Cyber-Incident Risk in Canada and the Role of Insurance

APRIL 2004

ICLR Research
Paper Series - No. 38

ISBN: 0-9733795-4-5

Authors:

Paul Kovacs
Executive Director
Institute for Catastrophic Loss Reduction
Adjunct Research Professor, Economics
The University of Western Ontario
www.iclr.org

Melissa Markham
Co-ordinator, Urban Issues
Institute for Catastrophic Loss Reduction
www.iclr.org

Robert Sweeting
Manager, Research
Institute for Catastrophic Loss Reduction
www.iclr.org

The Institute for Catastrophic Loss Reduction, established in 1998, is a world-class centre for multi-disciplinary disaster prevention research and communications. ICLR is an independent, not-for-profit research institute founded by the insurance industry and affiliated with the University of Western Ontario. ICLR staff and research associates are recognized internationally for their expertise in wind and seismic engineering, atmospheric science, risk perception, hydrology, economics, geography, health sciences, and public policy, among other disciplines.

ICLR's mission is to reduce the loss of life and property caused by severe weather and earthquakes through the identification and support of sustained actions that improve society's capacity to adapt to, anticipate, mitigate, withstand, and recover from natural disasters. ICLR's mandate is to confront the alarming increase in disaster losses caused by natural disasters and to work to reduce disaster deaths, injuries, and property damage. ICLR is committed to the development and communication of disaster prevention knowledge.

ICLR is a leader in disaster loss prevention research and the development of loss prevention strategies with respect to the growing frequency and severity of extreme weather events. Multi-disciplinary research is central to ICLR's work in helping communities to become more resilient and better able to prevent natural hazards from becoming disasters.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1.0 Introduction

In 2003, the Institute for Catastrophic Loss Reduction began a study to research the insurance industry and its role in cyber-risk transfer and loss prevention. The work was carried out in two Phases:

- Phase I — *Case Study Review*. A literature review and data collection exercise was undertaken to examine cyber-incident risk in Canada and to describe the insurance environment of, and coverage for, these threats.

- Phase II — *Consultation with Industry Stakeholders*. A cross-section of insurance and reinsurance companies, and e-business solution providers were selected for consultation and a series of one-on-one interviews were concluded with senior officials from these firms.

This Final Report brings together the salient features of the Phase I and Phase II work in a single document. In broad terms, this Final Report:

- defines, details, and estimates cyber-incident risk costs and losses in Canada;

- discusses business vulnerability to cyber-incident risk and provides references to the global experience with the cyber-incident threat;

- examines the role of the insurance industry (including basic principles of insurance in providing standard policy coverage) in providing protection against cyber-incident risk; and

- discusses risk mitigation techniques to reduce the risk of cyber-incident events.

The paper describes the costs and vulnerabilities associated with cyber-incident risk and the ability of insurance to provide coverage for these risks.

2.0 What is Cyber-Incident Risk and How Much is it Costing Businesses?

This paper deals solely with risks associated with computer technology and the Internet, which includes hacking or unauthorized use of computer systems, denial of service issues, theft of proprietary information, and the distribution of viruses. It is not the intent of this paper to look at specific crimes conducted over the Internet (e.g., the misuse of telecom information or money laundering schemes).

In 2003, the CSI and the FBI conducted a *Computer Crime and Security Survey*. Survey respondents included computer security practitioners, government agencies, financial and

medical institutions, and universities throughout the United States. According to the survey, 92 percent of respondents reported attacks on their computer systems during 2002.

The annual cost of major virus attack losses has increased sharply since the mid-1990s. The financial impact of viruses worldwide was estimated to be almost $18 billion in 2003 (Computer Economics, 2004). Based on global losses of this magnitude, the Institute for Catastrophic Loss Reduction estimates that computer viruses cost Canada between $1 billion and $2 billion in 2003. Ernst & Young's 2003 *Global Information Security Survey* reports that hackers, worms, and other high-tech interference caused $11.1 billion in damages in 2002, more than a twenty-fold increase from 1995 (Ernst & Young, 2003).

3.0 Vulnerability to Cyber-Incident Risk

There are a number of significant cyber-incident risks that affect companies. A recent survey showed that three categories of cyber-incident risk — virus, denial of service, and theft of proprietary information — accounted for 81 percent of cyber-incident losses in the United States in 2002 (Computer Security Institute, 2003). When survey participants were asked whether they had insurance coverage for these types of losses, 33 percent said they believed that cyber-incident risks were covered by their general policies, while 34 percent said they did not have insurance (Computer Security Institute, 2003).

4.0 The Role of Insurance

Insurance companies provide coverage for many types of risk. Many corporations use insurance as a means to transfer risk. Insurance transfers individual risk to a pooled group, where the risk is absorbed by a larger market.

A. Standard Insurance Coverage

The standard market product for protecting businesses against the risk of accidents is Commercial General Liability (CGL) insurance. When this type of coverage was created, the Internet did not exist and other cyber-incident risks were not widespread (the concept of cyber-incident risk was relatively unknown and the majority of businesses dealt with tangible assets); consequently, their associated risk exposures were not addressed in policies. Current CGL policies make it clear, with specific exclusions, that they do not cover intangible property such as electronic data and business interruption.

B. Cyber Insurance

Considering the barriers to coverage of cyber-incident risks by standard insurance policies, the market has been left to individual insurance companies to develop specialized cyber insurance products. Although some overlap does occur between cyber and standard insurance, damages incurred by denial of service, hacker attacks and cyber-incident risks are not typically covered in standard forms of insurance. The courts

consistently uphold that data are not property and do not meet the "direct physical loss" requirement set out in standard insurance policies (IBC, 2003).

