Default.asp?language=English>.

[262]Industry Canada, "Policy and Licensing Procedures for the Auction of the 24 and 38 GHz Frequency Bands" *Spectrum Management and Telecommunications Policy* (29 May 1999), online: Industry Canada Strategis Web Site <http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/vwapj/AUCTIONS9.PDF/$FILE/AUCTIONS9.PDF>.

[263]Health Canada, *Limits of Human Exposure to Radiofrequency Electromagnetic Fields in the Frequency Range from 3 kHz TO 300 GHz - Safety Code 6* (17 October 2002), online: Health Canada Consumer Clinical Radiation Protection Web Page <http://www.hc-sc.gc.ca/hecs-sesc/ccrpb/publication/99ehd237/toc.htm>.

11.0 Current State of Information Infrastructure Accountability

On one level, this can be a very brief section of the report. Almost no one accepts accountability for the delivery of end-to-end public service on Canada's Information Infrastructure. Participants carefully limit, restrict and circumscribe the accountability they are prepared to accept. It is nevertheless true that there are a large number of recognized stakeholders in our Information Infrastructure. They see the current dangers facing Canada's Information Infrastructure and have opinions about what can, should, or must be done about our Critical Information Infrastructure.

We begin by describing the 10 key perceptions that came to the surface during our primary stakeholder interviews and in our extensive review of the secondary literature. This paints a useful picture of what the Information Infrastructure stakeholders believe about the current state and future prospects of this key national resource. This section of the report concludes with material relating accountability concerns with the governance approaches, which have traditionally been followed with respect to the Internet, nationally and internationally.

11.1 Stakeholder Perceptions

11.1.1 Open to Attack

All the stakeholders we interviewed felt that there were good and proper reasons to be apprehensive about the state of Canada's Critical Information Infrastructure. Opinions did vary somewhat. Some stakeholders felt that the Internet, and by extension Canada's Information Infrastructure, was inherently insecure and unreliable. One person went so far as to advise that our really Critical Information Infrastructure should be kept completely separate from the larger Internet.

The 'optimists' felt that there were things that Canada could do to improve the reliability, availability and security of our Critical Information Infrastructure. Even they were not convinced that there was a sufficiently strong public concern to galvanize Canada to action in time to prevent major future failures of our Critical Information Infrastructure.

11.1.2 Future Failure Likely

Virtually everyone we interviewed felt that a major failure in Canada's Critical Information Infrastructure was likely… *within the next five years!* That, more than any other single observation from our primary (and secondary) research, is cause for serious concern. The problems are widely recognized. There are recognized avenues of approach that Canada (and others) could follow to reduce our Critical Information Infrastructure exposures. But none of the people we interviewed believed that we would act in time to forestall a major failure within the next five years.

Will that future failure be sufficient to galvanize Canada and the world to act? If not the first major failure, then one of the following failures may move us to collective action. The short-term challenge is to identify the actions that we could take, once there is a will to act. The danger is that we will get into a situation in which action is a necessity, but the ground has not been properly prepared. We may find ourselves forced into the wrong actions.

11.1.3 Past Failures

Several observers pointed to the massive power blackout of 2003 as being caused (in part) by a failure of a key component in the North American Information Infrastructure. There is a documented case of the Slammer worm disabling a safety monitoring system at the Davis-Besse nuclear power reactor in Ohio for a period of five hours in January 2003. [264] Fortunately, the affected reactor was shut down when this happened, but it *did* happen. And it is true that the Blaster worm was just beginning to spread when the power blackout happened.[265] Could Blaster have taken down a critical monitoring system at just the right (wrong) time? Maybe.

We make no claim that the Blaster worm did cause the massive power blackout of 2003. The interesting point is that several informed observers are prepared to believe that it could have been a key causal factor. This reinforces the observations about the exposure and likely future failure of our Critical Information Infrastructure.

11.1.4 Monopoly Problems

Microsoft has been judged (by a U.S. court) to be a monopoly.[266] A strong argument has been mounted that the resulting Microsoft monoculture is a serious threat to cyber security.[267] It's an argument by analogy. Monocultures in agriculture are known to be particularly vulnerable to attack[268] and particularly unable to defend themselves from attack. The concern is that our desktop Microsoft monoculture is posing a similar threat to cyber security.

Several people interviewed pointed to the Microsoft monopoly monoculture as a danger. Even if the agriculture analogy is not accepted and not everyone accepts that argument,[269] there are still a number of dangers in a monopoly market. No vendor in a monopoly position can lightly make changes in their product(s) – too many depend on 'features' that others feel need to be corrected. We offer no conclusion about Microsoft and monocultures, but do point out that the Microsoft near monopoly on the desktop and in the office suite market may require special responses.

---

[264]See Duncan Graham-Rowe, "Electricity grids left wide open to hackers" *New Scientist Online News* (27 August 2003), online: New Scientist.com <http://www.newscientist.com/hottopics/tech/article.jsp?id=99994094&sub=Transport%20and%20Energy>.

[265]See Kayla Michaels, "Blackout 2003: Could have Been Internet Worm/Virus; Bush Blocked Funding to Protect the Grid" *OpEdNews.com* (15 August 2003), online: OpEdNews <http://www.opednews.com/michaels_blackout_2003.htm>.

[266] One of the rulings in the recent U.S. case against Microsoft was a determination of fact that Microsoft was a monopoly. See, BBC News Staff, "Microsoft vs U.S. Justice Dept" *BBC News* (23 November 1999), online: BBC News World Edition <http://news.bbc.co.uk/1/hi/special_report/1998/04/98/microsoft/201889.stm>.

[267]Geer *et al*., *supra* note 63.

[268]"The most common species of banana, which has been bred for the trait of seedlessness to the point of sterility, suffers 40 percent to 50 percent casualties from pests every year. And 85 percent of the orange trees in Brazil, the world's leading producer of the fruit, are susceptible to a mysterious blight known as *sudden death*." See Robert Lemos, "Agriculture epidemics may hold clues to Net viruses" *ZD Net Australia* (16 January 2004), online: ZD Net Australia <http://www.zdnet.com.au/news/security/0,2000061744,39115682,00.htm>.

[269]See Mike Gunderloy, "Questioning the Monoculture Argument" *ADTMAG.com* (19 January 2004), online: Application Development Trends Magazine <http://www.adtmag.com/print.asp?id=8793>.

11.1.5 International Scope

Our primary and secondary research consistently led us to the conclusion that Canada's Critical Information Infrastructure cannot be effectively separated from the global Information Infrastructure. We are not and can never be an island, secure unto ourselves in cyber-space. The world outside our boundaries will have a profound impact on what we can, should, and must do about our Critical Information Infrastructure.

One of the people interviewed, however, pointed out that this interdependence could be an opportunity for Canada to play a leading role. We could help the world discover better ways to achieve a reliable, available, and secure Critical Information Infrastructure. Quite aside from the justifiable pride that Canada could take from such a leadership role, this would also open important commercial opportunities for Canadian suppliers to help other countries with their Critical Information Infrastructure.

11.1.6 Professional Standards

The traditional professions such as medicine and accounting have established Standards of Practice, which are required of all licensed practitioners. There are a large and growing number of proposed computer and network security standards.[270] There are several certification programs for computer security professionals.[271] Several people we interviewed expressed a wish that those responsible for our Critical Information Infrastructure be held to the same kind of Standards of Practice required of traditional professionals.

Certification can help, but there is no force of law behind voluntary certification and all security certification efforts have thus far been voluntary. Canada is unlike most of our trading partners in having restricted areas of practice mandated by the provincial acts empowering professional engineering societies.[272] It would certainly be possible to imagine a Canadian future in which an appropriate engineering license is required in order to practice in the area of computer and network security. Such a move would, almost certainly, generate some considerable opposition.[273]

11.1.7 Government Skepticism

The whole history of the Internet has been one of minimum regulation. Governments have not been seen to be particularly successful when they have attempted to do anything more than provide funding for new development or for research into possible longer-term developments. It

---

[270]The range of security standards is extensive. ISO 17799 is considered elsewhere in this report. Here we would only point to COBIT (<http://www.isaca.org/>), The Standard for Information Security (<www.isfsecuritystandard.com>) and Information Technology Control Guidelines from Canada's Chartered Accountants (<http://www.cica.ca/index.cfm/ci_id/1004/la_id/1.htm>).

[271]The International Information Systems Security Certification Consortium is one of the international bodies that provides such certification. See, online: <https://www.isc2.org/cgi-bin/index.cgi>.

[272]The explanation for how it works in Alberta and Ontario can be found on the APEGGA and PEO Web sites – see, online: <http://www.apegga.org> and <http://www.peo.on.ca>.

[273]The Canadian Information Processing Society has protested moves by various engineering bodies in Canada to restrict the right to title of software engineers. See, online: <http://www.cips.ca/it/position/software/>. Similar opposition could be expected where there moves to restrict right to title, or right to practice, in computer or network security areas.

has almost been a case of, “Give us the money, but don’t bother us with your oppressive restrictions.” And, by and large, the Internet has been incredibly successful.

Many of the people who talked with us expressed deep skepticism about interventions by governments. Our point would not be that government cannot or should not regulate, but that it needs to recognize that many stakeholders view government regulation as something that should almost automatically be opposed. At a minimum, this widespread perception needs to be recognized by any plans to introduce public regulation.

11.1.8 Funding Needed

Almost in the same breath that stakeholders would oppose government regulations, they would also recognize the importance of government funding for projects and collaborative initiatives. As detailed elsewhere in this report, the Internet grew out of projects funded by the U.S. Department of Defence. And for many years, basic Internet service was heavily subsidized by the U.S. government. There is a wide-spread recognition that appropriate public project funding can lead to important and useful improvements in our Information Infrastructure. Our own CANARIE[274] is a respected example of how public funding can be embraced by our Internet stakeholders. Similar funding models could be considered in connection with Canada’s Critical Information Infrastructure.

11.1.9 Attention Required

Public money can help, but even more important is public recognition that Canada faces a number of important challenges in connection with our Critical Information Infrastructure. The public is happy to enjoy the benefits of seamless and rapid data flows make possible by our Information Infrastructure. But it’s a capability that is largely invisible to the general public. In general, the public doesn’t know or care about the enabling role of our Information Infrastructure. And the public certainly doesn’t recognize the importance of measures aimed at improving the reliability, availability and security of our Critical Information Infrastructure. The people we interviewed all recognized this as important when developing any plans in connection with our Critical Information Infrastructure.

11.1.10 External Force

The last point on our list arose from reflections on the reasons for the Y2K success – the remediation efforts resulted in very few significant Y2K failures. To a large extent, the people with direct responsibility for information systems were unable to win the full support of senior management for Y2K remediation efforts. Resources were dedicated to Y2K efforts *after* key external stakeholders began to insist on the importance of remediation. Bankers, accountants and lawyers advised or insisted that their clients pay attention to potential Y2K problems. It seemed as though everyone was concerned about Y2K.

[274] “Canada’s advanced Internet development organization is a not-for-profit corporation supported by its members, project partners and the Federal Government.” See, online: <http://www.canarie.ca/about/about.html>.

That kind of massive external force was sufficient to 'solve' the Y2K problem.[275] It would be desirable if we can avoid the need for such massive external force as the motivation to address the Critical Information Infrastructure challenge. First, the result is likely to be a significantly inefficient process – that could be quite expensive. And second, the force is only likely to come as a result of a serious failure that dramatically raises public awareness: it would be desirable if we were able to avoid such a serious failure.

11.2 The State of Accountability

The Internet largely began as a peer-to-peer sharing of resources between different networks. This was in stark contrast to the central control models then popular for other computer networks.[276] There was no central Internet authority. Yes, U.S. federal money helped make it all happen, but many of the key roles were undertaken on a voluntary basis by interested members of the Internet community.[277] This voluntary, sharing approach coloured all the early thinking about the Internet and how it should be governed. Accountability under the law was very far from the early thinking about the Internet.

Harvard law students developed an interesting snapshot of Internet governance in 2000. In the introduction to their collective paper on this topic they pose a basic question about what is required by the Internet:

> As the Internet's promise as a transformative cultural, economic and political phenomenon has become more widely recognized, increasing attention has been paid to the question of whether we need Internet governance and, if so, in what form. Do we need a formal governance structure or will informal means of governance – namely behavioural norms established by the Internet community or by the code itself – suffice?[278]

[275]Given the massive pressure applied, it's not surprising that there was some considerable inefficiency in how organizations tackled their Y2K problems. In a perfect world, just a bit less pressure may have resulted in greater efficiency, but too much less pressure could have left us with major Y2K problems.

[276]IBM's System Network Architecture was then one of the leading network architectures. It had an IBM mainframe computer at its logical heart. "A seven-layer networking protocol. Each layer of the protocol has a set of associated data communication services. The services of the uppermost layer are embodied in a Logical Unit (LU). Each LU type defined in SNA has its own specific set of services available to an end user for communicating. The end user may be a terminal device, or an application program. The SNA structure enables the end user to operate independently, unaffected by the specific facilities used for information exchange." See, online: <http://edocs.bea.com/elink/elinkjam/v411/jamug/gloss.htm>.

[277]For many years, the University of British Columbia undertook the assignment of Canadian domains on a voluntary basis. No one paid UBC to do this work. It was their contribution to the collective Canadian good. See: *A Nation Goes ONLINE*, CA.net Institute, online: <http://www.canarie.ca/press/publications/ango.pdf>.

[278]Gina Paik & P-R Stark, "The Debate Over Internet Governance: A Snapshot in the Year 2000," online: The Berkman Center for Internet & Society at Harvard Law School <http://cyber.law.harvard.edu/is99/governance/introduction.html>.

Community norms have been effectively used to enforce the standards[279] required of interconnecting networks and if a participant consistently violates those norms, access to other networks will be barred. The process has proven to be remarkably successful.

On one key point there must be a central authority. There must be one and only one system to translate from Internet addresses that people can understand into the four integers that make up actual cyber addresses.[280] ICANN[281] (the Internet Corporation for Assigned Names and Numbers) has been given that authority by the U.S. government. ICANN was created in 1998 and is a registered non-profit corporation in the State of California. ICANN has, in turn, assigned important technical roles to the private company VeriSign.[282] In Canada, CIRA[283] (Canadian Internet Registration Authority) oversees the .ca top-level domain.

ICANN has been at the centre of a number of on-going disputes about how the Internet should be governed. In February 2004, eight registrars sued[284] both ICANN and VeriSign because they felt disadvantaged by a scheme for back-ordering Web addresses that VeriSign had proposed. VeriSign has sued[285] ICANN because it wants to proceed with a new for-profit scheme to redirect unresolved Web addresses. And People for Internet Responsibility[286] have called for an emergency meeting on "Preventing the Internet Meltdown" – with the vigorous support of three very senior people in the field.[287] There has been little agreement about even the modest role assumed by ICANN.

Accepting accountability for any end-to-end public or shared Internet service has been almost totally lacking. There are now expectations that the major backbone network providers will do everything possible to maintain Internet service. The system works remarkably well.[288] But there are few expectations that service will continue in the face of 'acts of God.'[289] Indeed, many

---

[279]Most of the Internet standards began as RFC (or Request For Comment) documents. A consensus developed, or failed to develop, over the proposal put forth by the RFC. The process began in 1969 with RFC 1 - see <http://www.rfc-archive.org/getrfc?rfc=1>. It has progressed to the place where the most recent RFC was numbered 3729 and dated March 2004 – see <http://www.rfc-archive.org/getrfc?rfc=3729>. The RFC documents are now overseen by The Internet Society – see <http://www.isoc.org/isoc/>.

[280]All locations on the Internet are actually addressed by four integers between 0 and 256. For example, <www.gowlings.com> is really just 199.43.129.10. It is clear that there can only be one authority empowered to grant domain names and there can only be one mechanism by which actual Internet addresses are determined.

[281]See, online: <http://www.icann.org/>.

[282]See, online: <http://www.verisign.com/>.

[283]See, online <http://www.cira.ca/>.

[284]Matt Hicks, "Registrars Sue ICANN, VeriSign to Block Domain Name Service" *EWeek-Enterprise News and Reviews* (27 February 2004), online: eWeek <http://www.eweek.com/print_article/0,1761,a=120522,00.asp>.

[285]Matt Hicks, "VeriSign Sues ICANN" *EWeek-Enterprise News and Reviews* (26 February 2004), online: eWeek <http://www.eweek.com/article2/0,1759,1539737,00.asp>.

[286]See, online: PFIR - People For Internet Responsibility <http://www.pfir.org/>.

[287]Lauren Weinstein, Peter G. Neumann and David J. Farber.

[288]The authors' personal experience is typical. Ten years ago when the Internet was first opened for commercial use in Canada all the end-user connections were slow and unreliable. Today, the major network access providers are expected to be up and reliable all the time. Delivered service will often exceed 99.9% availability, with no loss of email.