Because companies frequently do not report cyber-incident attacks, there are difficulties associated with historical data. Companies often do not report incidents when they occur because they believe consumer confidence will decrease with each cyber-incident occurrence. Consequently, the confidential nature of cyber incidents — driven by corporate fears of losing existing and potential customers if these incidents were made public — makes it difficult for insurance companies to collect data to project future losses. In the case of cyber-incident coverage, there are no historical records so insurers are setting prices without being able to completely quantify risks.

C. Cyber Insurance Pricing

While insurance companies have tried to quantify cyber-incident risk, it remains to be seen whether current premiums will prove to be adequate. Premiums can range from a few thousand dollars for base coverage for small businesses (less than $14 million in annual revenue) to several hundred thousand dollars for major corporations seeking comprehensive coverage. Cyber-related premiums range from $7,000 to $85,000 per $1.5 million worth of coverage, depending on the size and exposure of each company to online or electronic risk (McAfee Security, 2003).

In 2003, three industry groups accounted for two-thirds of all cyber insurance policies purchased in the United States: the technology and telecommunications industry accounted for 38 percent, the financial services industry accounted for 18 percent, and the retail and wholesale industry accounted for 11 percent (Marsh Inc., 2003).

Brokers estimated that, in 2002, businesses purchased only $150 million to $300 million of this type of insurance, despite estimates of potential cyber-related losses in the billions of dollars (Kelly, 2003). As companies become more informed about cyber insurance, the market has the potential to become one of the biggest growth areas for insurers over the next few years — one that could develop into a $3.6 billion U.S. market by 2005 (Insurance Information Institute, 2003).

D. Types of Cyber Insurance Coverage

The growth of computer and Internet technology has led to an increased demand for insurance products that provide for various cyber-incident risks. Cyber-incident coverage is available currently as a specific stand-alone policy, which is tailored to meet the needs of each individual company. There are several insurance companies that underwrite the risk of cyber activity, although each policy differs regarding the level of risk exposure. During the course of this paper's consultations, American International Group (AIG), Chubb, Marsh, St. Paul Insurance Company, and Zurich North America were identified as insurance companies having some type of coverage available for cyber-incident risks.

During the stakeholder interviews, the cyber insurance coverages discussed most frequently were loss/corruption of data, business interruption, liability, cyber extortion, and rewards.

E. Current Issues with Cyber Insurance

When asked why businesses are not investing in cyber-incident insurance, the majority of our insurance, reinsurance, and e-business solution industry stakeholder interviewees stated that most of their clients are too small to afford the cost of insuring for this risk. The majority of e-business solution interviewees stated that their main clientele was comprised exclusively of Fortune 500 and large multi-national organizations. Companies have begun to look inward to self-insure their organizations because of rising premiums associated with cyber insurance.

F. Use of Risk Management

E-business solution interviewees noted that their companies provide services to firms at risk for business continuity — providing support such as data recovery, and mitigating software and hardware products that secure the system prior to an attack. E-business solution interviewees observed that all of the businesses that employ their services have an existing structure in place (such as a risk manager) to identify the need for these services.

The use of risk managers is low in small- to mid-size companies, while larger multi-national companies are better able to support a risk management staff. While large corporations, such as Fortune 500 companies, are able to identify and manage their cyber-incident risks through the use of mitigation and loss prevention methods, small- to mid-sized companies have fewer remedies available. These companies typically manage their risks through the purchase of software and hardware products to secure their systems against malicious attacks, viruses, and theft of proprietary data.

5.0 Loss Prevention and Mitigation

Growing dependence on information networks and changes in technology make it critical for businesses to adopt effective techniques to mitigate information security risks and to prevent losses. Information that flows freely over networks can be intercepted by outside sources, which make businesses vulnerable to copyright and other violations.

The insurance industry believes that mitigation techniques (for example, risk avoidance, deterrence, prevention, detection, recovery, and transfer) are essential toward improving the insurability of businesses and government agencies against cyber-incident risk (Gordon, et. al., 2003). By writing policies to insure against cyber-incidents, insurers provide risk transfer for cyber exposure, including incentives to employ best practices and improved mitigation strategies for managing these risks.

Gordon, Loeb and Sohail describe a cyber-incident risk management framework for information security that reduces and maintains risk at an appropriate level:

1. **Assess risks**. This requires companies to determine their own risk exposure and true costs. They must determine what their current level of insurance covers, including existing computer systems and the level of maintenance required.

2. **Reduce risks**. There are several techniques that can be employed to reduce risk, such as employee education, upgrades to anti-virus software and operating systems, increased security protocol, improvements in monitoring systems to detect intrusions, and the use of firewalls, encryption, and access control.

3. **Maintain an acceptable level of risk**. This can be achieved by determining the type of insurance policy required for each particular company, including the methods employed to reduce potential losses and increase security measures.

6.0 Conclusion

This paper has described the costs and vulnerabilities associated with, and the ability of insurance to provide coverage for, cyber-incident risk, including hacking or unauthorized use of computer systems, denial of service, theft of proprietary information, and virus distribution. The research has indicated clearly that:

- **Cyber-incidents are pervasive, costly, and escalating**. Cyber-incidents have become quite extensive in the business community, with roughly 90 percent of U.S. companies currently reporting unauthorized system access, and cyber-incident losses shared roughly one-third each between denial of service, theft of private information, and virus distribution and other attacks. Considering virus attacks alone, some measures of the annual global financial impact of such strikes indicate a twenty-fold to forty-fold increase over the period from 1995 to 2003.

- **The insurance industry has a meaningful role to play in cyber-risk transfer and loss prevention**. While standard insurance policies do not cover cyber-incident risk exposure, the insurance industry has designed a cyber-incident insurance product that responds to consumer needs. Recent (2002) estimates place business purchases of cyber-incident insurance coverage at $150 million to $300 million with the technology and telecommunications industry being the largest purchaser of cyber insurance policies in the U.S. By writing cyber insurance policies, insurers provide risk transfer for cyber exposure, including incentives to employ best practices and improved mitigation strategies for managing these risks.

- **Risk reduction and mitigation strategies play a critical function in securing systems**. Cyber-related premiums range from $7,000 to $85,000 per $1.5 million worth of coverage, depending on the size and exposure of each company to online or electronic risk. Consequently, many companies look inward and self-insure their organizations. In this regard, risk reduction and mitigation strategies (including the

purchase of software and hardware products, such as upgrades to anti-virus software and operating systems, increased security protocol, improvements in monitoring systems to detect intrusions, and the use of firewalls, encryption, and access control) play a critical function in securing systems.

- **Cyber-incident statistics need to improve**. The insurance industry is currently confronted by a dearth of cyber-incident data and insurers have been obligated to price cyber-incident coverage without being able to completely quantify risks. Because of the under-reporting of cyber-incident attacks (businesses are reluctant to report incidents for fear of economic losses), historical data on which to base cyber insurance premiums are limited.

After only a few years of experience with cyber-incident insurance coverage, it is clear that a sizeable market for the product has yet to emerge. Initial pricing for the coverage is material, and reinsurers continue to exclude it from their policies. Large amounts of new capital are not currently available to property-casualty insurers to fund cyber-incident risks. While the inability of insurers to fully fund such high-severity events may cause businesses to question the value of cyber-incident risk coverage, given time, awareness, and the prospect of additional cyber-incident attacks, more businesses are expected to seek insurance coverage.

1.0 Introduction

In 2003, the Institute for Catastrophic Loss Reduction began a study to research the insurance industry and its role in cyber-risk transfer and loss prevention. The work was carried out in two Phases:

- Phase I — *Case Study Review*. A literature review and data collection exercise was undertaken to examine cyber-incident risk in Canada and to describe the insurance environment of, and coverage for, these threats.

- Phase II — *Consultation with Industry Stakeholders*. A cross-section of insurance and reinsurance companies, and e-business solution providers were selected for consultation and a series of one-on-one interviews were concluded with senior officials from these firms.

This Final Report brings together the salient features of the Phase I and Phase II work in a single document. In broad terms, this Final Report:

- defines, details, and estimates cyber-incident risk costs and losses in Canada;

- discusses business vulnerability to cyber-incident risk and provides references to the global experience with the cyber-incident threat;

- examines the role of the insurance industry (including basic principles of insurance in providing standard policy coverage) in providing protection against cyber-incident risk; and

- discusses risk mitigation techniques to reduce the risk of cyber-incident events.

This Final Report is organized as follows:

- Chapter I — *Introduction* — provides the background to this paper.

- Chapter II — *What is Cyber-Incident Risk and How Much is it Costing Businesses?* — provides a definition of cyber-incident risk and some measures of cyber-incident losses.

- Chapter III — *Vulnerability to Cyber-Incident Risk* — explores business vulnerability to cyber-incident risk as sources of revenue shift from tangible to intangible assets.

- Chapter IV — *The Role of Insurance* — describes the role of insurance companies in providing standard insurance coverage and the impact this has on cyber insurance, including the case of Y2K, and the legal decisions that flowed from a U.S. court case

that examined whether specific cyber-incident coverage was provided by standard insurance policies.

- Chapter V — *Loss Prevention and Mitigation* — details a loss prevention and mitigation approach for dealing with cyber-incident risk.

- Chapter VI — *Conclusion* — summarizes the current thinking surrounding cyber-incident risk and the role of insurance.

- Chapter VII — *References/Bibliography* — provides details of the information sources used in this paper.

- Appendix A — *Interviewees* — provides a list of the insurance, reinsurance, and e-business solution providers interviewed.

- Appendix B — *Insurer Interview Questions* — provides the interview questions that were asked of the insurance and reinsurance industry stakeholders.

- Appendix C — *E-Business Solution Provider Interview Questions* — provides the interview questions that were asked of the e-business solution providers.

The paper describes the costs and vulnerabilities associated with cyber-incident risk and the ability of insurance to provide coverage for these risks. This paper does not set out to provide a comprehensive list of companies that provide cyber insurance products, nor does it seek to provide a detailed explanation of what their current coverage includes.

2.0 What is Cyber-Incident Risk and How Much is it Costing Businesses?

An investigation of the cyber-incident literature reveals that the subject is relatively new and that few definitions exist. Statistics Canada defines the term cyber-incident as "a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence" (Kowalski, 2002). Both the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) view cyber issues as including fraud, theft of proprietary information, distribution of viruses, wiretapping, unauthorized insider access and abuse, denial of service, telecom eavesdropping, sabotage, and system penetration.