[289]"[A] natural catastrophe which no one can prevent such as an earthquake, a tidal wave, a volcanic eruption, a hurricane or a tornado. Acts of God are significant for two reasons 1) for the havoc and damage they wreak and 2) because often contracts state that "acts of God" are an excuse for delay or failure to fulfill a commitment or to

Service Level Agreements absolve vendors from their regular contractual obligations when confronted by an 'act of God.' Yet that is precisely the time that we should be most concerned about preserving our Critical Information Infrastructure.

The simple, but inevitable, conclusion is that there is very little acceptance of accountability for any end-to-end public or shared Information Infrastructure services in Canada. And establishing such accountabilities would have to overcome the well-entrenched anti-regulation thinking behind the Internet and our Information Infrastructure. The path forward will be full of challenge.

---

complete a construction project. Many insurance policies exempt coverage for damage caused by acts of God, which is one time an insurance company gets religion. At times disputes arise as to whether a violent storm or other disaster was an act of God (and therefore exempt from a claim) or a foreseeable natural event." See Gerald & Kathleen Hill, *Law.com Dictionary*, *s. v.* "act of God", online: law.com Law Dictionary <http://dictionary.law.com/definition2.asp?selected=2318&bold=%7C%7C%7C%7C>.

12.0 Barriers to Accountability

A number of technical, economic, legal and historical factors combine to create certain barriers to accountability in the elements of the Information Infrastructure.

12.1 Diffusion of Responsibility

As we have mentioned elsewhere, systems have become more and more complex. Paradoxically, this has occurred as a competitive response to the demand of the public to have systems that are simpler to use. Your car no longer has a crank at the front, nor do you have to set the advance of the spark manually or pull the choke to get it to start.[290] Instead, thanks to complex mechanisms that can only be repaired by a dealer, you simply turn the key and drive off – the systems you rely upon are more complex in order to make them simpler to use.

Complex Information Infrastructures may contain thousands of interoperating elements. No one engineer, nor even any small group of engineers, is capable of designing, creating and understanding all those elements and how they work together. Instead, many individuals and many groups have a hand in the design of the elements. Others create them and yet again others, working independently, cobble them all together into a system. Those who maintain them make up yet another constituency of actors and none of those, individually or together, understand the whole system.

So who gets the blame when something goes wrong?

Consider a relatively simple system like the telephone in your own home. If you buy the equipment from one company and get the service from another (a common scenario), you could find, when you call for repairs, that each supplier blames the other when the system doesn't work. It is not a desire to shirk responsibility that actuates such a response; it is rather more likely that each of the contributors to the system honestly believes that the problem does not reside with its equipment or service. What's more, it could be true. The problem could arise from third party interference, such as the operation of a back-hoe on the street outside your home.

Consequently, a major barrier to holding accountable the contributors to our far-flung, organic Information Infrastructure may be the legitimate inability to point to one particular element as the root cause of a problem. Accountability requires a wrong of some kind. If the wrong cannot be pinned on one contributor, or a distinct group, then just and fair accountability may be difficult or impossible.[291]

[290] Younger readers will have no idea what we are talking about. This proves the point.

[291] In the August 2003 power failure, one might have been forgiven for coming to the conclusion that two maxims might apply: (i) "Many hands make light work" and (ii) "Many hands make light go out."

12.2 Cost of Accountability

This work has earlier demonstrated that the legal instruments (especially software licensing agreements) that are used by many players in our Information Infrastructure invariably contain exculpatory language that lessens the cost of failure in the hands of those players. It is a net shift of business and financial risk from the provider to the user. If society now wishes to hold these players accountable beyond the limits of that exculpatory language – if risk is re-assigned to them – then they will have to increase the prices they charge for what they provide.

The result will be that the public will generally pay more to the providers who are successful in extracting the higher prices, instead of paying more in the opportunity costs of infrastructure failures.[292]

In short, the unavoidability of increased costs to be borne by those whom society wishes to hold accountable for failures in our Information Infrastructure is also a barrier to accountability.

While it is incontrovertibly true that society now pays for periodic failures of its Information Infrastructure in lost opportunities, there will be a different kind of societal cost to holding the providers of that infrastructure accountable. Accountability is useless without enforcement. And enforcement costs money (read "taxes"). Legislators will have to exert prodigious political will if they are to both hold such providers accountable and spend the tax dollars to enforce accountability.[293] Is the political will there? Will it be exercised?

Hence, the cost of enforcement, either by public action or private action, is a barrier to effective accountability.

12.3 Reduction in Innovation

What behaviour would be driven by increased accountability for the Information Infrastructure sector? For one thing, the increased business and financial risk arising from the imposition of accountability would result in slower release of innovative products. The reason for this is that every product absorbed into our Information Infrastructure would result in more vulnerability to its innovator. Innovators will think twice before introducing new products. Balanced against the reluctance to introduce new products will be the competitive desire to get new products – at least, those that work well – into the market.

In consequence, the potential for reduction in innovation – which the market will not like – stands as a possible barrier to accountability.

[292]The providers who are unable to extract such higher prices will, of course, go the way of all flesh.
[293]Merely giving members of the public a private right of action, even in these days of increasing popularity of class action claims, may be insufficient enforcement.

12.4 Competition

Canadian society places a high premium on competition. The *Competition Act* was enacted for the purpose of encouraging competition and discouraging anti-competitive behaviour, including, in particular, collusion on pricing.

It is quite certain that the imposition of accountability upon the providers of Information Infrastructure will result in the exit of some players from the market. The strongest of those players will survive and they will be the ones who contribute products and services to our Information Infrastructure. The effect of having fewer players in the field – with accountability acting as a barrier to the entry of new players – might well be a lessening of competition that could place upward pressure on prices. This also may act as a countervailing force to the encouragement of diversity.

We speculate that the potential for political fallout from reducing competition, or even the perception that such is the case, might lessen the political will to impose accountability and therefore act as a barrier to accountability.

12.5 Unilateral Action

Canada enjoys a high level of participation in the global Information Infrastructure. However, there is no Canadian hegemony. As a result, the perception that any unilateral action Canada might take to effect accountability could act as a barrier to its imposition.

For example, if Canada, acting alone,[294] were to effect laws stating that limitations of liability, disclaimers of implied warranties and exculpatory language in licences and procurement agreements were ineffective, developers would react by trying to get out of the reach of Canadian laws. Canadian developers might consider moving from Canada, and foreign developers would avoid having a permanent establishment in Canada in order to ensure that the law applicable to their agreements would be interpreted by courts where limitations of liability, disclaimers, and exculpatory language might be effective.[295] Anticipation of this reaction by developers would hold Canada back from enacting laws that promote accountability, and we believe that Canada would only enact such laws in concert with other countries in order to bring about a more nearly global system of accountability.

---

[294]This discussion does not touch on whether such action would even be constitutional for the federal government to take without the agreement of the provincial legislatures. Let us assume complete co-operation and political will within Canada for the purposes of this discussion.

[295]It is interesting to review the Supreme Court of Canada case of *Morguard Investments Ltd.* v. *De Savoye*, [1990] 3 S.C.R. 1077. The court held that if there is a "real and substantial connection" between a cause of action and a foreign jurisdiction, then the decision of a court in that foreign jurisdiction will be upheld in Canada. Mr. Justice LaForest stated, "… the rules of private international law are grounded in the need in modern times to facilitate the flow of wealth, skills and people across state lines in a fair and orderly manner…. It seems to me that the approach of permitting suit where there is a real and substantial connection with the action provides a reasonable balance between the rights of the parties. It affords some protection against being pursued in jurisdictions having little or no connection with the transaction or the parties." By inference, then, companies will try to reduce the chance of their activities and business having a "real and substantial connection" to Canada in order to avoid the reach of Canadian law.

12.6 Standards

The current state of standards of practice and standards of measurement tend to act as a barrier to accountability for the Information Infrastructure. While there are methodological standards in existence[296], there is a need for many additional standards.

Here's why: in order to hold someone accountable, there must be a measure against which it can be determined whether he or she complies or does not comply. Accountability implies objective fairness in the application of standards, but today there is no body of standards that can comprehensively act as the measure of performance or, on the contrary, negligence in the field of Information Infrastructure.

In other words, before society can hold players in the Information Infrastructure field accountable, standards must be generally agreed upon and adopted. We are still a long way from this.

12.7 Human Nature

Human nature is one of the most significant barriers to accountability. We are 'wired' – and have been since the dawn of humanity – to regard emergencies as things that happen quickly, not slowly. That's why we can smoke for decades and not regard it as an emergency until we are diagnosed with cancer. Or why entire villages can be built on the side of a volcano and inhabitants don't regard it as a dangerous place to live until the lava is streaming down the side of the hill. We are genetically more suited to regarding a charging tiger as a threat.[297]

We are convinced that a sudden emergency that causes a major and long-lasting disruption in our economy is the kind of event that will be required before the public will demand that the players in the Information Infrastructure be held accountable for the functioning of their technologies.

12.8 Custom in the Trade

Business does best under conditions of predictability. So-called 'custom in the trade' has been held for many years by courts in many jurisdictions as a major consideration in the interpretation of contracts. Where a contract is not clear on its face, courts often hear evidence as to what is customary in the particular trade in order to give meaning to unclear contractual terms.

The custom in the information technology trade is that limitations of liability, disclaimers of implied warranties and exculpatory language are used in licences and procurement agreements. While a lawyer might expend a lot of energy trying to get another contracting party to budge on one of these key provisions, 'custom in the trade' most often prevails. The need to change the culture in the information technology business is a major barrier to accountability because of the allegations that will be made that such a change is 'bad for business.'

[296] For example, ITIL and ISO 17799.
[297] Although, admittedly, these are both less a threat in recent times.

12.9 Incomplete Understanding

Our Information Infrastructure, depending on your point of view, is either a Frankenstein's monster or a thing of beauty.[298] One thing is true. It is immensely complex and beyond the comprehension of any one person. What's more, it constantly changes. Its very complexity and incomprehensibility is a considerable barrier to accountability.

In order for society to effect accountability for our Information Infrastructure, it would be good to consider which approach to accountability is most likely to strike the best balance between the rights of the purveyors of the system and the rights of its users. In order to accomplish this, we should first come to universal agreement about what are the ideal rights of the purveyors on one hand, and the users on the other. Then we have to come to agreement on the balance between the two. Finally, we have to agree upon the steps that have to be taken in order to strike that balance in practice.

The problem is this: none of those things are possible unless and until we come to a more comprehensive understanding of the organic nature and the use and societal importance of our Information Infrastructure. If society tries to impose full accountability, all at once, without considering these factors, we will be unable to extrapolate, except in the grossest terms, the effects that different models of accountability will have on society as a whole. In short, we could jump from the frying pan into the fire.

[298]The analogy is apt. Victor Frankenstein's hapless monster was created full of love for humanity, but became evil by forces that he could not, ultimately, influence. In the end the monster attacked, not his creator, but those his creator loved, in order to inflict more pain on the creator.

13.0 Introduction to Accountability Models

The desired end-state is that Canada's Critical Information Infrastructure should almost always deliver reliable, available and secure service, and that if failures occur, they will have only a limited impact on overall service. As has been amply demonstrated elsewhere in this report, realizing that goal will not be a simple process. We believe that a key ingredient in making that happen will be the assignment of appropriate accountabilities to the correct parties. We also clearly recognize that additional work on possible public policies is required before government can act with confidence in the outcome.

During the course of our extensive primary and secondary research into the issues, we have been led to some preliminary observations about possible accountability models. Our observations are not offered as being exhaustive or comprehensive in their coverage. Rather we have drawn upon our research work to highlight the *dimensions* that may go into an accountability model for our Critical Information Infrastructure. Further, we highlight *mechanisms* that may be used to establish, apply and enforce desired accountabilities for our Critical Information Infrastructure.

13.1 Accountability Dimensions

It is virtually certain that a universal accountability model would not be effective. All parties should not be held to the same accountabilities for all possible actions. An effective accountability model must focus on specific actions, by particular parties, under identified conditions in order to determine the accountabilities, which should be assumed or assigned. The *dimensions* presented in this section provide initial suggestions for the paths that could be followed to identify useful accountabilities.

13.1.1 Accountability for Outcome… or Process?

There is a basic and important difference between holding an agent accountable for an *outcome,* versus holding it accountable for a *process*. From a public policy perspective it's obviously attractive if an agent can be identified to be held accountable for the desired outcome. Find the agent and make it accountable for the reliable, available and secure operation of our Critical Information Infrastructure. Unfortunately, that can only work if the agent has a reasonable degree of control over all the multiple factors that contribute to the reliable, available and secure operation of our Critical Information Infrastructure. All the evidence suggests that no such agents can be found.

The alternative is to hold participants in the delivery of service for our Critical Information Infrastructure accountable for following appropriate processes. Multiple agents can be held accountable for following the requisite processes as they contribute to the delivery of Critical Information Infrastructure services. If we but know the requisite processes that lead to the desired outcome, then the assignment of accountabilities is relatively simple. Unfortunately, there are no ironclad connections leading from process to desired outcome. We may have no option except to settle for requisite processes that, under most conditions, will increase the likelihood of obtaining the desired outcome.

13.1.2 Reasons to Accept Accountability

An individual or an organization may elect to voluntarily be held accountable. There is almost always a sense of vested self-interest in such voluntary submissions – the engineer accepts certain kinds of accountabilities and in exchange enjoys the rights and privileges that go along with being recognized as an engineer. Another common path is that the individual or organization may accept accountability because it is a required component of an otherwise desirable relationship. This is often seen in relationships between suppliers and their large and powerful customers. Wal-Mart, for example, can require certain accountabilities from its suppliers and many will accept such accountability requirements because they want or need to do business with Wal-Mart. Finally, governments at all levels have multiple ways they can impose accountability requirements on individuals and organizations which engage in certain kinds of activities.

13.1.3 Parties Accepting Accountability

The individual may be the party to be held accountable. This is common when the individual is a licensed professional in Canada. Doctors, lawyers, accountants and engineers see themselves as professionals and accept certain accountabilities in exchange for the right to practice their profession in Canadian provinces. This is also an example of a group of individuals – the profession – accepting and enforcing accountabilities in exchange for being recognized as a distinct group with special rights and privileges. The group is the conduit through which accountabilities flow to individual members.

Organizations of all kinds and sizes can be held accountable. There are particularly interesting examples of not-for-profit organizations being held accountable for aspects of the operation and management of the global Information Infrastructure and of the Canadian portion of that Information Infrastructure. ICANN[299] has global responsibilities for the operation and management of key Web addresses, as does CIRA[300] in Canada. The Internet Society[301] is another interesting example of a not-for-profit organization that plays a key role in the management and development of the global Information Infrastructure. Canada's own CANARIE[302] could be a similar not-for-profit Canadian organization.

13.1.4 Enforcement Procedures

The goal is to avoid failure in the operation of our Critical Information Infrastructure. Assigning accountabilities to various participants in our Critical Information Infrastructure is one means Canada can employ to make sure that our Critical Information Infrastructure continues to deliver the required services. What happens if a participant fails to discharge their responsibilities? Who notices? Who reports? The massive power blackout of 2003 provides an interesting example of what can happen in the aftermath of a failure. In that case, the failure was obvious – millions

[299]ICANN, *supra* note 281.
[300]CIRA, *supra* note 282.
[301]See, online: Internet Society <http://www.isoc.org/>.
[302]See, online: CANARIE <http://www.canarie.ca/>.

were without electric power in their homes and places of work. Determining *the* cause of the blackout has not been an easy process.[303]

The North American electric power grid is a relatively simple network in comparison to the North American Information Infrastructure. The cause or causes of failure in the power grid should be relatively easy to determine. With our Critical Information Infrastructure it may never be clear what caused a significant failure, if or when such a failure occurs. Do we then fall back on a zero exceptions approach to assumed responsibilities? That may be self-defeating because it could cause participants to ignore assigned accountabilities as unrealistic rules imposed by a government that doesn't really understand.

13.1.5 Consequences of Failure

As a society we have a number of ways in which we could impose penalties on those who fail to meet their accountabilities. We could hold individuals or organization up to public ridicule. Such public ridicule could have serious consequences for the individual's or organization's ability to continue to operate. It could penalize, but would not compensate. As an alternative, we could impose fines or liabilities commensurate with losses suffered as a result of failure to meet accountabilities. Given the scope and extent of our Information Infrastructure, even a 'small' failure could lead to a massive financial obligation. In the normal way of viewing such things, this could be a case in which 'natural' justice is not seen to be done.

Canada could also take the approach of Sarbanes-Oxley[304] and Ontario's Bill 198[305] – hold senior executives personally accountable for failure to follow the requisite procedures. A jail sentence of up to five years would be seen by many as a strong deterrent. There would be costs associated with imposing such a discipline on those who provide Canada's Critical Information Infrastructure. That cost could have a noticeable impact on Canada's global competitiveness. And it is not even clear that we have the knowledge needed to establish requisite procedures for those who provide our Critical Information Infrastructure.