To manage the scope of this paper, to bring clarity to the discussion, and to provide a framework for cyber-incident, this paper deals solely with risks associated with computer technology and the Internet, which includes hacking or unauthorized use of computer systems, denial of service issues, theft of proprietary information, and the distribution of viruses. It is not the intent of this paper to look at specific crimes conducted over the Internet (e.g., the misuse of telecom information or money laundering schemes).

Although the field of cyber-incident research is broad, there are few data available pertaining to the use of insurance as part of corporate cyber-incident risk management practices. There are, for example, no reliable data available regarding the actual costs of these losses (as recognized by individual companies) or of the number of cyber-incidents that actually occur. Most of the available information relates to the issue of computer viruses, as does the literature – reflecting the large number of businesses that are affected adversely by these attacks. Still, some data do exist to illuminate elements of the cyber-incident issue. These data are discussed below.

In 2003, the CSI and the FBI conducted a *Computer Crime and Security Survey*. Survey respondents included computer security practitioners, government agencies, financial and medical institutions, and universities throughout the United States. According to the survey, 92 percent of respondents reported attacks on their computer systems during 2002. By comparison, the same survey reported that 70 percent of companies suffered computer attacks in 2000, and 42 percent reported attacks in 1996 (Computer Security Institute, 2003). These data show how rapidly cyber-incident risk is growing.

The annual cost of major virus attack losses has increased sharply since the mid-1990s (see Table 2.1). As shown in Table 2.1, the financial impact of viruses worldwide was almost $18 billion in 2003. Based on global losses of this magnitude, the Institute for Catastrophic Loss Reduction estimates that computer viruses cost Canada between $1 billion and $2 billion in 2003.

Table 2.1 Annual Global Financial Impact of Major Virus Attacks ($CDN)

Year	Worldwide Economic Impact
2003	$17.5 billion
2001	$20.4 billion
1999	$18.0 billion
1997	$4.6 billion
1995	$0.7 billion

Source: ICLR, based on data from Computer Economics, 2004.

Notes: Figures include (1) the labour cost associated with analyzing, repairing, and cleansing of operating systems, applications, databases, networks, and machines; (2) the procurement cost of tools (hardware and software) required to assist technicians in performing the tasks listed above; (3) the expenses associated with hiring consultants or contract personnel to assist in any of the tasks listed above; and (4) the potential and direct loss of revenues due to a denial of service or a significant slowdown of services that are offered via the Internet or other "network" or "computer" channels that may have been impacted.

In the context of cyber incidents, greater reliance on computer systems is having negative impacts on business organizations. Companies are creating systems that are becoming more difficult to penetrate, but the next generation of computer hackers and terrorists will be products of the digital world with even more tools of destruction at their disposal (Denning, 2000). In 2002, 90 percent of U.S. businesses reported unauthorized system access (Insurance Information Institute, 2003). In a recent U.S. survey, 80 percent of respondents acknowledged economic losses as a result of cyber incidents (Computer Security Institute, 2003). These figures continue to rise, although the majority of respondents cannot identify precisely the financial costs of cyber incidents. According to the International Data Corporation (IDC), a global market advisory firm in the information technology and telecommunications industries, system security has become a priority among chief executives. As a result, spending on security-related software is the fastest growing area of information technology (IDC, 2003).

The increasing costs associated with cyber incidents are restrictive to companies that rely on computer and network systems to conduct business. Cyber-incident risks and related costs are usually too large for an individual company to manage without help. While many companies use firewalls, encryption, and anti-virus software, they are still at risk. The enormity of potential revenue loss by industry, coupled with the increase in major virus attacks, makes it difficult to determine how to protect businesses against these risks.

Ernst & Young's 2003 *Global Information Security Survey* describes cyber-incident risk costs as harmful to companies that rely on the Internet and network systems to conduct their business. The Ernst & Young survey also comments on research conducted by Computer Economics Inc. that estimates that hackers, worms, and other high-tech interference caused $11.1 billion in damages in 2002, more than a twenty-fold increase from 1995 (Ernst & Young, 2003). The survey also noted a change in the factors that

inhibited information security. In 2002, the speed of change and increasing sophistication of threats were the leading factors inhibiting effective information security. In 2003, a shortage of available funds rose to the top of the list. The survey also noted that slightly more than half (52 percent) of the participants had experienced an unscheduled or unexpected outage of a critical business system, and 22 percent of these outages were attributed to major viruses or worms (Ernst & Young, 2003).

3.0 Vulnerability to Cyber-Incident Risk

Many organizations depend on computers and network systems to conduct their daily business. These systems have allowed companies to become more efficient and to reach a wider client market for their products and services. While there are enormous benefits to conducting business over network systems, there are also associated costs that are incurred due to increased corporate vulnerability to cyber-incident risks.

As a business tool, the use of a network for complex data transactions and proprietary computer data storage methods can have a dramatic effect on the management of a company. Nowadays, a company's decision to undertake these activities is no longer just an IT issue: risk management techniques are required to protect the security of information. For example, cyber incidents impinge on the privacy of personal information, which is now protected in Canada by the Information Protection and Electronic Document Act (this legislation is discussed later in this paper), and this presents a new challenge for Canadian businesses. As revenue generation shifts from tangible to intangible assets, companies are faced with an expanding number of intangible exposures, and "as much as 80% of the market value of public companies come from intangible assets" (Wleugel, Dowdall and Grange, 2003). While network, Internet, and e-commerce activities are a source of cyber-incident risk for business, at this point in time, there are no reliable prevailing practices to quantify these risks and few historical data exist to place them in perspective.

Specific cyber-incident risks include viruses, Trojan horses, unauthorized access, proprietary data theft, business interruption, and denial of service attacks. These events can affect many aspects of a company, including reputation and physical, informational, and systemic assets. The testimony of Richard Pethia of the CERT Coordination Center (CERT/CC) before the House Select Committee on Homeland Security in June 2003 relays how vulnerable network systems are to cyber-incidents. His testimony also provides a convenient means to measure the increase in cyber-incident vulnerability. In his testimony, Mr. Pethia stated that CERT/CC receives reports of new sources of vulnerabilities. These vulnerabilities represent a weakness in a product that can be exploited in some way to help an attacker compromise a system (Pethia, 2003). In 1995, CERT/CC received 140 reports of new sources of vulnerabilities and by 2002, the number of annual reports received grew to more than 4,000. CERT/CC believes that technology is evolving so rapidly that software vendors are concentrating on the mass distribution of their products to market, and minimizing the time devoted to creating security features (Pethia, 2003). A better understanding of these issues should convince companies of the need for protection from cyber-incident attacks.

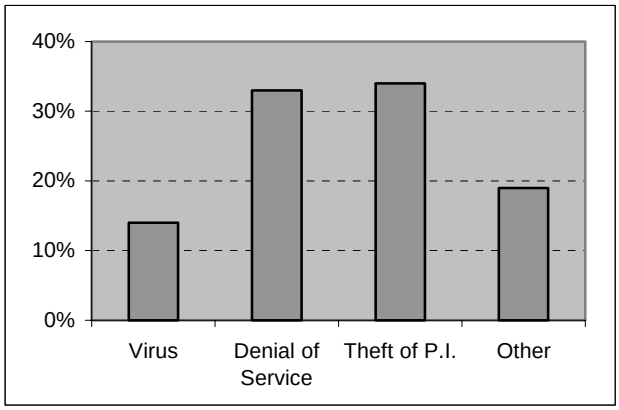
The world is relying increasingly on technology to provide high-quality customer service, and, as a consequence, it has become more exposed to the threat of cyber-incidents. Canada's critical infrastructure, for example, is heavily reliant on computers, and is a prime target for hackers and other cyber criminals. Infrastructure such as power grids, transit systems, and air-traffic control are a few of the areas that are vulnerable to cyber-incident risk. One example that highlights the complexity and interdependency of

Canada's infrastructure is described by PSEPC: in 1999, an employee dropped a wrench at a telecommunications switching station in Toronto, and this one incident disrupted electronic banking systems from British Columbia to Nova Scotia, resulting in the interruption of trading on the Toronto Stock Exchange. This single cyber-incident resulted in a financial loss of over $1 billion to Canadian businesses and the federal government (Purdy, 2001).

A. Types of Cyber-Incident Risk

There are a number of significant cyber-incident risks that affect companies. As shown in Chart 3.1, a recent survey showed that three categories of cyber-incident risk — virus, denial of service, and theft of proprietary information — accounted for 81 percent of cyber-incident losses in the United States in 2002 (Computer Security Institute, 2003). When survey participants were asked whether they had insurance coverage for these types of losses, 33 percent said they believed that cyber-incident risks were covered by their general policies, while 34 percent said they did not have insurance (Computer Security Institute, 2003).

Chart 3.1 Losses by Type of Cyber-Incident Risk, United States, 2002



Source: CSI/FBI 2003 Computer Crime & Security Survey, 2003.

Along with greater reliance on technology has come greater vulnerability to network disruptions, security breaches, computer viruses, information theft, and a host of other liabilities and direct losses. In most cases, the exposures caused by these events fall outside the realm of traditional insurance policies, creating serious coverage gaps for companies looking to safeguard their systems and intangible assets, such as databases housed on these systems. Since no system is completely impenetrable and few companies have purchased coverage for cyber-incident risks, it is important to consider what role the insurance industry should play in helping minimize cyber-incident impacts. This issue is discussed in the next section of this paper.

4.0 The Role of Insurance

As companies become more vulnerable to cyber-incident risks, they are looking increasingly to the insurance industry to offer coverage for these events. In this context, it is important that the role of insurance be understood. The Insurance Bureau of Canada (IBC) defines insurance as follows:

> **General insurance (property and casualty, or "P&C" insurance) is a promise to pay (reimburse) should certain things go wrong. Insurance replaces uncertainty with a degree of certainty, providing financial peace of mind in a world filled with risk. The basic principle of general (non-life) insurance is that the fees or "premiums" (and often the investment income derived from those premiums) of all participants or "policyholders" pay for the losses of an unfortunate few. It's a way of sharing financial risk.** (IBC, 2003)

Many corporations use insurance as a means to transfer risk. Insurance transfers individual risk to a pooled group, where the risk is absorbed by a larger market. Before examining the role the insurance industry has to play in providing cyber insurance policies and cyber-incident coverage, standard insurance policy coverage must first be understood. This is discussed below.

A. Standard Insurance Coverage

Insurance companies provide coverage for many types of risk. The standard market product for protecting businesses against the risk of accidents is Commercial General Liability (CGL) insurance. When this type of coverage was created, the Internet did not exist and other cyber-incident risks were not widespread (the concept of cyber-incident risk was relatively unknown and the majority of businesses dealt with tangible assets); consequently, their associated risk exposures were not addressed in policies. While businesses are currently looking to the insurance industry to provide services to diminish their direct cyber-incident risks, it must be recognized that this protection does not exist within their existing CGL insurance policies.