13.2 Accountability Mechanisms

There are a number of mechanisms by which accountabilities may be imposed. They range widely in their social acceptability and effectiveness. Canada could mount an advertising campaign to advocate voluntary acceptance of certain accountabilities in connection with our Critical Information Infrastructure. Some social force would be exerted. At another end of the scale, Canada could impose new legislative requirements on those who provide aspects of our National Information Infrastructure. The law would be used to enforce accountabilities.

We stress that this section is not offered as a comprehensive presentation of possible accountability mechanisms. We highlight some of the mechanisms that arose during the primary

[303]It is not our place, here, to provide even a superficial analysis of what cause the power blackout of 2003.
[304]See, online: U.S. Securities and Exchange Commission - Spotlight on Sarbanes-Oxley Rulemaking and Reports <http://www.sec.gov/spotlight/sarbanes-oxley.htm>
[305]See "April 7, 2003 - Ontario responds to the *Sarbanes-Oxley Act*," online: Gowlings News <http://www.gowlings.com/news/index.asp?intNewsId=107&strShowWhat=all>.

and secondary research we performed. This material is offered as a suggestion of the possible range of mechanisms that Canada may wish to consider.

13.2.1 Public Advocacy

Public opinion does have an impact on members of our society. Public opinion can change stock prices. Public opinion can change business flow for individuals or firms. Public opinion can have very serious consequences for all kinds of organizations. Governments can impact public opinion in a number of different ways. Public opinion needs to be one of the forces employed to increase the willingness of participants to accept accountability for their role in delivering our Critical Information Infrastructure. But public opinion will not sway everyone, nor will its impact always lead to desired behaviour – some are just 'contrary' by nature.

Notwithstanding all the limitations of public advocacy, our research suggests that the willingness of many participants to accept accountability will critically depend on public opinion. Certainly, if the public comes to see the imposition of accountabilities as harsh and unreasonable demands by the government, resistance is likely and likely to be successful. Public opinion should not be ignored in any plan to assign accountabilities.

13.2.2 Directed Purchasing

Governments at all levels exert considerable influence through their purchasing decisions. There is a steady flow of cash from governments to those who supply our Information Infrastructure. Indeed, government business is a vital component in the overall business for many Information Infrastructure suppliers. Governments have the natural power to act like any large and powerful customer; they can impose conditions on those wishing to sell them goods or services.

There are obvious limitations on the penalties that governments can attach to accountability failure. Vendors have a natural reluctance to accept contracts with the possibility of any large penalties. And, thus far, most suppliers to the North American Information Infrastructure have been successful in avoiding such contracts.

13.2.3 Standards Development

It seems likely that some of the desirable accountabilities will be for following standards of practice. In the case of our Critical Information Infrastructure, we do not yet know all the standards of practice that will lead to the desired outcomes. Promising standards of practice need to be developed and field-tested. The standards development process is time consuming and expensive. Government could, in a number of ways, encourage development of standards of practice that are particularly relevant to our Critical Information Infrastructure.

Government could encourage and support participation by appropriate government employees in the standards development process. Government could encourage departments to act as the location for field trials of appropriate proposed standards of practice. Government could fund others to work on development or fund other organizations to allow them to be field test locations. And last, but not least, government could require acceptance of standards of practice within its own Departments and by its own suppliers.

13.2.4 Standards Enforcement

Government has a voice in how a number of sectors of our society are required to operate. In many cases, it has the power to impose requirements on how various activities are carried out within Canada. To the extent that such power is in the hands of government, it could use that power to enforce the application of appropriate Standards of Practice. It should be noted, however, that Standards of Practice cannot be arbitrarily imposed if there is to be much chance of their successful adoption. The community expected to follow those Standards of Practice needs to be 'ready' to follow the standards.[306] There will be a need to do a serious amount of 'selling' of Standards of Practice prior to their imposition on a community.

13.2.5 Professional Licensing

There are some uniquely Canadian opportunities and challenges in connection with professional licensing. The professions in Canada are a provincial concern. Recognized professional societies are provincial organizations. Each province, for example, has its own professional engineering society. There is some degree of cooperation at the national level, but licensing is a strictly provincial affair. Increasingly, there is recognition that Standards of Practice must be international in application, notwithstanding the provincial scope of licensing. The engineers have 'solved' the problem of national accreditation of engineering degree programs by voluntarily agreeing to pool their efforts under a single national accreditation effort.[307]

With licensing we face a uniquely Canadian challenge of a national concern that can only be regulated provincially. We also face a uniquely Canadian opportunity because we are unusual in recognizing broadly applicable restricted rights to practise. The mechanism exists, albeit at the provincial level, to enforce a restricted right to practice, certainly in connection with engineering practice. Extending this to cover aspects of our Critical Information Infrastructure would have a strong appeal to many provincial engineering societies.[308]

13.2.6 Market Regulation

Canada has taken a number of steps to regulate markets within our borders. The provinces have also taken steps to regulate markets within their borders. It is beyond the scope of this report to identify the most promising ways that the market for goods and services connected to our Critical Information Infrastructure can or should be regulated. Our purpose here is to suggest that markets are never completely 'free'. The state always has a role to play in the operation of markets within its borders.

Consideration might be given to using federal and provincial powers to regulate markets to influence the terms and conditions under which transactions connected with our Critical Information Infrastructure are allowed. The attraction of using the indirect approach of market

---

[306]The dynamic leading to "successful" standards has been much studied by the international standards community. The approach taken by the International Organization for Standards (<http://www.iso.org>) has generally proven successful. They try to collect best practices which are generally being followed, and then repurpose them as a standard guide.

[307]The Canadian Council of Professional Engineers (<http://www.ccpe.ca/>) has the delegated responsibility to accredit engineering degree programs across Canada.

[308]Private communication from a former President of the Professional Engineers of Ontario.

regulation is that participants will have some choice about the degree and extent to which they are prepared to participate in such a regulated market.

13.2.7 Direct Regulation

In matters of public good and public safety, the state has considerable power to regulate what is allowed, required, or forbidden. Such public safety powers have not traditionally been used to directly regulate our Information Infrastructure, but a strong argument could be mounted that such regulation could be necessary and appropriate. We recognize that the possibility of direct regulation could lead to a vigorous national debate[309] about the appropriate actions to be taken by government to protect our Critical Information Infrastructure. But it is true that our Information Infrastructure is critically important to public safety. Perhaps we should consider engaging Canadians in such a debate if, after further study, it has been determined that direct regulation is a path that Canada should consider.

13.3 Accountability Models

The process of developing accountability models for our Critical Information Infrastructure is necessarily complex and multi-faceted. All we have been able to do in this section of the report is to suggest the scope and range of accountability dimensions and accountability models.

[309]The debate within the U.S. about Homeland Security is illustrative of what could be expected within Canada. See, online: Antiwar.com <http://www.antiwar.com/paul/paul39.html>.

14.0 Potential Approaches for Improving the Critical Information Infrastructure

Our research has highlighted four areas that may merit consideration when exploring how we might improve the reliability, security and functionality of the Critical Information Infrastructure. These suggestions represent the synthesis of the opinions of key stakeholders. They would all require extensive research and consultation before implementation could be contemplated.

14.1 Encourage Diversity in the Shared Information Infrastructure

Diversity, properly encouraged, can enhance the reliability of Canada's overall Information Infrastructure. There may be significant potential benefits from multiple instances of different, separate, yet functionally equivalent components at each level of the shared Information Infrastructure.

There are multiple arguments that can be advanced in favour of diversity. Many of the key stakeholders we interviewed pointed to the problems they see in Microsoft's near monopoly in the desktop operating system and office suite markets. Our secondary research lent strong support to the beneficial view of diversity. Our conclusion is that there may be large potential reliability benefits that would flow from an overall Information Infrastructure in which there is a healthy diversity in components and suppliers.

As a first step, we would need to better understand the actual current component and supplier diversity in our Information Infrastructure and specifically in our Critical Information Infrastructure. In many sub-markets, there is already a diversity of suppliers and installed components. No encouragement of diversity would be required or justified. We know about the lack of diversity on the desktop. Where else in our Critical Information Infrastructure is there a lack of diversity? What benefits could flow from encouraging diversity in those areas where it is currently absent?

Once it has been determined where diversity would be beneficial, models could be developed for how best to achieve the desired levels of diversity. In extreme cases, government may have no practical option but to, itself, become a supplier to our Critical Information Infrastructure. In most cases we expect that desired diversity might be best achieved through less aggressive intervention by government. A continuing watching brief might be maintained by government.

14.2 Enforce Accountability for the Shared Information Infrastructure

Greater accountability could be placed on those who build and operate shared services within the Information Infrastructure. Because these services are the result of the cooperative action of many players, most accountability will probably be accountability for process.

The first step might be to develop a comprehensive picture of all those who build or operate an aspect of shared services within Canada's Information Infrastructure. Given the high degree of interdependence that may exist between any two aspects of our shared Information

Infrastructure, the picture should be comprehensive; even a ‘small’ participant may play an absolutely critical role. At the same time, a refined understanding could be developed for the criticality of each participant in delivering reliable, available and secure Critical Information Infrastructure services.

This work could lead to a better understanding of who might be held accountable. Another question which needs to be answered concerns the nature of each participant’s accountability. Can an outcome be identified for which the participant can be held accountable? In most cases, the requisite cooperative actions preclude practical accountability for outcomes. The alternative is to hold the participant accountable for following appropriate processes. The challenge may be to identify or develop the processes which must be followed to achieve the desired security, availability and reliability of our Critical Information Infrastructure. This will not be an insubstantial undertaking.

Having identified who can be held accountable for what, the challenge becomes one of making it happen and making sure that it continues to happen. In Section 13 we described some of the means that could be employed to answer this challenge. Consultation with those who are to be affected would be prudent. This would represent a significant change in how our Information Infrastructure is developed, operated and managed. Any change of this magnitude will probably be traumatic. We should prepare for the likely trauma.

14.3 Enforce Accountability for the Private Information Infrastructure

Those who operate private services that connect with the shared Information Infrastructure could be held more accountable. Because these services are largely the responsibility of those who operate them, most accountability might be for results. The results might usually be best measured at the interface between the private service and the shared Information Infrastructure.

The challenges of accountability for private services parallel those for shared Information Infrastructure services. The first step might be to understand which private services from which entities are connected to the shared Information Infrastructure. The range of such connected private services is extensive and expanding rapidly. Millions of Canadian computers already connect to our shared Information Infrastructure. There are products available today to connect automobiles, furnaces, cameras and telephones to the shared Information Infrastructure. And the online refrigerator is coming.

It is already the case that computer viruses spread from infected home computers. Noise from a malfunctioning cable modem can cause severe degradation in service to all computers connected to the same cable segment. At the other end of the spectrum, there are private Canadian networks with thousands of connected devices. Problems in such extensive private networks can have an impact that ripples across the entire Canadian Information Infrastructure. We would need to identify who may be responsible for exporting problems to the larger Canadian Information Infrastructure and develop an appreciation of how severe those problems may be.

With this information in hand, we may be in a position to posit the kinds of accountabilities that ought to be assumed and could begin to identify who may be held accountable. Essential in this process is the identification of the precise nature of the accountability that could be assumed.

What behaviour, if any, is required or forbidden from the vendor or owner of an online refrigerator? How can we determine that the right behaviour happens? What remedies could reasonably be imposed on the vendor or owner of a misbehaving refrigerator? The refrigerator example may be somewhat light-hearted, but the same questions should be asked of the company that has thousands of devices connected to a network that crosses Canada.

'All' that would remain is to make it happen in an expeditious fashion that is seen as fair by all concerned. That would be no small feat. Complete success is unlikely, but we can make progress in reducing the risk to our shared Information Infrastructure from connected private services. The stakes are high. Meaningful and informed action should be beneficial.

14.4 Encourage Standards Development and Adoption

In general, standards are useful for the implementation of accountability. Standards allow us to measure, certify and interconnect pieces of the Information Infrastructure. International standards may be the most important because of the global nature of the Information Infrastructure, but Canadian standards may also play important roles.

The basic interconnection standards work remarkably well. Anyone or anything that wants to connect is able to do so and the minimum required interconnection standards are well-known. There are other network standards that are less well-known and less consistently implemented. Some of these could be key to preserving our Critical Information Infrastructure in the face of selective loss of overall network capability. For example, the new Internet Protocol (IPv6) includes a way for packets to request higher priority service. With IPv6 in place, it would be possible in cases of partial Information Infrastructure failure to reserve all remaining capabilities to meet the needs of our Critical Information Infrastructure. There are a number of other standards that could also be used to preserve service to our Critical Information Infrastructure.

Work could be undertaken to identify the most promising network standards that could be used to preserve service to our Critical Information Infrastructure. In different ways, the three preceding suggestions all depend on identifying or developing product or process standards and ensuring that they are applied in practice. The standards challenge is multi-faceted:

- Identify the most important standards for a reliable, available and secure Critical Information Infrastructure.
- Work within the international standards community on the development and maintenance of those key standards.
- Support the adaptation and adoption of those key standards for use in connection with our Critical Information Infrastructure.
- Encourage or require the use of those key standards by those who build or operate our overall Information Infrastructure.

In this context, there is a uniquely Canadian standards opportunity. Our various provincial engineering acts give Canadian engineers the exclusive right to restricted areas of practice. This mechanism, available only in Canada, could be used to enforce the application of key standards.

15.0 Knowledge Gaps

A number of times throughout this report we have made the point that society has become increasingly dependent on the existence and proper operation of the Critical Information Infrastructure. All the other critical infrastructures: power, transportation, financial services, etc., heavily depend upon it. Thus, the continuation and progressive positive evolution of the Critical Information Infrastructure as a viable, robust entity is of paramount importance, both to Canada as well as to the rest of the world.

The functioning and growth of the Critical Information Infrastructure is in large part dependent upon providers of software and IT systems. However, in most cases, these entities have a very low level of accountability / legal liability with respect to the products and services that they offer. This disparity becomes even more evident if we compare their level of accountability to providers of goods and services in other critical infrastructure sectors.

If the Critical Information Infrastructure is to continue to evolve and expand in terms of functionality, robustness and security, we should consider the merits of improving overall governance of and accountability for the Critical Information Infrastructure. We would be in a much better position to contemplate such improvement if we filled critical gaps in our knowledge. Some of these gaps are outlined below as potential research projects.

The list below is intended to be representative, not exhaustive. We also recognize that there is some commonality in these project suggestions and that the timelines for these projects may span fiscal years. Before undertaking any given project, we recommend a pre-project review to ensure that there are no current, overlapping initiatives.

15.1 Stakeholder Directory

Statement of Work

Develop a directory of key stakeholders in the Critical Information Infrastructure, including the sphere of influence and sphere of concern for each. This would be part of the foundation information required to begin the process of getting a broadly-based consensus for proactive changes to Critical Information Infrastructure accountability.

Rationale

Having a good working knowledge of the interests, objectives, priorities and perceptions of key stakeholders could be important when defining changes that would improve and expand Critical Information Infrastructure accountability for the future. As a step toward generating stakeholder consensus, stakeholders should be clearly identified and categorized, with respect to their objectives, agendas and priorities.

15.2 Initial Case Study

Statement of Work

Conduct a case study that defines a function provided by the Critical Information Infrastructure that is required to support another critical sector. Identify the entire Information Infrastructure involved in delivering this functionality. Provide an analysis that highlights the parts of this infrastructure slice most prone to failure.

Rationale

Identification of the weakest links in various parts of the Critical Information Infrastructure is important, owing to the interdependence of different segments of the Critical Information Infrastructure upon each other. In addition, the Critical Information Infrastructure serves as a foundation upon which many other sectors of the overall national critical infrastructure are overlaid.

15.3 Further Case Studies

Statement of Work

Conduct a series of case studies, such as the one outlined in the previous section, involving the Critical Information Infrastructure supporting a range of other critical infrastructure segments. Analyze the weak links to determine the degree of commonality across segments.

Rationale

The rationale for this subsection is basically a restatement of that discussed in the previous subsection. Furthermore, once the degree of commonality across all segments of the Critical Information Infrastructure is ascertained and analyzed, it should become easier to identify the most likely failure points and failure scenarios. In addition, this knowledge could assist in developing possible solutions that would eliminate or strengthen these weak links in the Critical Information Infrastructure.

15.4 Information Infrastructure Failures

Statement of Work
Undertake research to complete/expand the following chart:

Table 15.1 Critical Information Infrastructure Failures with Health and Safety Impacts

Category	Incident(s)	Alleged Deaths/Injuries	License(s) in Effect	Relevant Statutes or Regulations
Air Transport	Chinook Helicopter Crash			
Defence	Patriot Missile Failure			
Healthcare	Nuclear Medicine – Therac-25 Irradiation Machine			
Others	Data			

Rationale
As discussed in this report, a prime motivator for public sector intervention in Critical Information Infrastructure accountability might be the presence of major health and safety issues. This research initiative can identify such areas. It could also provide information on any pertinent existing regulations or legislation.