Standard insurance coverage was designed to protect tangible assets. Standard forms of insurance primarily cover bodily injury and tangible property loss, and they do not cover the legal liabilities arising from the transmission of a computer virus or computer theft of customer information (Assurex International, 2000). While uncertainty has existed in the past concerning what cyber-incident risks are covered under traditional business insurance policies, current CGL policies make it clear, with specific exclusions, that they do not cover intangible property such as electronic data and business interruption.

For a risk to qualify as insurable, it must meet three key underwriting requirements (IBC, 1999):

1. **A relatively large population is exposed to a risk**. This condition must be met because it ensures that the insurance companies have a large enough group for risk transference.

2. **A small share of the exposed population is likely to incur a loss at any particular time**. In order for insurance companies to deal with an event, it is essential that the risks they underwrite will not impact all of their companies at once, or they would not have the capacity to cover all of their losses.

3. **There is a random occurrence of losses**.

These three insurability requirements are significant. Most of the insurance companies' senior officials who were interviewed for this paper made reference to cyber-incident exclusions based on these criteria.

The significance of these three insurability requirements can be illustrated with a number of cases. Below, Case 1 — *Y2K and the Role of Insurance* — considers the Y2K issue, which brought much attention to insurance coverage in the late 1990s and was the first major cyber-incident risk to command the attention of the public and the insurance industry. Y2K was not considered to be an insurable peril. It highlighted the limited coverage insurers provide for the risks of computer failure.

Case 1. Y2K and the Role of Insurance

The Y2K computer problem received worldwide attention in the late 1990s. The Y2K problem flowed from the fact that computers were not initially programmed to deal with the rollover in time from 1999 to 2000. To ensure that computers would continue to function in the year 2000, companies needed to update their programming to accommodate this change. It was widely believed that the computer technologies on which the world relied for critical services could fail at midnight on New Year's Eve 1999/2000.

The insurance industry was very active describing their role in relation to Y2K losses. Three key underwriting requirements were put forward to qualify for coverage (IBC, 1999):

- a relatively large population is exposed to a risk;
- a relatively small share of the exposed population is likely to incur a loss at any particular time; and
- a random occurrence of losses.

In the case of Y2K, these requirements were not met and, as a result, standard insurance policies did not address this risk. In the case of Y2K, equipment failures were not insured losses, although some indirect losses would have been covered. Throughout the build-up to Y2K, insurance companies stressed the importance of managing risk by anticipating and mitigating possible failures. Because Y2K was both foreseen and predicted, businesses had time to take the necessary precautions to prevent adverse impacts.

In the circumstance of Y2K, it was demonstrated that cyber-incident risks related to the event did not qualify for standard insurance coverage because they did not meet all three key underwriting principles. As a cyber-incident risk, Y2K exposed a relatively large population, but a large (rather than small) share of that population was liable to incur a loss at any time, and the losses anticipated generally would not be random occurrences.

During our consultations with industry stakeholders, many insurance and reinsurance executives viewed cyber-incident risks as catastrophic events that are not insurable under standard insurance policies. One of the reinsurance company interviewees made reference to the three key underwriting principles and described the problems that arise when insuring for a catastrophic risk. This interviewee stated that "a catastrophic risk occurs when there is a high probability that many businesses will experience a loss or be damaged at the same time."

Cyber-incident risks are not covered under standard insurance policies. Nevertheless, there are a few insurance companies willing to underwrite risks related to cyber-incidents. Interviewees often contrasted cyber-incident risk with automobile insurance. One insurer interviewee stated that their company has a large enough market to spread the risk of automobile insurance because few accidents happen in relation to the large number of people who are insured and each event is a random occurrence. This insurer explained that they do not provide cyber insurance coverage because this risk does not meet with the same insurability requirements as does automobile insurance coverage. Interviewees also noted that, while actuarial data exist to estimate (with a high degree of reliability) potential losses for automobiles, there are so many unknowns associated with cyber-incidents that the examination of several years of historical data would be required before an estimation of potential losses could be undertaken with any degree of accuracy.

Several claims have been filed in recent years related to cyber-incident losses in the United States. These cases have gone to the courts to determine whether standard insurance policies cover losses from cyber-incident risks. At issue is the assertion of insurers and reinsurers that a loss caused by network or computer problems is not covered under a type of physical loss of damage to businesses. Case 2 — *AOL v. St. Paul Insurance* — supports this opinion (see below).

Case 2. AOL v. St. Paul

One way to establish whether specific cyber-incident coverage is provided by standard insurance policies is to consider how the courts are dealing with the issue. A recent case that addressed this issue in the United States was AOL v. St. Paul. In this case, a trial court ruled that damage to computer data did not constitute "property damage" under a Commercial General Liability (CGL) insurance policy, concluding that data were not "tangible property." The same court also ruled that loss of use of a computer (indisputably, "tangible property") on which data reside, and under the particular facts of AOL v. St. Paul, was not covered because of the "impaired property" exclusion. Rossi concluded that, faced with this type of uncertainty in standard insurance coverage, companies will purchase stand-alone polices for greater peace of mind.

As early as 2000, reinsurers were limiting coverage from losses arising from cyber and network risks. In 2001, revisions to the CGL policy form clarified the definition of "property damage," stating that "electronic data is not tangible property." This revision illustrates a key coverage limit that currently exists in standard insurance policies.

Source: Rossi, 2002.