15.5 Performance Metrics Development

Statement of Work
Examine the current state of analysis/measurement of performance of the Critical Information Infrastructure and its associated networks, systems and components. Hypothesize the possible future evolution of performance standards. This includes both process standards as well as results standards. Suggest methodologies and possible frameworks needed to develop these standards. Recognizing that the defining of standards is a very complex and arduous task, how shall we proceed in this endeavour?

Rationale
Before we can attempt to evaluate security metrics for the Critical Information Infrastructure, we should have a sense of the expected performance levels of components and systems that comprise the Critical Information Infrastructure. Before we can even discuss accountability, we should ask the question: accountable for what? Currently, we are being impeded by the inability to consistently measure things. Both process standards and results standards should be considered. Because the Internet is global, consistent worldwide standards should be developed and implemented.

15.6 Security Metrics Development

Statement of Work

Examine the current state of analysis/measurement of the security of the Critical Information Infrastructure and its associated networks, systems and components. Identify the current deficiencies and gaps. Theorize with respect to the future evolution of security assessment and analysis. Suggest methodologies and frameworks needed to develop these security measurement tools and methods.

Rationale

At the present time, we cannot really quantify the level of security inherent in the Critical Information Infrastructure, nor what the optimum level should be. We should consider defining both security test standards and security process standards. These standards may need to be defined and implemented globally. Basically, we may desire the functional equivalent of GAAP (Generally Accepted Accounting Principles) with respect to security measurement and assessment for the Critical Information Infrastructure.

15.7 Public Knowledge of Cyber Law

Statement of Work

Conduct a survey study of the general public in order to ascertain the current level of awareness and concern with respect to cyber law issues.

Rationale

Anecdotal evidence leads us to believe that the current level of awareness and concern on the part of the general public with respect to cyber law issues is quite low. This is especially significant in the light of the high level of society's dependence upon the Critical Information Infrastructure. There may be little incentive for our lawmakers to improve and reform applicable laws if the public's level of awareness, and therefore compliance, is low.

15.8 Communication of Cyber law to the Public

Statement of Work

If the above-mentioned study verifies that the current level of public awareness of cyber law is low, research further research could help to ascertain the best method(s) to raise the level through communication. The methods decided upon should be both feasible and cost-effective.

Rationale

It has recently come to light that even those professionals who are employed in areas that are directly impacted upon by cyber law do not really understand the current state of the law.[310] This includes Canadian Recording Industry Association executives, professional musicians, newspaper writers who specialize in this area, and so on. Therefore, it is not logical or even

[310]Shane Schick, "How the downloading debate is starting to infect other areas of IT,"*IT Business*, (2 March 2004), online: itbusiness.ca <http://www.itbusiness.ca/index.asp?theaction=61&sid=54933#>.

reasonable to expect that the general public would be able to understand this highly complex legal regime.

15.9 Communication of Cyber Law to Corporations

Statement of Work
Corporations are composed of individual persons; therefore some of the ideas from the previous section may apply here as well. However, corporations may require additional accountability mechanisms, such as:

1. Self-Certification
2. Third-party tests/certifications

Conduct a study to evaluate the effectiveness of the above suggested methodologies. Assess under which circumstances the various options should be utilized (i.e. When, where, how?).

Rationale
As previously mentioned, corporations are made up of people, thus Section 15.1.9 has relevance to corporations also. However, if legislation and/or regulation (e.g. the *Sarbanes-Oxley Act of 2002* in the U.S.) are employed in order to deter certain behaviours, additional accountability mechanisms may be required. With respect to corporations, compliance may need to be made explicit, rather than implicit.

15.10 Trends in Cyber Criminal Activity

Statement of Work
Conduct research in order to classify the types of offences included. Ascertain the levels and types of cyber crimes in the past, as well as the current situation. Make future projections and estimates of the type and quantum of cyber crimes.

Rationale
It is important to assess the impact of each type of cyber offence upon the Critical Information Infrastructure.

15.11 Criminal Law as a Deterrent in Cyber Crime

Statement of Work
Conduct primary research in order to ascertain how the current criminal law might be reformed/amended to more effectively deal with and deter cyber crime. This would likely include interviewing criminal lawyers, criminal psychologists, youth workers, law enforcement personnel, etc.

Rationale
The current regime of criminal law has had difficulty keeping pace with the rapid technological advances and changes inherent in our computer and information dominated society. Furthermore, the unique nature of information, when combined with the borderless/international nature of cyber crime, has placed demands upon traditional criminal law that are difficult to deal with

effectively. The *Criminal Code* evolved to serve a 'bricks and mortar' world and is not as good when dealing with offences related to information in cyberspace.

In addition, the two main types of cyber criminals we identified do not seem to be effectively deterred by the current criminal regime. Novice cyber criminals do not understand or realize that they can ever get caught for their computer-assisted crime. At the opposite end of the spectrum are the professional cyber criminals, who have used their technical expertise to minimize their risks of ever being caught. In addition, they are willing to assume this risk as "part of their business".

15.12 The Evolution of Cyber Insurance

Statement of Work
Section 9.4 presents a brief overview of the potential of cyber insurance. Since only the highlights are explored, it may be useful to study this subject in much greater depth. The various types of cyber insurance could be explored, in the light of their strengths and weaknesses, as well as their applicability to various components of the Critical Information Infrastructure.

Rationale
It is useful to develop a consensus regarding the evolution of cyber insurance with respect to the Information Infrastructure. Whatever direction is eventually taken should be compatible with prevailing market forces, so as to encourage a timely and efficient development of appropriate insurance products and services.

15.13 Product Liability Law and Software

Statement of Work
Conduct a research study of the current status (and possible future status) of product liability law with respect to software.

Critical knowledge gaps to be filled in order expedite the positive evolution of Information Infrastructure accountability could be identified. Areas to monitor on an ongoing basis will also be suggested and monitoring techniques will be proposed.

Rationale
Since software is generally licensed, ownership of the program remains with the manufacturer. This applies both to commercial off-the-shelf software as well as custom software. Since no product is actually purchased, it is possible that the common-law notions of the fitness of goods, the provisions of the *Sale of Goods Act*, or other consumer protection laws will have limited utility when applied to a software manufacturer.

15.14 Licensing of Software Professionals

Statement of Work
Perform research to investigate the issue of whether software professionals could be licensed or not, or perhaps certified or regulated in some other manner. Should they be regulated, as are professional engineers? Is self-regulation a possibility, such as in the regulated health professions?

Rationale
With respect to other engineering professions, it required some major disasters (e.g. failures of bridges) to make certification compulsory. It may be more prudent to approach the issue of regulation of software professionals in a proactive manner, rather than to wait for it to occur as a reaction to some future software failure-induced disaster (e.g., a failure of portions of the Critical Information Infrastructure that result in loss of life).

15.15 Assigning Critical Information Infrastructure Accountabilities

Statement of Work
Conduct a research study to clarify and ascertain how the current levels of accountability that are associated with the various participants in the Critical Information Infrastructure affect the operation and development of the Critical Information Infrastructure. Relate these varying quanta of accountability to both desirable and undesirable aspects of the current Critical Information Infrastructure. What lessons can be learned from this, and how can this information be utilized to create a more robust and functional Critical Information Infrastructure in the future?

Rationale
There appears to be a broad spectrum of levels of accountabilities (or lack thereof) existing within the current Critical Information Infrastructure. By studying this phenomenon in a rigorous manner, we may be able to standardize and improve the overall accountability level and the reliability and robustness of the future Critical Information Infrastructure.

15.16 Attributes of the Current/Future Critical Information Infrastructure and Their Implications

Statement of Work
Conduct research to ascertain the known attributes of the current Critical Information Infrastructure. What are the interrelationships between these attributes? How is the desired state of the future Critical Information Infrastructure related to each such attribute? How are the various attributes of the Critical Information Infrastructure related to the policies that govern the Critical Information Infrastructure?

Rationale
By being able to accurately assess and have a good working awareness of the attributes of the current Critical Information Infrastructure, both desirable and undesirable, lessons may be learned as to how to improve the future Critical Information Infrastructure. In addition, by studying the interrelationships between the attributes and the policies that govern the Critical

Information Infrastructure, it may be possible to develop new and improved accountability paradigms for the future Critical Information Infrastructure.

15.17 Privacy Concerns and Critical Information Infrastructure Vulnerabilities

Statement of Work

Conduct research with respect to the topic of how information regarding threats and vulnerabilities to the Critical Information Infrastructure can be disseminated and shared between the private sector and law enforcement organizations, while protecting privacy of individuals (or minimizing privacy breaches).

Rationale

It has been stated that dealing with the problems of the Critical Information Infrastructure requires a multidisciplinary response.[311] In addition to proposed technical solutions, managerial solutions, public education, and so on, the gathering and sharing of information by and between law enforcement and the private sector may be required if solutions are to be developed to deal with the current vulnerabilities of the Critical Information Infrastructure. However, such secondary use of information invariably raises serious concerns with respect to the protection of personal privacy. The research could investigate ways in which information sharing can be performed that will have a minimal impact on the privacy of individuals.

[311]Patterson & Personick, *supra* note 181 at 61.

16.0 Concluding Remarks

The Critical Information Infrastructure is unlike any other Critical Infrastructure:

- It is the only infrastructure where the critical portion is defined as that which supports the other Critical Infrastructures.
- The boundaries of the Critical Information Infrastructure are amorphous and shifting and there are many indirect interdependencies.
- The complexity and dynamism of the Critical Information Infrastructure far exceeds what is found in all other Critical Infrastructures.

Many simple proposals have been advanced to achieve a desired level of reliability, availability and security in our Critical Information Infrastructure. The most cursory examination of the issues presented in Section 11 of this report validates the maxim that "Complex problems have answers that are simple, easy to understand … and wrong!"

Notwithstanding the challenges, Canada has a responsibility to develop the best possible answer to the question, "How do we, as a nation and a society, best move to increase the reliability, availability and security of the Critical Information Infrastructure on which we depend?"

Broadly, it is our opinion that we should:

1. Develop a better, more detailed, understanding of the Critical Information Infrastructure;
2. Develop better ways to measure the performance of the Critical Information Infrastructure;
3. Make the best, informed tradeoffs between cost and risk;
4. Concentrate our efforts on the weakest aspects of the Critical Information Infrastructure; and
5. Recognize that our Critical Information Infrastructure vigilance is a continuing process.

This is an ambitious agenda, but this is a challenge that we ignore at our peril as a nation and a society. Business as usual is not an option. We must show courage and leadership. It is in every Canadian's best interest to have a reliable, available, and secure Critical Information Infrastructure.

Bibliography

680 News Staff. (2004). “Parts of Microsoft source code leaked over Internet, software giant says.” http://www.680news.com/news/business/article.jsp?content=b0212154A (13 February 2004).

ADP Canada. (2004). “ADP Solutions and Services”. http://www.adp.ca/en/index.html (5 March 2004).

Alderson, Douglas and Deanne Montesano. (2003). *Regulating, De-regulating and Changing Scopes of Practice in the Health Professions – A Jurisdictional Review* (a report prepared for the Health Professions Regulatory Advisor Council (HPRAC) at 3, http://www.oaccpp.on.ca/news/appendix1-dp.pdf (12 February 2004).

Anderson, Robert H. *et al*. *The Global Course of the Information Revolution: Technological Trends: Proceedings of an International Conference* Santa Monica: RAND, 2001.

Anderson, Ross. (2001). “Why Information Security is Hard – An Economic Perspective.” (Proceedings of the 17th Computer Security Applications Conference, New Orleans, Louisiana, Dec. 2001). *Annual Computer Security Applications Conference*. http://www.acsac.org/2001/papers/110.pdf (16 February 2004).

Anton, Philip S., Silberglift, Richard & James Schneider. *The Global Technology Revolution – Bio/Nano/Materials Trends and Their Synergies with Information Technology by 2015, A Report Prepared for the National Intelligence Council by RAND National Defence Research Institute*. Santa Monica: RAND, 2001.

Apicella, Mario. “Shaking hands is not enough.” *InfoWorld* Vol. 23, No. 18 (30 April 2001): pp. 49–53.

Arce, Iván. (2004). “More Bang For the Bug: An Account of 2003’s Attack Trends.” *IEEE Security & Privacy*. http://www.computer.org/security/v2n1/j1att.htm (12 March 2004).

Arkin, Ofir. (2002). Atstake Corporate White Paper. “Trace-Back: A Concept for Tracing and Profiling Malicious Computer Attackers.” pp. 1–17. http://www.atstake.com (30 December 2003).

Associated Press. (2004)“Chinese standards don't work with Intel.” *The Globe and Mail*. http://www.globetechnology.com/servlet/story/RTGAM.20040311.gtwifimar11/BNStory/Technology/ (11 March 2004).

Baase, Sara. (1974). “IBM: Producer or Predator.” *Reason* (April 1974) pp. 4–10. http://www-rohan.sdsu.edu/faculty/giftfire/ibm.html (03 March 2004).

Bace, Rebecca, Geer, Daniel, Gutmann, Peter, Metzger, Perry, Pfleeger, Charles P., Quarterman, John S., and Bruce Schneier. (2003). "Cyber*In*security: The Cost of Monopoly – How the Dominance of Microsoft's Products Poses a Risk to Security." http://www.ccianet.org/papers/cyberinsecurity.pdf (2 February 2004).

Banisar, David. "Perspective: manufacturers should be liable when computer bugs leave consumers in the lurch." *Regional Review* Vol. 12, No. 3 (September 2002): pp. 2–5.

Banisar, David. (2001). "Save the Net, Sue a Software Maker." http://www.securityfocus.com/columnists/47 (9 February 2004).

Baptista, Joe. (2002). "Electronic privacy issues affecting Canadians, business and government". (Letter to Privacy Commissioner of Canada re: Internet Root Servers). http://cecua.customer.netspace.net.au/Acrobat1/Root%20Server%20Privacy%20Complaint.pdf (3 February 2004).

Baran, Paul. (1964). "On Distributed Communications." *The Rand Corporation*. http://www.rand.org/publications/RM/RM3420/index.html (14 February 2004).

Barrett, Jennifer. (2004). "More Doom? The infection rate for the world's fastest growing email virus ever is subsiding, but security experts say the risk of new attacks is not." *Newsweek*. http://www.msnbc.msn.com/id/4154289 (4 February 2004).

Barrett, Jennifer. (2004). "We're Making Rapid Progress." *Newsweek*. http://msnbc.msn.com/id/4100822/ (4 February 2004).

Barrett, Katherine. 2002. Food Fights: Canadian regulators are under pressure to face the uncertainties of genetically modified food. *Alternatives Journal*. Vol. 28, No. 1: 28–33.

Bennett, Elizabeth. (2003). "Improving Your Bottom Line – Certifiably." *Baseline Magazine*. http://www.baselinemag.com/article2/0,3959,1408933,00.asp (13 January 2004).

Berlind, David. (2004). "Greed: the real reason for Sobig and MyDoom's "success." ZD Net Tech Update. http://techupdate.zdnet.com/techupdate/stories/main/the_real_reason_for_Sobig_and_MyDoom_success.html (9 February 2004).

Berlind, David. (2004). "Instead of indemnification, consider 'open source insurance'." *ZD Net Tech Update.* http://techupdate.zdnet.com/techupdate/stories/main/open_source_insurance_print.html (24 February 2004).

Berlind, David. (2004). "Phishing: Spam that can't be ignored." *ZD Net Tech Update.* http://techupdate.zdnet.com/techupdate/stories/main/Phishing_Spam_that_cant_be_ignored_print .html (13 January 2004).

Berlind, David. (2004). “The SCO legal train: Know your options.” *ZD Net Tech Update.* http://techupdate.zdnet.com/techupdate/stories/main/SCO_legal_train_print.html (24 February 2004).

Blakely, Stephen. “Left in the dark about power failures.” *Nation's Business* Vol.85, No. 6 (June 1997): p. 74.

Blanchfield, Mike and Rick Mofina. “Canada's cyber network, pipelines and power grids, which are all tied to the United States, are the most likely targets of terrorists exercising vendettas against America.” *Can West News*. (21 December 1999).

Bloor, Robin. (2004). “The Lawyers are coming.” *IT-Analysis.com*. http://www.it-analysis.com/article_pf.php?articleid=11666 (13 February 2004).

Blue Ribbon Advisory Panel on Cyberinfrastructure. (2003). *Revolutionizing Science and Engineering Through Cyberinfrastructure: Report of the National Science Foundation Blue Ribbon Advisory Panel on Cyberinfrastructure*. http://www.communitytechnology.org/nsf_ci_report/ (8 January 2004).

Bohnen, Linda S. *Regulated Health Professions Act – A Practical Guide*. Toronto: Canada Law Book, 1994.

Bowen, Jonathan P., Isaksen, Ulla, and Nimal Nissanke. (1996). “System and Software Safety in Critical Systems.” http://www.museophile.lsbu.ac.uk/pub/jpb/scs-survey-tr97.pdf (3 February 2004).

Boyd, Clark. (2003). “Cyber threats risk net's future.” *BBC News UK Edition*. http://news.bbc.co.uk/1/hi/technology/3322449.stm (19 December 2003).