Without reinsurance coverage for these types of losses, insurers have increased the use of exclusionary wording in insurance policies dealing with cyber-incident coverage. For example, the Insurance Bureau of Canada has produced an "Advisory Model Wording" to describe current coverage related to the Commercial Building, Equipment and Stock Broad Form. Section 6 (D) of that document states that:

> **This form does not insure against loss or damage caused directly or indirectly by the failure of any:**
>
> **a. electronic data processing equipment, or other equipment, including micro-chips embedded therein;**
> **b. computer program;**
> **c. software;**
> **d. media;**
> **e. data;**
> **f. memory storage system;**
> **g. memory storage device;**
> **h. real time clock;**
> **i. date calculator; or**
> **j. any other related component, system, process or device,**
>
> **to correctly read, recognize, interpret or process any encoded, abbreviated or encrypted date, time or combined date/time data or data field. Such failure shall include any error in original or modified data entry or programming.**

With this exclusion in standard insurance coverage, businesses need to purchase specific policies that provide coverage for cyber-incident risks. That is, while cyber-incident risks do not qualify for traditional insurance coverage, there are other ways for these events to be insured. Typically, when a new loss exposure arises, a number of brokers and insurers will respond to the challenge by creating products to fund these potential new losses. Considering the barriers to coverage of cyber-incident risks by standard insurance policies, the market has been left to individual insurance companies to develop specialized cyber insurance products. This is discussed in the sections below.

B. Cyber Insurance

A useful definition for cyber insurance was provided by Ty Sagalow (from American International Group (AIG) e-Business Risk Solutions). He defines cyber insurance as a specialized policy that provides both insurance and risk management services against various types of cyber-incident risk (Sagalow, 2001).

Insurance that covers cyber-incident risk has been in existence since the late 1990s. The major factor that led to greater business interest in cyber insurance was the realization – after issues such as Y2K – that these risks were largely not covered under basic insurance policies, at a time when corporate vulnerability to cyber incidents was growing.

Although some overlap does occur between cyber and standard insurance, damages incurred by denial of service, hacker attacks and cyber-incident risks are not typically covered in standard forms of insurance. The courts consistently uphold that data are not property and do not meet the "direct physical loss" requirement set out in standard insurance policies (IBC, 2003). An interview respondent expressed this sentiment as follows: "data is intangible and the perils to data are viruses and hackers, not fire and flood, which are the standard hazards that insurance companies insure against". The primary concern in insuring against cyber-incident risks is to identify and protect intangible property.

Underwriting cyber-incident risks is complex. Cyber insurance is an evolving field and current policies that exist to protect against cyber-incident risks will require continuing modifications to respond to the changing environment. Coverage for cyber-incident risks must take into account myriad factors such as the technology being used by an individual company and the risk that is involved. With a lack of historical data and a rapidly changing technological environment, businesses are providing services that were not even contemplated a few years ago. By writing policies for cyber-incident exposures, the insurance industry is providing (III, 2003):

1. Virtual risk transfer for network security exposures.
2. Incentives for network security best practices, including lower insurance premiums.
3. Improved cyber-risk management and education.

To design policies to protect against cyber-incident risk, insurance companies must consider three key issues — pricing, adverse selection, and moral hazard (Gordon, et. al., 2003). These three issues are discussed below.

Pricing

Traditionally, the pricing of insurance coverage is related directly to the calculation of risk. Insurance companies rely on actuarial tables (constructed from historical records) to determine proper pricing for cyber-incident coverage. If this approach were applied to cyber-incident risk, insurers would need to know how often cyber-incident events have occurred in the past and the likelihood of future occurrences. In the case of cyber-incident coverage, there are no historical records so insurers are setting prices without being able to completely quantify risks.

Because companies frequently do not report cyber-incident attacks, there are difficulties associated with historical data. Companies often do not report incidents when they occur because they believe consumer confidence will decrease with each cyber-incident occurrence. Consequently, the confidential nature of cyber incidents — driven by corporate fears of losing existing and potential customers if these incidents were made public — makes it difficult for insurance companies to collect data to project future losses. As a result of under-reporting, historical data on which to base cyber insurance

premiums are limited (Insurance Information Institute, 2003). From a Canadian perspective, Statistics Canada also reports that cyber-incident crime may be one of the most under-reported forms of criminal behaviour because businesses are reluctant to report incidents for fear of economic losses (Kowalski, 2002). Cyber-incident statistics need to improve.

Case 3 — *Mafiaboy* — illustrates how financial losses can occur when cyber-incidents are reported (see below).

Case 3. Mafiaboy

An incident in 2000 demonstrated the extreme risks that cyber crimes pose to companies worldwide. This cyber-incident case was caused by an inexperienced 15-year old Montreal computer hacker who was responsible for 58 attacks and security breaches of Internet sites in Canada, the United States, Denmark, and Korea in February 2000. Known as "Mafiaboy", he launched a denial-of-service attack that overloaded targeted websites with so much data that users were unable to gain access to these web addresses for several hours.

Many companies were affected by Mafiaboy, including Yahoo!, eBay, Amazon, CNN, and the Microsoft network. The volume of Internet-related customers that these companies serve requires them to be Internet-accessible at all times to conduct their business. The denial-of-service attack either disrupted Internet service or completely shut down each website for a time period of an hour to more than three hours.