Bradley, Patrick E. and Jennifer R. Smith. 2000. Liability for Software Defects. New Jersey Law Journal. Vol. 62, No. 1: 3–9.

Brewin, Bob. (2003). “Industry and gov't call for U.S.-wide cattle ID system.” *IT World Canada*. http://www.itworldcanada.com/Pages/Docbase/ViewArticle.aspx?ID=idgml-c5bdcf2d-148f-4f1f-a2a9-b18e20ec942f&Portal=E-Government (5 January 2004).

Bridis, Ted. (2004). “Microsoft Warns on Windows Security Flaws.” http://apnews.myway.com//article/20040210/D80KJ01G1.html (11 February 2004).

Bridis, Ted. (2004). “Microsoft Warns Windows Prone to Hacking.” http://apnews.myway.com/article/20040211/D80L3AD80.html (11 February 2004).

British Telecommunications, PLC (BT). (2003). BT's Response to OFTEL's Consultative Document: "Encouraging self- and co-regulation in telecoms to benefit consumers." http://www.btplc.com/pda/Corporateinformation/Regulatory/RegulatoryInformation/OftelConsultativeDocuments/SelfRegulationSept2000/response.pdf (19 February 2004).

Brown, Alan S. 2002. SCADA vs. the Hackers: can freebie software and a can of Pringles bring down the U.S. power grid? Mechanical Engineering-CIME. Vol. 124, No. 12: 37–41.

Bruce, P. James. (2003). "Disaster Mitigation and Preparedness in a Changing Climate." http://www.ocipep.gc.ca/research/scie_tech/disMit/disMit/disas_miti_e.asp (30 December 2003).

BTexact Technologies (a division of British Telecommunications). (2001)."Technology Timeline." http://www.btexact.com/docimages/42270/42270.pdf (5 March 2004).

Business Week Staff. "The Best Way to make Software Secure: Liability." *Business Week* Vol./No. 3774 (18 March 2002): p. 61.

Business Week Staff. "This Law is User-Unfriendly." *Business Week* Vol./No. 3677 (17 April 2000): pp. 94–97.

Buxton, J. M., Naur, Peter, and Brian Randell, eds. Software Engineering: Concepts and Techniques. New York: Petrocelli/Charter, 1976.

Callahan, Dennis. (2004). "Sarbanes-Oxley: Road to Compliance." *EWeek-Enterprise News and Reviews*. http://www.eweek.com/article2/0,4149,1527933,00.asp (17 February 2004).

Campus Information Technologies and Educational Services. (2004). *Glossary of Acronyms and Technical Terms*. http://www.cites.uiuc.edu/glossary/#i. (22 February 2004).

Canadian Broadcasting Corporation. (2004). "Computer Invasion: A History of Automation in Canada." *CBC Archives* http://archives.cbc.ca/IDD-1-75-710/science_technology/computers/ (26 February 2004).

Canadian Community Reinvestment Coalition. (1997). "An Accountability System For Financial Institutions in Canada: How To Ensure They Meet a High Standard of Performance." *CCRC Position Paper #5*. http://www.cancrc.org/english/posdoc5eng.html (December 1997).

Canadian Community Reinvestment Coalition. (2001). "Comparison of Amendments set out in Bill C-8 to Financial Institution and other Laws vs. CCRC Recommendations." http://www.cancrc.org/english/recomm01.html (19 February 2004).

Canadian Press. (2004). "Ottawa not ready for emergency, documents show." *The Globe and Mail*. http://www.theglobeandmail.com/servlet/story/RTGAM.20040111.wblack0111/BNPrint/National/ (13 January 2004).

CANARIE. *A Nation Goes Online – Canada's Internet History*. Montreal: CA*net Institute, 2001. http://www.canarie.ca/press/publications/ango.pdf (3 March 2004).

Carey, David (interviewer). “Inside Microsoft: helming IT at software's ground zero [Interview with John Connors].” *Information Technology Management* Vol. 7, No. 4(1999): pp. 22–32.

Carlson, Caron. (2003). “Worms Spur Call for Diversity.” *EWeek – Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=59124,00.asp (2 February 2004).

Carnegie Mellon University Software Engineering Institute. (1996). “Testimony of Richard Pethia Manager, Trustworthy Systems Program and CERT Coordination Center.” *1996 Congressional Hearings Intelligence and Security*. http://www.fas.org/irp/congress/1996_hr/s960605m.htm (3 February 2004).

Carnegie Mellon University Software Engineering Institute. (2003). “Before You Connect a New Computer to the Internet.” *CERT® Coordination Center*. http://www.cert.org/tech_tips/before_you_plug_in.html (30 December 2003).

Carr, David F. “Case 101 – A Dissection – U.N. Mission in Sierra Leone – On the Edge of Peace.” *Baseline Magazine* No. 26 (January 2004): pp. 32–52.

Carr, Jack, Mathewson, Frank, and Neil Quigley. 1995. Stability in the absence of deposit insurance: the Canadian banking system, 1890–1966. Journal of Money, Credit & Banking. Vol. 27, No. 4: 1137–59.

Carrier, Brian. (2002). Atstake Corporate White Paper. “Open Source Digital Forensics Tools: The Legal Argument.” pp. 1–11. http://www.atstake.com (30 December 2003).

Casey, James and Frances Picherack. (2003). *The Regulation of Complementary and Alternative Health Care Practitioners: Policy Considerations*. Health Systems Division-Health Canada http://www.hc-sc.gc.ca/hppb/healthcare/pubs/comp_alt/regs.html#t3 (12 February 2004).

CATA Alliance. (2004). “Cyber Security at the Top of CATA's Business Agenda.” http://www.cata.ca/Media_and_Events/Press_Releases/cata_pr02090401.html (10 February 2004).

CED Magic Web Site. (1981). “The IBM Personal Computer is Introduced.” *CED in the History of Media Technology*. http://www.cedmagic.com/history/ibm-pc-5150.html (1 March 2004).

Cerf, Vinton G. *et al*. (2003). “A Brief History of the Internet.” *Internet Histories*. http://www.isoc.org/internet/history/brief.shtml (19 February 2004).

Cerf, Vinton G. (2001). “A Brief History of the Internet and Related Networks.” *Internet Histories*. http://www.isoc.org/internet/history/cerf.shtml (19 February 2004).

Cerf, Vinton G. (1997). “Computer Networking: Global Infrastructure for the 21st Century.” *Computing Research Association*. http://www.cs.washington.edu/homes/lazowska/cra/networks.html (17 February 2004).

Chabrow, Eric. (2004). “GAO Faults 'Inconsistent' Online Security Programs.” *Information Week*. http://www.informationweek.com/shared/printableArticle.jhtml?articleID=17301563 (30 January 2004).

CICA – Accounting Standards Oversight Council. (2003). *Meeting the Challenge – Annual Report 2002–2003 of the Accounting Standards Oversight Council*. http://www.cica.ca/index.cfm/ci_id/15410/la_id/1.htm (2 March 2004).

Claburn, Thomas. (2004). “The Password Is: Liability.” *Information Week.* http://www.informationweek.com/shared/printableArticle.jhtml?articleID=18200511 (26 February 2004).

Clarke, Richard, and Lee Zeichner. (2004). “How To Protect Yourself Against Hackers.” *Internet Week*. http://interactiveage.com/security02/showArticle.jhtml?articleID=17200532 (8 January 2004).

CNN.com Staff. (2004). “Expert: Microsoft dominance poses security threat – Biology stirs software 'monoculture' debate.” http://www.cnn.com/2004/TECH/biztech/02/16/microsoft.monoculture.ap/index.html (17 February 2004).

Coffer, Walter, and Luces M. Faulkenberry. *Electrical Power Distribution and Transmission*. Englewood Cliffs: Prentice-Hall, Inc., 1996.

Cohen, Marjorie G. (2001). From public good to private exploitation: GATS and the restructuring of Canadian electrical utilities. Canadian-American Public Policy. Vol. 48: 1–79.

Collins, Tony. (2001). “Chinook pilots may have been unable to slow down, squadron leader tells Lords.” *Computer Weekly*. http://www.computerweekly.com/Article106950.htm (5 February 2004).

Collins, Tony. “Lives on the line?” *Computer Weekly* (27 July 1995): pp. 26–28.

Collins, Tony. (2001). “Lords vote to undertake limited Chinook inquiry.” *Computer Weekly*. http://www.computerweekly.com/Article101370.htm (5 February 2004).

Collins, Tony. (2002). “MoD refuses to concede error in Chinook verdict.” *Computer Weekly*. http://www.computerweekly.com/Article114442.htm (5 February 2004).

Collins, Tony. (2001). “RAF chiefs rubbish software claims.” *Computer Weekly*. http://www.computerweekly.com/articles/article.asp?liArticleID=108277&liArticleTypeID=1&liCategoryID=2&liChannelID=28&liFlavourID=1&sSearch=&nPage=1 (5 February 2004).

Collins, Tony. (2002). “Victory! Lords confirm CW stand – software flaw could have caused Chinook crash.” *Computer Weekly*. http://www.computerweekly.com/Article109778.htm (5 February 2004).

Compass Inc. (2002). “National Study of Academic Researchers.” http://www.ocipep.gc.ca/research/scie_tech/CI/climatechg/2002-D012_e.asp (30 December 2003).

Computer Hope Web Site. (2004). “Programming Definitions.” http://www.computerhope.com/jargon/program.htm (2 March 2004).

Computer Science and Telecommunications Board – National Research Council. (2002). *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. http://www.cybersecure.ca/popl.pdf (23 January 2004).

Computer Weekly Staff. (2000). “Defence Minister misleads MPs over Chinook accident.” *Computer Weekly*. http://www.computerweekly.com/Article20211.htm (5 February 2004).

Computer Weekly Staff. (2002). “Lessons to be learned from Chinook tragedy.” *Computer Weekly*. http://www.computerweekly.com/Article109772.htm (5 February 2004).

Cooper, Charles. (2003). “Lock 'em up for substandard software.” http://zdnet.com.com/2100-1104_2-5129641.html (19 December 2003).

Cornish, Bill. (2001). “Wireless Devices and the New Security Challenges.” *CanCERT Bulletin* Vol. 4, No. 2 (August 2001): pp. 6–17 http://www.cancert.ca/Bulletins/CanCERT_Bulletin_Vol4_No2.pdf (9 March 2004).

Costa, J. Keith. (2001). “Concerned about threats to critical infrastructures...Canadian official calls for Cyber-Security Exercise with United States.” *Inside the Pentagon*. http://www.ocipep.gc.ca/whoweare/articles/article_ipent1_e.asp (30 December 2003).

Costa, J. Keith. (2002). “While reaching out to Washington, other allies…Canada forges ahead with master plan to guard key infrastructures.” *Inside the Pentagon*. (30 December 2003). http://www.ocipep.gc.ca/whoweare/articles/article_ipent2_e.asp

Coursey, David. (2004). “Why broadband over power lines is a bad idea.” *ZD Net Anchor Desk* http://reviews-zdnet.com.com/AnchorDesk/4630-7298_16-5123406.html?tag=print (3 March 2004).

Cox, Mark. (2004). “Customers still in dark about blackouts: Accenture study.” *ConnectIT* http://www.integratedmar.com/connectIT/story.cfm?item=367 (16 February 2004).

Crawford, C. Merle, C. Anthony Di Benedetto and Roger J. Calantone. *New products Management*. New York: Irwin McGraw-Hill, 2000.

Customer Relationship Management Research Center. (2004). http://www.cio.com/research/crm (28 February 2004).

Cusumano, Michael A. (2004). Who is Liable for Bugs and Security Flaws in Software? Communications of the ACM. Vol. 47, No. 3: 25–27.

D. Scott Campbell & Associates Inc., Lipchak, Andrew and McDonald, John. (2002). *A Case for Action for Information Management*. http://www.archives.ca/06/docs/action_e.pdf (23 January 2004).

Daly, Brian. “Experts say personal information, networks vulnerable as Internet grows.” *Canadian Press News Wire* (27 August 2002).

Daniels, Ron and Michael J. Trebilcock. (2000). Electricity Restructuring: The Ontario Experience. The Canadian Business Law Journal. Vol. 33, No. 2: 161–192.

Darby, Chris, Geer, Dr. Daniel, Germanow, Abner, and Chris Wysopal. (2002).“The Injustice of Insecure Software.” pp. 1–6. http://www.atstake.com (30 December 2003).

Darko, Anima. (2002). “Computer Aided Disaster.” http://www.ee.ualberta.ca/~musilek/cmpe510/Computer_Aided_Disaster.pdf (5 February 2004).

Darroch, James L. 1992. Global competitiveness and public policy: the case of Canadian multinational banks. Business History. Vol. 34, No.3: 153–176.

Darwinmag.com. (2002). “Service level Agreements.” *Darwin Magazine.* http://embedded.com/98/9805br.htm (9 February 2004).

Darwinmag.com. (2002). “Service level Agreements – Overview.” *Darwin Magazine.* http://guide.darwinmag.com/technology/outsourcing/sla/index.html?action=print (9 February 2004).

Davis, Tom. (2003). “2003 Federal Computer Security Report Card.” *Committee on Government Reform*. http://www.reform.house.gov/TIPRC/Hearings/EventSingle.aspx?EventID=652 (10 December 2003).

DeMarco, Tom and Timothy Lister eds. *Software State-of-the-Art: Selected Papers.* New York: Dorset House Publishing, 1990.

Devlin, Dennis. (2002). “Primum Non Nocere.” *Secure Business Quarterly*. Vol. 2, Issue 3. http://www.sbq.com (30 December 2003).

Digital Defence. (2002). “5 Charged In Child Porn Case.” *Information Security News 2002.* http://digitaldefence.ca/news/2002_020123.htm (26 February 2004).

Doss, David and William Yurcik. (2002). “CyberInsurance: A Market Solution to the Internet Security Market Failure.” In *Workshop on Economics and Information Security*, University of California, Berkeley May 2002. http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/53.pdf (3 February 2004).

Dowd, Kevin. 1994. Competitive banking, bankers' clubs and bank regulation. Journal of Money, Credit & Banking. Vol. 26, No. 2: 289–308.

Doyle, Chris. (1997). Self regulation and statutory regulation. Business Strategy Review. Vol. 8, No. 3: 35–43.

Duke Law and Technology Review. (2002). “Protecting the Homeland by Exemption: Why the Critical Infrastructure Information Act of 2002 will degrade the Freedom of Information Act.” http://www.law.duke.edu/journals/dltr/articles/2002dltr0018.html (30 December 2003).

Duncan, Jim. (2002). “Responsible Vulnerability Disclosure: Challenges for Vendors Whose Products Are Infrastructural.” *Secure Business Quarterly*. Vol. 2, Issue 3. http://www.sbq.com/sbq/vuln_disclosure/sbq_disclosure_vendor_challenges.pdf (29 January 2004).

Dutt, Robert. (2004). “MyDoom spawns another sequel.” http://www.integratedmar.com/connectit/story.cfm?item=355 (11 February 2004).

Dvorak, John C. (2004). “The Big One.” *Newsweek.* http://www.pcmag.com/article2/0,4149,1490702,00.asp (4 February 2004).

Easynet Group. (2004). *Investor Information Glossary*. http://www.easynet.com/investorinfo/investorinfo_glossary.asp (11 February 2004).

Evans, Bob. (2004). “Business Technology: Keep Apps Simple As Possible, No Simpler.” *Information Week.* http://www.informationweek.com/story/showArticle.jhtml?articleID=17700250 (17 February 2004).

EWeek-Enterprise News and Reviews Staff. (2004). “Linux & Open Source,” *EWeek-Enterprise News and Reviews.* http://www.eweek.com/category2/0,4148,1237915,00.asp (1 March 2004).

Evans, Mark. (2003). “Rogers Edges Toward Telephony War v. BCE ‘Prudent For Us’: Will Start Service Using Internet By 2005, Says CEO.” *National Post* http://www.vonage.com/corporate/press_news.php?PR=2003_12_10_1 (2 March 2004).

Fabian, Robert. (2004). “Should Software Professionals be licensed?” *IT World Canada*. http://www.itworld.com/Career/3710/040105itlicense/pfindex.html (8 January 2004).

Farber, Dan. (2003). “Massive software engineering reform a must.” http://techupdate.zdnet.com/techupdate/stories/main/Massive_software_engineering_reform_is_a_must.html (12 December 2003).

Fisher, Dennis. (2004). “IT Losing Ground in Virus Battle.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=117996,00.asp (2 February 2004).

Fisher, Dennis. (2004). “Newest Trojan: Disguised to Do Damage.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/article2/0,4149,1429886,00.asp (2 February 2004).

Fisher, Dennis. (2003). “Report: Windows' Dominance a Hindrance to Security.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=107975,00.asp (2 February 2004.)

Fisher, Dennis. (2004). “Security Maven Calls for Internet 'Disease Control' Agency.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=117881,00.asp (2 February 2004).

Fisher, Dennis. (2004). “Security Vendors Partner to Improve Threat Response Time.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=115726,00.asp (9 January 2004).

Fisher, Dennis. (2002). “Software Liability Gaining Attention.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=21030,00.asp (30 January 2004).

Fitzsimons, Adrian P., Levine, Marc H., and Joel G. Siegel. 1995. Comparability of accounting and auditing in NAFTA countries. The CPA Journal. Vol. 65, No. 5: 38–45.

Forno, Richard. (2004). “Anti-virus industry: white knight or black hat?” *The Register UK*. http://www.theregister.co.uk/content/55/35579.html (17 February 2004).

Foster, Ed. “It's time to act: let's require vendors to disclose known bugs and incompatibilities.” *InfoWorld* Vol. 18, No. 10 (4 March 1996): pp. 56–57.

Foster, Scott. (2004). “Agriculture group puts safe food tracking on the menu.” *IT Businesss.ca*. http://www.itbusiness.ca/index.asp?theaction=61&sid=54738# (9 February 2004).

Foster, Scott. (2003). “E-marketers unite to address spam debate.” *IT Businesss.ca.* http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=53943 (17 February 2004).

Foster, Scott. (2004). “Industry on hold for CRTC VoIP decision.” *IT Businesss.ca.* http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=54816 (17 February 2004).

Foster, Scott. (2003). “Virus victims weigh cyber-insurance options: insurance providers offer policies to cover corporate damage caused by worms such as Blaster.” *Computing Canada*. http://www.findarticles.com/m0CGC/19_29/108992880/p1/article.jhtml (27 February 2004).

Fratto, Mike. (2004). “The 2004 Security Survivor’s Guide.” *Internet Week*. http://www.internetweek.com/breakingNews/showArticle.jhtml?articleID=17100035 (6 January 2004).

Freedman, David F. “Smart Machines.” *Inc.* (15 November 1999): p. 180.

Fried, Ina. (2003). “Is bulked-up HP ready for battle?” http://zdnet.com.com/2102-1103_2-5116531.html?tag=printthis (10 December 2003).

Friedland, Martin L. (2002). “Notes for *The University of Toronto – A History*.” University of Toronto Press http://www.utppublishing.com/uoft_history/notes/notes_chapter39.pdf (4 March 2004).

Fyfe, Stephen and William McLean. (2002.) Opportunities for Municipally Owned Corporations in Ontario's Electricity Market. Canadian Tax Journal. Vol. 50, No. 3: 970–1010.

Gage, Debbie. (2004). “Should the Government Regulate Internet Security?” *Baseline Magazine.* http://www.baselinemag.com/print_article/0,1406,a=120340,00.asp (3 March 2004).

Gage, Debbie, and John McCormick. (2004). “Can Software Kill?” *EWeek-Enterprise News and Reviews.* http://www.eweek.com/print_article/0,1761,a=121063,00.asp (9 March 2004).

Gage, Debbie, and John McCormick. (2004). “We Did Nothing Wrong.” *Baseline Magazine.* http://www.baselinemag.com/print_article/0,1406,a=121048,00.asp (11 March 2004).

Galli, Peter. (2004). “Novell to Offer Linux Indemnification Program.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=116219,00.asp (13 January 2004).

Ganssle, Jack. (1998). “Disaster.” *Break Points*. http://embedded.com/98/9805br.htm (9 February 2004).

Geer, Dan *et al*. (2003).“Cyber*In*security: The Cost of Monopoly – How the Dominance of Microsoft’s Products Poses a Risk to Security.” *Computer & Communications Industry Association*. http://www.ccianet.org/papers/cyberinsecurity.pdf (28 February 2004).

Geer Jr., Dr. Daniel E. (2002). “What is Vulnerability Disclosure?” *Secure Business Quarterly*. Vol. 2, Issue 3. http://www.sbq.com (30 December 2003).

Ghosh, Anup K. and Michael J. Del Rosso. (1999). “The Role of Private Industry and Government in Critical Infrastructure Assurance.” http://www.isi.edu/gost/cctws/delroso-ghosh.PDF (3 February 2004).

Gibbs, Nancy. “Lights Out: First the good news: the biggest blackout ever in North America brought out the best in millions of citizens. Now the bad: it exposed a woefully fragile electrical system. How did it happen? And how vulnerable are we to another shutdown?” *Time* Vol. 162, No. 8 (25 August 2003): pp. 30–36.

Gilbertson Davis Emerson LLP. (2000). *Nostradamus' Strategy For Millennium Bug Litigation:"I Told You So."* http://www.gilbertsondavis.com/publications/nostra_strategy.htm (2 March 2004).

Goodwins, Rupert. (2004). “Software lessons from Mars.” *News Commentary*. http://zdnet.com.com/2102-1107_2-5148988.html?tag=printthis (29 January 2004).

Greiner, Lynn. “Demand more accountability from vendors.” *Computing Canada* Vol. 24, No. 47 (14 December 1998): pp. 17–19.

Gross, Grant. (2003). “Gov’t agency uses buying power to encourage security.” http://www.infoworld.com/article/03/09/23/Hngovbuying_1.html (30 December 2003).

Hachman, Mark. (2004). “RSA Panel: Cryptography Can't Foil Human Weakness.” *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=120168,00.asp (25 February 2004).

Hamilton, Tyler. (2004). “Music Groups Appeal Copyright Ruling.” *The Toronto Star*. http://www.thestar.ca/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1074035410130&call_pageid=970599109774&col=Columnist971715454851 (15 January 2004).

Handa, Sunny, Johnston, David and Charles Morgan. *Cyberlaw –W hat You Need to Know about Doing Business Online*. Toronto: Stoddart Publishing Co., 1997.

Hardin, Garrett. (1968). “The Tragedy of the Commons.” *Science* 162 (1968): 1243–1248. http://www.dieoff.com/page95.htm (19 February 2004).

Harlick, James E. Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “Canadian Information Technology Security Symposium.” http://www.ocipep.gc.ca/whoweare/speeches/jh_cits_e.asp (30 December 2003).

Hasan, Ragib. (2002). “History of Linux.” *Department of Computer Science University of Illinois at Urbana-Champaign*. https://netfiles.uiuc.edu/rhasan/linux/ (1 March 2004).

Health Canada. (2002). "Limits of Human Exposure to Radiofrequency Electromagnetic Fields in the Frequency Range from 3 KHz to 300 GHz – Safety Code 6." *Consumer and Clinical Radiation Protection.* http://www.hc-sc.gc.ca/hecs-sesc/ccrpb/publication/99ehd237/chapter1.htm (9 March 2004).

Health Professions Regulatory Advisory Council. (1999). *Weighing the Balance – A Review of the Regulated Health Professions Act – Request for Submissions*. http://www.hprac.org/downloads//fyr/weighing.pdf (13 February 2004).

Heckman, Carey. (2003). "Two Views on Security Software Liability: Using the Right Legal Tools." *IEEE Security & Privacy*. Vol. 1, No. 1 (January/February 2003): pp. 73–75. http://csdl2.computer.org/dl/mags/sp/2003/01/j1073.htm (24 February 2004).

Help Desk Solutions. (1999). "Changes in the Customer Support Industry." *Computer News.* http://www.helpdesksolutions.com/Publications/change_support.htm (27 February 2004).

Hewitt, Michael. "FYI: Recent Canadian decisions on accountants' liability (1997–2001)." *Beyond Numbers* (1 October 2002): pp. 28–32.

Hobby, Jason. "See you in court." *Computer Weekly* (26 October 1995): pp60–62.

Hoffman, Steve. 1996. Enhancing power grid reliability. EPRI Journal. Vol. 21, No.6: 6–15.

Holloway, Derek. (1992). "Liability Implications of CADD." *Loss Control Information – Architects and Engineers.* Bulletin 91 (January 1992). http://www.encon.ca/english/lcb/bulletins/display.cfm?ID=29 (9 February 2004).

House of Representatives. (2002). *Cyber Security Research and Development Act*. http://www.house.gov/science/hot/cyber/cyberfile.pdf (29 January 2004).

Howe, Walt. (2004). *Walt's Internet Glossary – Glossary of Internet Terms*. http://www.walthowe.com/glossary/n.html (22 February 2004).

Hrab, Roy and Michael J. Trebilcock. (2003). What will keep the lights on in Ontario: responses to a policy short-circuit. C.D. Howe Institute Commentary. 191–220.

Huber, Peter, and Mark Mills. "Brawn & Brains." *Forbes* Vol. 172, No. 5 (15 September 2003): pp: 46–48.

Hulme, George V. (2004). "Application Security Standard Edges Forward." *Internet Week.* http://www.internetweek.com/shared/printableArticle.jhtml?articleID=18100224 (24 February 2004).

Hulme, George V. (2004). "Security Threats Won't Let Up This Year." *Internet Week.* http://www.internetweek.com/shared/printableArticle.jhtml?articleID=17200253 (8 January 2004).

Hulme, George V. (2003). “Spending To Fend Off Online Attacks Grows In 2004.” *Information Week*. http://www.informationweek.com/story/showArticle.jhtml;jsessionid=OO0GE5JL5WV1KQSNDBCSKHQ?articleID=17100128 (29 December 2003).

Huuhtanen, Matti. (2004). “'Mydoom' Creators Start Up 'Doomjuice'” http://apnews.myway.com/article/20040210/D80KGV5O0.html (11 February 2004).

Hyder, Elaine B. et al. (2002). “eSourcing Capability Model for IT-enabled Service Providers v1.1.” *CMU-CS-02-155 – Computer Science Department – School of Computer Science – Carnegie Mellon University*. http://itsqc.srv.cs.cmu.edu/escm/documents/eSCM_Model_1.1.pdf (11 February 2004).

Iacobucci, Edward, Trebilcock, Michael J., and Ralph A. Winter. (2003). “Economic Deregulation of Network Industries Managing the Transition to Sustainable Competition.” http://128.100.167.70/pages/DEREGULATION_MAY%2015%202003.doc. (16 February 2004).

IBM Corp. (2004). “Linux at IBM,” http://www-1.ibm.com/linux/ (27 February 2004).

IBM Corp. (2004). *IBM Deep Computing Institute*. http://www.research.ibm.com/dci/cat4_domain.shtml (5 March 2004).

ICB Toll Free News. (2000). “Dot Com Wars.” http://icbtollfree.com/article.cfm?articleId=1399 (3 February 2004).

IEEE Computer Society. (2004). “History of the Joint IEEE Computer Society and ACM Steering Committee for the Establishment of Software Engineering as a Profession.” http://www.computer.org/tab/seprof/history.htm (28 February 2004).

Ihnatko, Andy. “Right-protected software.” *MacUser* Vol. 9, No. 3 (March 1993): pp29–34.

Industry Canada. (1999). “RSS-102 – Evaluation Procedure for Mobile and Portable Radio Transmitters with respect to Health Canada's Safety Code 6 for Exposure of Humans to Radio Frequency Fields.” *Spectrum Management and Telecommunications Policy – Radio Standards Specification*. http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/vwapj/rss102.pdf/$FILE/rss102.pdf (9 March 2004).

Industry Canada. (2004). “Digital Apparatus.” *Spectrum Management and Telecommunications Policy – Interference-Causing Equipment Standard*. http://strategis.ic.gc.ca/epic/internet/insmtgst.nsf/vwapj/ices003e.pdf/$FILE/ices003e.pdf (9 March 2004).

Industry Canada. (2004). "RSS-192 – Fixed Wireless Access Equipment Operating in the Band 3450–3650 MHz." *Spectrum Management and Telecommunications Policy – Radio Standards Specification*. http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/vwapj/rss192e.pdf/$FILE/rss192e.pdf (9 March 2004).

Industry Canada. (2004). "RSS-195 – Wireless Communications Service Equipment Operating in the Bands 2305–2320 MHz and 2345–2360 MHz." *Spectrum Management and Telecommunications Policy – Radio Standards Specification*. http://strategis.ic.gc.ca/epic/internet/insmtgst.nsf/vwapj/rss195e_dec30.pdf/$FILE/rss195e_dec30.pdf (9 March 2004).

InfoSec Research Council. (1999). "National Scale INFOSEC Research Hard Problems List."http://www.infosec-research.org/docs_public/IRC-HPL-as-released-990921.doc (9 February 2004).

Institute for Information Infrastructure Protection. (2002). *National Information Infrastructure Protection – Research and Development Agenda Initiative Report – Information InfrastructureProtection: Survey of Related Roadmaps and R &D Agendas.* http://www.thei3p.org/documents/analyses/I3P_Roadmap_Analysis_V1.0s.pdf (10 March 2004).

INTEL Corp. (2002). "Expanding Moore's Law – The Exponential Opportunity" *Intel Technology Update* (Fall, 2002) ftp://download.intel.com/labs/eml/download/EML_opportunity.pdf (2 March 2004).

INTEL Corp. (2002). "Moore's Law". http://www.intel.com/research/silicon/mooreslaw.htm (28 February 2004).

Isenberg, Doug. (2004). "Unexpected twists in Internet law" http://zdnet.com.com/2100-1107_2-5134877.html (6 January 2004).

IT Cortex. (2004). "Failure Rate." http://www.it-cortex.com/Stat_Failure_Rate.htm (27 February 2004).

IT Disaster Recovery Planning. (2003). *Ensuring Business Continuity with Effective Asset Availability Management Conference*. http://www.drie.org/documents/ITDRP.pdf (30 December 2003).

IT World.com. (2001). "10 myths about service-level agreements." http://www.itworld.com/Man/2679/ITW010427sla/ (9 February 2004).

Jackson, William. "Frustrated lawmakers prod justice, vendors for accountability in worm and virus crimes." *Government Computer News* Vol. 22, No. 28 (22 September 2003): pp. 13–14.

Jackson, William. “IT, power grids not primary terror targets, FBI says.” *Government Computer News* Vol. 22, No. 27 (15 September 2003): pp. 12–13.

Jacquith, Andrew. (2002). Atstake Corporate White Paper. “The Security of Applications: Not all are Created Equal.” pp. 1–12. http://www.atstake.com (30 December 2003).

Jerome, Marty. “Software Safeguards.” *PC/Computing* Vol. 3, No. 2 (February 1990): pp. 119–121.

Jesdanun, Anick. (2004). “GE Energy acknowledges blackout bug.” *The Associated Press* http://www.securityfocus.com/printable/news/8032 (16 February 2004).

Jesper / Laisen / DK. (2001). “Hack, Hackers, and Hacking.” http://www.laisen.dk/Hack__Hackers__and_H.1233.0.html (5 March 2004).

Johnson, R. Colin. “Power-grid planners plug in to neuro-fuzzy.” *Electronic Engineering Times* (27 September 1999): pp. 73–74.

Joyce, Ed. “Software bugs: a matter of life and liability”. *Datamation* Vol. 33, No. 10 (15 May 1987): pp. 88–97.

Kadlec, R.E. (1993). Winds of change in utility regulation. Canadian Business Review. Vol. 20, No. 4: 39–42.

Kahney, Leander. (2003). “Fast Track for Science Data.” *Wired News*. http://www.wired.com/news/print/0,1294,61102,00.html (17 November 2003).

Kane, Edward J. 1996. De jure interstate banking: why only now? Journal of Money, Credit & Banking. Vol. 11, No. 2: 141–161.

Kanellos, Michael. (2004). “Is security getting any easier?” *CNET News.com*. http://zdnet.com.com/2102-1105_2-5164431.html?tag=printthis (25 February 2004).

Kaner, Cem. (1999). “The Future of Software Liability.” *Cem Kaner Testing Computer Software Conference June 1999*. http://www.kaner.com/pdfs/uspdi_keynote.pdf (30 January 2004).

Kaner, Cem. (2000). “Why You Should Oppose UCITA.” http://www.badsoftware.com/claw2000.htm (4 February 2004).

Keizer, Greg. (2003). “Phishing Attacks Soar.” *Internet Week*. http://www.internetweek.com/shared/printableArticle.jhtml?articleID=17100208 (6 January 2004).

Keizer, Greg. (2003). “Security: From Bad to Worse?” *Information Week*. http://www.informationweek.com/shared/printableArticle.jhtml?articleID=17100254 (5 January 2004).

Kenneally, Erin. (2001). “Stepping on the digital scale – Duty and Liability for Negligent Internet Security.” *;login: The Magazine of USENIX & SAGE*. Vol. 26, No. 8 (December 2001): pp. 62–77. http://www.usenix.org/publications/login/2001-12/pdfs/kenneally.pdf (24 February 2004).

Kenneally, Erin. (2002). “Who’s Liable for Insecure Networks?” *IEEE Security & Privacy*. Vol. 35, No. 6 (June 2002): pp. 93–95. http://csdl2.computer.org/dl/mags/co/2002/06/r6093.htm (24 February 2004).

King, Michael C. “An Introduction to the Health Professions Act.” Calgary Regional Health Authority. http://www.calgaryhealthregion.ca/clin/adultpsy/articles/hpa2.pdf. (4 February 2004).

Kleinrock, Leonard. “Information Flow in Large Communication Nets.” *RLE Quarterly Progress Report* (July 1961).

Koerner, Brendan I. “Bugging Out – Is your software screwing up? Tough.” *The New Republic* (27 November 2000): pp. 13–15.

Krebs, Brian. (2003). “Gov’t Computer Security Lagging – Report.” *The Washington Post*. http://www.washingtonpost.com/ac2/wp-dyn/A49030-2003Dec9?language=printer (10 December 2003).

Labaton, Stephen. (2004). “F.C.C. Begins Rewriting Rules on Delivery of the Internet.” *The New York Times on the Web*. http://www.nytimes.com/2004/02/12/technology/12CND-NET.html?ex=1077682218&ei=1&en=7d5a82c84583aff0 (23 February 2004).

Law Society of Upper Canada. (2003). *Emerging Issues Committee – Report to Convocation* (26 June 2003). http://www.lsuc.on.ca/news/pdf/convjune03_emergingissues.pdf (4 February 2004).

Leech, John. (2002). “Our Shared Responsibility: Interview with Margaret Purdy.” *Canadian Government Executive Magazine*. http://www.ocipep.gc.ca/whoweare/articles/article_ipent3_e.asp (30 December 2003).

Lemos, Robert. (2003). “A two-pronged approach to cybersecurity.” *The Washington Post*. http://www.washingtonpost.com/ac2/wp-dyn/A49030-2003Dec9?language=printer (3 December 2003).

Lemos, Robert. (2003). “Bush unveils final cybersecurity plan.” http://zdnet.com.com/2102-1105_2-984697.html?tag=printthis (10 December 2003).

Lemos, Robert. (2003). “Feds get a ‘D’ in computer security.” http://zdnet.com.com/2102-1105_2-5118344.html?tag=printthis (10 December 2003).

Lemos, Robert. (2004). “Government planning cyberalert system.” *CNET News.com* http://news.com.com/2102-7348_3-5148708.html?tag=st_util_print (29 January 2004).

Lemos, Robert. (2003). “Report: Microsoft dominance poses security risk.” http://zdnet.com.com/2102-1105_2-5081214.html?tag=printthis (29 January 2004).

Lemos, Robert. (2004). “Security a work in progress for Microsoft.” http://zdnet.com.com/2102-1105_2-5141765.html (16 January 2004).

Lemos, Robert. (2004). “Tracking the seeds of destruction.” http://zdnet.com.com/2102-1105_2-5140991.html (16 January 2004).

Lemos, Robert, and Declan McCullagh. (2002). “Cybersecurity plan lacks muscle.” http://zdnet.com.com/2100-1105-958545.html?tag=nl (10 December 2003).

Leveson, Nancy G. 1991. Software safety in embedded computer systems. Communications of the ACM. Vol. 34, No. 2: 34–45.

Leyden, John. (2004). “Flaw on Tuesday, exploit by Monday.” *The Register UK*. http://www.theregister.co.uk/content/55/35592.html (17 February 2004).

Leyden, John. (2004). “Windows source code exploit released.” *The Register UK*. http://www.theregister.co.uk/content/55/35611.html (17 February 2004).

Lewis, Ted G. and Paul W. Oman eds. *Milestones in Software Evolution* Los Angeles: IEEE Computer Society Press, 1990.

Linden, Allen M. *Canadian Tort Law*, 5th ed. Toronto: Butterworths, 1993.

Lohr, Steve. (2003). “Product Liability Lawsuits Are New Threat to Microsoft.” *The New York Times.* http://www.lexisone.com/news/n100603a.html (2 March 2004).

Lowenstein, Frank. “Software Liability.” *Technology Review* Vol. 90 (January 1987): pp. 9–10.

Madar, Daniel. 2002. Rail mergers, trade, and federal regulation in the United States and Canada. Publius. Vol.32, No. 1: 143–159.

Mann, Charles C. (2002). “Why software is so bad ... ... and what's being done to fix it.” *MSNBC Technology and Science.* http://www.cs.queensu.ca/~dingel/whySWIsSoBad.pdf (5 March 2004).

Marron, Keith. (2003). “New audit rules count for IT departments.” *The Globe and Mail*. http://www.globetechnology.com/servlet/story/RTGAM.20031210.wsarb1210/BNPrint?Technology/?main (11 December 2003).

Matthews, Ian. (2003). "The Amazing Commodore PET." *Commodore Business Machines Product Line Up*. http://www.commodore.ca/products/pet/commodore_pet.htm (22 February 2003).

McCullagh, Declan. (2004). "New security law sacrifices privacy." *CNET News.* http://zdnet.com.com/2100-1107-5155462.html?tag=sas.email (10 February 2004).

McFadden, David. "Power to the people: The opening of Ontario's electricity market is not just a Get-rich scheme for a greedy few. It will benefit the economy, the environment and Consumers." *Financial Post* (*National Post*) (2 May 2002): FP 15.

McGeary, Johanna. "An Invitation To Terrorists?" *Time* Vol. 162, No. 8 (25 August 2003): p. 38.

McGraw, Gary and Greg Morrisett. (2000). "Attacking Malicious Code: A Report to the Infosec Research Council." *IEEE Software.* (September–October 2000): pp. 33–41 http://www.infosec-research.org/docs_public/ISTSG-MC-report.pdf (10 March 2004).

Mead, Nancy R. (2003). "International Liability Issues for Software Quality." *CERT Research Center Special Report CMU/SEI-2003-SR-001*. http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03sr001.pdf (24 February 2004).

Mears, Jennifer. (2004). "SCO renews threats; Novell offers indemnification." *Network World Fusion.* http://www.nwfusion.com/news/2004/0119linuxidem.html (2 March 2004).

MEMS and Nanotechnology Clearinghouse. (2004). "What is MEMS Technology?" http://www.memsnet.org/mems/what-is.html (February 23, 2004).

Meyer, Gabriel S, Raul, Alan Charles, and Frank R. Volpe. (2001). "Liability for Computer Glitches and Online Security Lapses." *BNA Electronic Commerce Law Report* Vol. 6, No. 31 (8 August 2001): 849 http://www.sidley.com/cyberlaw/features/liability.asp (27 February 2004).

Moffina, Rick and Mike Blanchfield. "Canada's cyber network, pipelines and power grids, which are all tied to the United States, are the most likely targets of terrorists." *CanWest News* (21 December 1999): pp. 1–3.

Moore, Gordon E. (1965). "Cramming more components onto integrated circuits." *Electronics* Vol.38, No. 8 (19 April 1965). ftp://download.intel.com/research/silicon/moorespaper.pdf (1 March 2004).

Morgan, Brian. "New Liabilities." *CA Magazine* Vol. 136, No. 5 (1 June 2003): pp. 34–36.

Morrissey, Jane. "Lawmakers to Consumers: Tough Luck!" *PC World* Vol. 16, No. 10 (October 1998): p.70.

Mucklestone, Connie. (2001). “Strategic Plan Vision sparks lively discussion.” *March 26, 2001 meeting: Professional Engineers Ontario.* http://www.peo.on.ca/publications/DIMENSIONS/mayjune2001/MJ01InCouncil.pdf (1 March 2004).

Mueller, Milton. 1999. ICANN and Internet Regulation. Communications of the ACM. Vol. 42, No. 6: 41–45.

Munro, Jay. (2004). “Beating the New MyDoom (Windows) Variant.” *EWeek-Enterprise News and Reviews*. http://www.pcmag.com/print_article/0,3048,a=117754,00.asp (2 February 2004).

Myers, Edith. “End to as-is sales? Buyers want more protection, but the last thing vendors want are laws that say they must provide warranties with their products”. *Datamation* Vol. 31 (15 September 1985): pp. 68–70.

National Infrastructure Protection Center. (2002). *Risk Management: An Essential Guide to Protecting Critical Assets*. November 2002. http://www.nipc.gov/publications/nipcpub/P-Risk%20Management.pdf (28 December 2003).

Natkin, Kenneth H. 1994. Legal risks of design/build. Architecture. Vol. 83, No. 9: 125–129.

Neumann, Peter G. (1997). “Computer Security in Aviation: Vulnerabilities, Threats, and Risks.” *International Conference on Aviation Safety and Security in the 21st Century – White House Commission on Safety and Security, and George Washington University* http://www.gwu.edu/~cms/aviation/track_ii/neumann.html (12 February 2004).

Newton, John. (2003). “Federal Legislation for Disaster Mitigation: A Comparative Assessment between Canada and the United States.” http://www.ocipep.gc.ca/research/scie_tech/disMit/en_mitigat/1995_D014_e.asp (30 December 2003).

Nissenbaum, Helen. 1994. Computing and accountability. Communications of the ACM (Association for Computing Machinery). Vol. 37, No. 1: 72–81.

Norman, John. (2004). “Ontario’s electricity dilemma: crisis or opportunity?” *The Varsity.* http://www.thevarsity.ca/global_user_element?printpage.cfm?storyid=598305 (12 February 2004).

Nulty, Peter, and Edward Prewitt. “Utilities flirt with Adam Smith; respected utility executive are demanding greater freedom to buy, make, and transmit power.” *Time* Vol. 117, No. 12 (6 June 1988): pp. 173–178.

O'Neil, Michael. 2001. Cybercrime Dilemma. Brookings Review. Vol. 19, No. 1: 28–35.

OneStat.com. (2002). “Microsoft’s Windows OS global market share is more than 97% according to OneStat.com.” http://www.onestat.com/html/aboutus_pressbox10.html (4 March 2004).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “About Critical Infrastructure Protection.” http://www.ocipep.gc.ca/critical/index_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). *An Assessment of Canada’s National Critical Infrastructure Sectors*. http://www.ocipep.gc.ca (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “Disaster Mitigation.” http://www.ocipep.gc.ca/NDMS/consult_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2002). *DRAFT – Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets*. http://www.ocipep.gc.ca (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2001). “Emergency Preparedness Digest – Back Issues.” http://www.ocipep.gc.ca/ep/ep_digest/js_2001_feal_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “Federal Emergency Preparedness in Canada.” http://www.ocipep.gc.ca/info_pro/fact_sheets/general/backgd_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “International Consortium Releases List of the Top Twenty Internet Security Vulnerabilities.” http://www.ocipep.gc.ca/info_pro/NewsReleases/NR/2003/NR03-0810_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “Legislation – Emergency Preparedness in Alberta.” http://www.ocipep.gc.ca/ep/legisla/ep_ab/e_p_p_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “Microsoft SQL 2000 “Slammer” Worm – Impact Paper.” pp. 1–13. http://www.ocipep.gc.ca (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). “National Critical Infrastructure Assurance Program.” http://www.ocipep.gc.ca/info_pro/fact_sheets/general/CIP_NCIAP_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2002). "National Critical Infrastructure Assurance Program Discussion Paper." http://www.ocipep.gc.ca/critical/nciap/disc_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). "National Critical Infrastructure Assurance – The Case for Action." http://www.ocipep.gc.ca/critical/nciap/synopsis_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). "Search the Database." http://www.ocipep.gc.ca/disaster/search.asp?lang=eng. (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness. (2003). "The Government Emergency Operations Coordination Centre (GEOCC)." http://www.ocipep.gc.ca/info_pro/fact_sheets/general/EM_gov_em_op_e.asp (30 December 2003).

Office of Critical Infrastructure Protection and Emergency Preparedness (2003). "Threats to Canada's Critical Infrastructure." pp.1–59. http://www.ocipep.gc.ca (30 December 2003).

Oracle Corp. (2004). Oracle Web Site. http://www.oracle.com/ (4 March 2004).

Parnas, David L. 1990. Evaluation of safety-critical software. Communications of the ACM. Vol. 33, No. 6: 636–648.

Parsons, Patrick. 2003. The evolution of the cables-satellite distribution system. Journal of Broadcasting & Electronic Media. Vol. 47, No. 1: 1–16.

Patterson, Cynthia A. and Stewart D. Personick, eds. (2003). *Critical Information Infrastructure Protection and the Law – An Overview of Key Issues.* Washington, D.C.: The National Academies Press, 2003. http://books.nap.edu/catalog/10685.html (19 February 2004).

PC Magazine Staff. "Unintended Consequences – Blackouts and Worms." (18 August 2003).

PC Week Staff. "Better software and guarantees – Now. Complaints about Windows 98 raise questions about software quality control and vendor accountability." *PC Week* Vol. 15, No. 29 (20 July 1998): pp. 29–30.

Pelline, Jeff. (2004). "MyDoom downs SCO site." *CNET News.* http://zdnet.com.com/2102-1105_2-5151572.html?tag=printthis (2 February 2004).

Perks, Gord. (2004). "Revenge of the nerds." *Eye Weekly.* http://www.eye.net/eye/issue/print.asp?issue_02.19.04/city/enviro.html (19 February 2004).

Phillips, Douglas E. 1994. When software fails: emerging standards of vendor liability under the Uniform Commercial Code. Business Lawyer. Vol. 50, No. 1: 151–181.

Phipps, Steven. 2001. "Order Out of Chaos:" A Reexamination of the Historical Basis for the Scarcity of Channels Concept. Journal of Broadcasting & Electronic Media. Vol. 45, No. 1: 57–80.

Picarille, Lisa. “License law may limit liability.” *Computerworld* Vol. 31, No. 19 (12 May 1997): pp. 1–2.

Pink Elephant Inc. (2003). “The Benefits of ITIL White Paper.” http://www.pinkelephant.com/pdf/Benefits_of_ITIL.pdf (9 February 2004).

Pink Elephant Inc. (2003). “The ITIL Story.” http://www.pinkelephant.com/pdf/The_ITIL_Story.pdf (9 February 2004).

Poulsen, Kevin. (2004). “Gates 'optimistic' on security.” *SecurityFocus* http://www.securityfocus.com/printable/news/8111 (25 February 2004).

Poulsen, Kevin. (2003). “Slammer worm crashed Ohio nuke plant network.” *SecurityFocus* http://www.securityfocus.com/printable/news/6767 (16 February 2004).

Poulsen, Kevin. (2004). “Software Bug Contributed to Blackout.” *SecurityFocus* http://www.securityfocus.com/printable/news/8016 (16 February 2004).

Poulsen, Kevin. (2003). “Sparks over Power Grid Cybersecurity.” *SecurityFocus* http://www.securityfocus.com/printable/news/3871 (16 February 2004).

Protti, Raymond J. (2002). “Banking On Both Sides of the 49th Parallel: Addressing the Regulatory and Legislative Demands of an Integrated Market.” *Canadian Banker Magazine*. (January 2002). http://www.cba.ca/en/magazine/getArticle.asp?at_id=203&pm=true (11 February 2004).

Protti, Raymond J. (2002). “National Regulation: Time to Get On with the Job.” *Canadian Banker Magazine*. (January 2002). http://www.cba.ca/en/magazine/getArticle.asp?at_id=202&pm=true (11 February 2004).

Red Hat Inc. (2004). *About Red Hat – The Open Source Leader*. http://www.redhat.com/ (28 February 2004).

Reuters. (2003). “U.N. confab to see tussle over Net control.” http://zdnet.com.com/2100-1104_2-5113744.html (10 December 2003).

Ricadela, Aaron. (2001). “The State of Software Quality.” *Information Week* http://www.informationweek.com/838/quality.htm (12 February 2004).

Rogerson, Professor Simon. (2002). “The Chinook Helicopter Disaster.” (Originally published As ETHIcol in the IMIS Journal. Vol 12, No. 2 (April 2002). http://www.ccsr.cse.dmu.ac.uk/resources/general/ethicol/Ecv12no2.pdf (10 February 2004).

Rooney, Paula. (2004). “OSDL, IBM, Intel Launch SCO Legal Defense Fund For Users.” *Internet Week*. http://www.internetweek.com/shared/printableArticle.jhtml?articleID=17300517 (15 January 2004).

Rosch, W.C. “Are You Protected from Software Publishers' Slip-Ups?” *P.C. Week* Vol. 2, No. 3 (22 January 1985): pp. 28–29.

Rosch, W.L. “Reading Between The Lines: Software Warranties”. *P.C. Week* Vol. 1, No. 45 (13 November 1984): pp. 121–124.

Rosenbaum, Joseph. (2004). “Protect Thyself 101: A primer on indemnification.” *ZD Net Tech Update*. http://techupdate.zdnet.com/techupdate/stories/main/indemnification_primer_print.html (2 March 2004).

Rosencrance, Linda. (2003). “Hacker breaks into U.S. e-voting firm’s site.” *IT World Canada*. http://www.itworld.ca/Pages/Docbase/ViewArticle.aspx?ID=idgml-1a7072b3-a1bf-4d64-a099-caecde7c7a85 (6 January 2004).

Ruby, Daniel. “Who's responsible for the bugs?” *PC Week* Vol. 23, No. 1 (27 May 1986): pp. 51–57.

Sager, Ira. “The View from IBM.” *Business Week* (30 October 1995), http://www.businessweek.com/1995/44/b34481.htm (28 February 2004).

Salesforce.com. (2004). “Salesforce.com.” http://www.salesforce.com/ (4 March 2004).

Sam Palmisano Presentation Transcript. (2003). *IBM Business Leadership Forum – San Francisco* (12 November 2003) http://www.ibm.com/ibm/sjp/11-12-2003.shtml (26 February 2004).

Sammet, Jean E. *Programming Languages: History and Fundamentals* Englewood Cliffs: Prentice-Hall, 1969.

Samuelson, Pamela. 1993. Communications of the ACM (Association for Computing Machinery). Vol. 36, No. 1: 21–29.

SANS. (2003). “The Twenty Most Critical Internet Security Vulnerabilities (Updated) – the Experts Consensus.” http://www.sans.org/top20/. (30 December 2003).

Saydjari, O. Sami. (2004). Cyber Defense: Art to Science. Communications of the ACM. Vol. 47, No. 3: 53–57.

Scheier, Robert L. "Lock the damned door!" *Computerworld* Vol. 31, No. 6 (10 February 1997): pp. 66–69.

Schick, Shane. (2004). "How the downloading debate is starting to affect other areas of IT." *IT Business*.ca. http://www.itbusiness.ca/index.asp?theaction=61&sid=54933 (3 March 2004).

Schick, Shane. (2004). "Them's the rules." *IT Business*.ca. http://www.itbusiness.ca/print.asp?sid=54728 (5 February 2004).

Schiller, Jeffrey. (2002). "Response Vulnerability handling: 'A Hard Problem'." *Secure Business Quarterly*. Vol. 2, Issue 3. http://www.sbq.com/sbq/vuln_disclosure/sbq_disclosure_hard_problem.pdf (29 January 2004).

Schneier, Bruce. (2003). "Did Blaster cause the blackout?" http://zdnet.com.com/2102-1107_2-5118123.html?tag=printthis (9 December 2003).

Schneier, Bruce. (2002). "Fixing Network Security by Hacking the Business Climate." www.counterpane.com/presentation4.pdf (19 January 2004).

Schneier, Bruce. (New unpublished introduction for previously published book). *Secrets & Lies Digital Security in a Networked World*. New York: John Wiley & Sons, 2000.

Schneier, Bruce. (2004). "Total surveillance becoming reality." http://zdnet.com.com/2100-1107-5150608.html?tag=sas.email (3 February 2003).

Schoonmaker, Jim. (2004). "Security will ride shotgun with data in 2004." http://zdnet.com.com/2102-1107_2-5149942.html?tag=printthis (29 January 2004).

SearchCIO.com. (2004). "Sarbanes-Oxley Act. http://searchcio.techtarget.com/sDefinition/0,,sid19_gci920030,00.html (17 February 2004).

Seltzer, Larry. (2003). "Is Computer Monoculture The Way Of The World?" *EWeek-Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=108093,00.asp (2 February 2004).

Shankland, Stephen. (2004). "Red Hat offers software warranty." http://zdnet.com.com/2102-1104_2-5143326.html (21 January 2004).

Siklos, Pierre L. *Money, Banking and Financial Institutions – Canada in the Global Environment*. 2d ed. (Toronto: McGraw Hill Ryerson Limited, 1997.

Sikora, Vincent A. 2001. Public Agencies – Authority and Responsibilities. Journal of Environmental Health. Vol. 64, No. 1: 39.

Slofstra, Martin. "In conversation." (Interview with Daniel Cooper, computer law expert-partner in McCarthy Tetrault of Toronto). *Computing Canada* Vol. 16, No. 8 (12 April 1990): pp. 13–17.

Soat, John. (2003). "Cybersecurity Starts at Home(land)." *Information Week*. http://www.informationweek.com/story/showArticle.jhtml?articleID=16600192 (9 December 2003).

Stamp, Mark. 2004. Risks of Monoculture. Communications of the ACM. Vol. 47, No. 3: 120.

Starr, Paul. 2003. A license for power. The American Prospect. Vol. 14, No. 5: 21–22.

Statistics Canada. (2002). *North American Industry Classification (NAICS) 2002*. http://stds.statcan.ca/english/naics/2002/naics02-class-search.asp?criteria=813910 (8 February 2004).

Statistics Canada. (2003). "The computer industry." *Data and Computer*. http://www.statcan.ca/english/edu/power/ch4/industry/computers3.htm (24 February 2004).

Sun Microsystems, Inc. (2004). Internet Engineering group of Solaris Software http://playground.sun.com/pub/ipng/html/ipng-main.html (2 March 2004).

Surmacz, John. (2004). "Why Software Quality Still Stinks." *IT World Canada*. http://www.itworld.ca/Pages/Docbase/ViewArticle.aspx?ID=idgml-a7a11aa5-b6fa-4ad7-a9ef-d53b6acc01d1 (8 January 2004).

Sutton, Neil. (2004). "CATA forms alliance with cybersecurity specialist." *IT Business.ca.* http://www.itbusiness.ca/index.asp?theaction=61&sid=54757 (10 February 2004).

Taft, Darryl K. (2004). "Building Java, .Net Apps Sans Coding." *EWeek – Enterprise News and Reviews*. http://www.eweek.com/article2/0,4149,1536587,00&.asp (23 February 2004).

Takach, George. *Computer Law*, 2d ed. Toronto: Irwin Law, 2003.

Tan, John. (2001). Atstake Corporate White Paper. "Forensic Readiness." pp. 1–23. http://www.atstake.com (30 December 2003).

TechRepublic. (2002). "A glossary of security and cyberwarfare terms." *Tech Republic*. http://www.techrepublic.com (28 December 2003).

TechWeb News. (2004). “ISPs, Telecoms, Others Launch Global Anti-Spam Effort.” *Internet Week*. http://www.internetweek.com/shared/printableArticle.jhtml?articleID=17300952 (15 January 2004).

TechWeb News. (2004). “Security Firm Says Several More Microsoft Vulnerabilities Await Fixes.” http://www.internetweek.com/story/showArticle.jhtml?articleID=17603264 (12 February 2004).

The College of Physicians and Surgeons. (2004). “Fact Sheet – Self Regulation.” http://www.cpso.on.ca/Info_Public/factself.htm (4 February 2004).

The College of Physicians and Surgeons. (2004). “General College Information.” http://www.cpso.on.ca/About_the_College/geninfo.htm (4 February 2004).

The Economist (U.S.) Staff. “A lemon law for software?” *The Economist* (*U.S.*) (16 March 2002).

The Economist (U.S.) Staff. “Coping with the ups and downs.” *The Economist* (*U.S.*) Vol. 339, No. 7963 (27 April 1996): pp. 3–6.

The Economist (U.S.) Staff. (2003). “Fighting the worms of mass destruction.” *The Economist (U.S.)* (27 November 2003). http://www.sfu.ca/~anthonyc/cmpt301/pdf/security.pdf (9 February 2004).

The Economist (U.S.) Staff. (1997). “Hands off the Internet.” *The Economist* (*U.S.*) Vol.343, No. 8024 (5 July 1997): p. 7.

The Economist (U.S.) Staff. “Safe banking.” *The Economist* (*U.S.)* Vol. 339, No. 7963 (27 April 1996): pp. 27–30.

The Insurance Information Institute. (2003). “Most Companies Have Cyber-Risk Gaps in Their Insurance Coverage, States the I.I.I. – Traditional Insurance Policies Not Adequate For Cyber Exposures.” *Insurance Canada.ca.* http://www.insurance-canada.ca/consinfobusiness/IIICyber308.php?format=print (27 February 2004).

The Internet Society (ISOC). (2003). “News from the Internet Society Developing the Potential of the Internet through Coordination, not Governance.” *The Internet Society at the 'World Summit on the Information Society' (WSIS 2003)* http://www.isoc.org/news/7.shtml (12 February 2004).

The Oxford Encyclopaedic English Dictionary. Oxford (UK): Oxford University Press, Clarendon Press; 1991.

The President’s National Security Telecommunications Advisory Committee. (2003).*Internet Security / Architecture Task Force Report – Defining the Edge of the Internet* http://www.ncs.gov/Image-Files/ISATF_Issue_2_final.pdf (12 February 2004).

The SCO Group. (2004). The SCO Group. http://www.sco.com (04 March 2004).

The United States General Accounting Office. (2003). GAO Report Number GAO-03-119, "High-Risk Series-An Update." http://www.gao.gov/atext/d03119.txt (16 January 2004).

The United States General Accounting Office. (2003). GAO Report Number GAO-03-715T. *Homeland Security: Information Sharing, Responsibilities, Challenges, and Key Management Issues – Testimony Before the Committee on Government Reform, House of Representatives* http://www.gao.gov/new.items/d03715t.pdf (20 January 2004).

The United States General Accounting Office. (1996). GAO Report Number GAO/AIMD-96-84. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. http://www.fas.org/irp/gao/aim96084.htm (3 February 2004).

The U.S. Computer Emergency Readiness Team. (2003). "Best Practices and Standards: Corporate Governance." http://www.us-cert.gov/workwithus/index4.html (31 December 2003).

The White House. (1997). *A Framework for Global Electronic Commerce*. http://www.technology.gov/digeconomy/framewrk.htm (10 December 2003).

The White House. (2003). *The National Strategy to Secure Cyberspace*. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (30 December 2003).

Thibodeau, Patrick. "Government Seeks Vendor Accountability; Security directive means agencies will hold vendors responsible for troubled software. *Computerworld* (25 October 1999): p. 14.

Thibodeau, Patrick. "Homeland security bill limits vendor liability: private-sector software may also be affected by bill". *Computerworld* Vol. 36, No. 48 (25 November 2002): pp. 48–54.

Thompson, Clive. (2004). "The Virus Underground." *New York Times Online.* http://www.nytimes.com/2004/02/08/magazine/08WORMS.html?pagewanted=print&position (10 February 2004).

Thurston, Clive. "Bill 124 and the road ahead." *Daily Commercial News* Vol. 76, No. 171 (10 September 2003): p. 5.

Todd, Ewen. 1990. Epidemiology of foodborne illness: North America. The Lancet. Vol. 336, No. 8718: 788–790.

Torrie, Ralph D. (2003). "Electricity Productivity, "DSM" and Sustainable Futures for Ontario." *Presentation on behalf of CANET/CEG to the Ontario Energy Board* Advisory Group on DSM Toronto, October 2003 http://www.oeb.gov.on.ca/documents/directive_dsm_ClimateActionNetwork291003.pdf (16 February 2004).

Trope, Roland L. "In Pursuit of the Feasible: A Limited Warranty Of *Cyberworthiness*." *IEEE Security & Privacy*. [forthcoming in March 2003 issue].

Tutorials Agenda. (2003). http://www.cse-cst.gc.ca/en/symposium/tutorials/monday.html (30 December 2003).

U.S. Department of Homeland Security. (2003). "Ridge Creates New Division to Combat Cyber Threats." http://www.dhs.gov/dhspublic/display?content=915 (30 December 2003).

Vaas Lisa. (2004). "PeopleSoft, You Will Be Assimilated." *EWeek – Enterprise News and Reviews.* http://www.eweek.com/article2/0,4149,1517233,00.asp (5 February 2004).

Vamosi, Robert. (2004). "Security breach on Capitol Hill: Its criminal." http://reviews-zdnet.com.com/AnchorDesk/4520-7297_16-5118530.html?tag=adss (26 January 2004).

Vamosi, Robert. (2003). "We need a new national cybersecurity plan—now." http://reviews-zdnet.com.com/AnchorDesk/4630-7297_16-5111287.html?tag=print (10 December 2003).

Van Kirk, Doug. "What to do when your vendor pulls the plug; IS managers seek legal recourse against software publishers that fail to deliver." *InfoWorld* Vol. 16, No. 5 (31 January 1994): pp. 61–66.

Varian, Hal R. (2000)."Managing On-Line Security Risks." Economic Science Column. *The New York Times.* http://www.nytimes.com/library/financial/columns/060100econscene.html (03 March 2004).

Vaughn-Nichols, Steven J. (2004). "Intel Enters the SCO/Linux Wars on OSDL's Side." *EWeek – Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=116213,00.asp (13 January 2004).

Vaughn-Nichols, Steven J. (2004). "Novell Completes SUSE Acquisition, Details Indemnification Program." *EWeek – Enterprise News and Reviews*. http://www.eweek.com/article2/0,4149,1435577,00.asp (15 January 2004).

Vietor, Richard H.K. 1990. Contrived competition: airline regulation and deregulation, 1925–1988. Business History Review. Vol. 64, No. 1: 61–109.

Vijayan, Jaikumar. (2004). "DDoS attacks: prevention is better than cure." *Computer Weekly*. http://www.computerweekly.com/Article128198.htm (9 February 2004).

Vowler, Julia. “Clearing the legal mist.” *Computer Weekly* (10 June 1993): pp. 24–25.

Vowler, Julia. “Demanding a law for supply.” *Computer Weekly* (5 March 1992): pp. 34–35.

Wagner’s Weblog. (2004). “Security 2004: Fasten Your Seat Belts, Its Going to be a Bumpy Flight.” http://wagblog.internetweek.com/archives/000880.html (28 January 2004).

Warner, Bernhard. (2004). “SCO Debuts New Site as MyDoom Aims at Microsoft.” http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=4262986 (3 February 2004).

Washington Post Staff. (2004). “Congress and Cybersecurity – Government's Pressing Cybersecurity Issues” *The Washington Post* http://www.washingtonpost.com/wp-dyn/articles/A26684-2004Feb9.html (12 February 2004).

Watson, Albert. “Is Bill 124 really necessary?” *Building* Vol. 53, No.2 (April/May 2003): pp. 6–8.

Weiler, Robert K. (2002). “Decision Support: You Can't Outsource Liability For Security.” *Information Week*. http://www.informationweek.com/story/IWK20020822S0003 (24 February 2004).

Wende, David. “Financial Facts and Money Matters: Protecting the auditor from unlimited liability.” *Beyond Numbers* (1 October 2002): pp. 20–21.

Werbach, Kevin D. “Supercommons: Toward a Unified Theory of Wireless Communication,” *Texas Law Review*. [forthcoming in March 2004]. *Social Science Research Network Electronic Library*. http://papers.ssrn.com/sol3/delivery.cfm/delivery.cfm/SSRN_ID456020_code031013670.pdf?abstractid=456020 (3 March 2004).

West Wing Connections. (2003). “Homeland Security Actions.” http://www.whitehouse.gov/homeland/. (30 December 2003).

West Wing Connections. (2003). “National Security.” http://www.whitehouse.gov/response/index.html (30 December 2003).

Wikipedia.org. (2004). “Software Crisis.” *Wikipedia, the free encyclopedia* http://en.wikipedia.org/wiki/Software_crisis (03 March 2004).

Williams, Michael R. (1994). UTEC and Ferut: The University of Toronto’s Computation Centre. IEEE Annals of the History of Computing. Vol. 16, No. 2.

Williams, Patricia. “Bill 124 poses a thorny issue for contractors: proposal would add more to Project costs.” *Daily Commercial News* Vol. 76, No. 37 (21 February 2003): pp. 8–10.

Winn, Jane. (2002). “Legal Framework Needed for Vulnerability Disclosure Liability.” *Secure Business Quarterly*. Vol. 2 Issue 3. http://www.sbq.com (30 December 2003).

Wired News Staff. (2004). “Warning: Microsoft ‘Monoculture’.” http://www.wired.com/news/privacy/0,1848,62307,00.html (17 February 2004).

Wong, Craig. “Power outage across Ontario and northeastern U.S. shows interdependence.” *Canadian Press News Wire* (14 August 2003).

World Summit on the Information Society. (2003). “Draft Declaration of Principles.” http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-E.doc (8 January 2004).

Yager, Tom. “Open source takes hold – Tech executives are turning to open source to run mission-critical applications. Does this spell doom for Big Software?” *InfoWorld* Vol. 23, No. 35 (27 August 2001): pp. 49–51.

Yahalom, Raphael. (2002). “Liability Transfers in Network Exchanges.” In *Workshop on Economics and Information Security*, University of California, Berkeley May 2002. http://www.sims.berkeley.edu/resources/affiliates/ workshops/econsecurity/econws/46.ps (3 February 2004).

Young, R. Alan. (2002). “Bank Act Reform 2001 and the Banks.” *Canadian Banker Magazine.* (January 2002). http://www.cba.ca/en/magazine/getArticle.asp?at_id=201&pm=true (11 February 2004).

Yurcik, William. (2001). “National Missile Defense: The Trustworthy Software Argument.” http://www.cpsr.org/publications/newsletters/issues/2001/Spring/yurcik.html (3 February 2004).

ZDNet Reader, Tech Update. (2003).“Can software engineers be held accountable?” http://techupdate.zdnet.com/techupdate/stories/main/Can_software_engineers_be_held_accountable.html (12 December 2003).

Zhang, Xuemei. 1998. A software cost model with warranty cost, error removal times and risk costs. IIE Transactions. Vol. 30, No. 12: 1135–1142.

Ziff Davis Channel Zone. (2003). “Gates: Blazing the Longhorn Trail.” *EWeek – Enterprise News and Reviews*. http://www.eweek.com/print_article/0,3048,a=113069,00.asp (9 February 2004).