Companies accept a certain level of risk by relying primarily on the Internet for revenue. While many companies experience denial-of-service attacks, such strikes are often not reported to the police. They are referred to as "glitches" so as not to deter customers from using their services in the future because of concern over security issues. Mafiaboy's attacks on the Internet sites of Yahoo! and eBay resulted in a decrease in their stock values of between 17 and 23 percent in the weeks following the attacks. Market reactions such as this demonstrate why companies are reluctant to disclose cyber-incidents.

While insurance companies have tried to quantify cyber-incident risk, it remains to be seen whether current premiums will prove to be adequate. Premiums can range from a few thousand dollars for base coverage for small businesses (less than $14 million in annual revenue) to several hundred thousand dollars for major corporations seeking comprehensive coverage. McAfee Security states that cyber-related premiums range from $7,000 to $85,000 per $1.5 million worth of coverage, depending on the size and exposure of each company to online or electronic risk (McAfee Security, 2003). Brokers estimated that, in 2002, businesses purchased only $150 million to $300 million of this type of insurance, despite estimates of potential cyber-related losses in the billions of dollars (Kelly, 2003).

Adverse Selection

Insurance companies seek to all organizations fairly in terms of coverage and premiums, although some organizations may have information that they are at significant risk and may not share this knowledge with insurance companies when applying for coverage. Due to adverse selection, the companies and organizations most likely to purchase cyber insurance are often those with a high risk of cyber-incident attacks. To protect themselves from adverse selection, insurance companies require cyber-incident and information security inspections prior to coverage and companies must typically adopt certain loss prevention mechanisms in order to qualify for this insurance.

Moral Hazard

Owing to moral hazard, the companies that are insured for cyber-incident losses may be less likely to implement loss prevention measures. One way to address the issue is through the use of deductibles — this provides an incentive for companies to maintain a certain level of security. Another way to address the issue is to offer reductions in policy premiums for companies that successfully implement loss-prevention measures. The cyber-incident research also suggests that insurance companies have been using surcharges. For example, due to the poor security track record of Windows NT, insurance companies have placed surcharges on its users, making it expensive to insure (Brush, 2001).

C. Types of Cyber Insurance Coverage

The growth of computer and Internet technology has led to an increased demand for insurance products that provide for various cyber-incident risks. There are two broad cyber insurance policy coverages (Insurance Information Institute, 2003):

- **First-party coverage**. This includes losses that are suffered by the insured company as a result of loss or damage to assets, such as the destruction of data, business interruption, or damage from a computer virus.

- **Third-party coverage**. This is used to protect a company from lawsuits brought by its customers or trading partners. Third-party coverage includes the loss or theft of third-party personal information and, generally, the most expensive claims are for third-party liability. The majority of companies that have purchased cyber insurance have third-party coverage.

AIG provides a specific example that illustrates why companies choose third-party liability coverage. The particular case involved computer extortion threats against a web-based company. The incident occurred when a hacker stole approximately 300,000 customer credit card numbers from an online retailer. The hacker then attempted to use the stolen information to extort $100,000 from the company. Upon the company's refusal to cooperate, the hacker posted 23,000 card numbers online. As a result of denied charges, credit card cancellations, and re-issuance, the online retailer suffered

approximately $3.14 million in lost income and third-party damages (American International Group, 2002).

Cyber-incident coverage is available currently as a specific stand-alone policy, which is tailored to meet the needs of each individual company. There are several insurance companies that underwrite the risk of cyber activity, although each policy differs regarding the level of risk exposure. During the course of this paper's consultations, American International Group (AIG), Chubb, Marsh, St. Paul Insurance Company, and Zurich North America were identified as insurance companies having some type of coverage available for cyber-incident risks.

In the section below, we present the coverage provided by two major providers of cyber insurance, AIG netAdvantage® Suite and Zurich's The E-RiskEdge™ Product (in both cases, the language afforded is that of the provider). While these two insurance providers offer a larger range of products than those listed below, these coverages — loss/corruption of data, business interruption, liability, cyber extortion, and rewards — were the ones discussed most frequently during the stakeholder interviews.

Loss/Corruption of Data

"Coverage for the damage, destruction, corruption or theft of the insured's important information assets, including bandwidth, due to a covered computer attack." (AIG)

"This coverage pays the actual cost incurred to restore electronic data or software that has been destroyed or damaged by a loss event." (Zurich)

Business Interruption

"Coverage that protects the insured's income, both online and offline, in the wake of a computer attack. Coverage also includes extended business interruption and dependent business interruption." (AIG)

"This coverage not only replaces business income and additional expenses incurred as a result of interrupted e-business services caused by a loss event but also pays up to certain limits for the cost of investigating the reason for the loss of service." (Zurich)

Liability

Network Security Liability – AIG

> "Coverage for damage and defense costs suffered by others in the wake of a computer attack upon the insured's network, including liability caused by transmission of a computer virus, unauthorized access, denial-of-service, disclosure or confidential information and identity theft."

E-business Loss Event Liability – Zurich

"Covers claim losses the insured is legally obligated to pay as well as associated defense expenses resulting from covered loss events."

Web Content Liability – AIG

"Coverage for content-based injuries such as libel, slander, defamation, copyright title, trademark infringement or invasion of privacy arising from the display or material on the insured's web site."

Electronic Publishing Liability – Zurich

"Covers liability for libel, slander, or disparagement of any person or organization as well as for violating the right of privacy of a person or for the infringement of a copyright, title, trademark, etc. resulting from electronic publishing through the covered electronic business system."

Cyber Extortion

"Coverage for the investigation and settlement of an extortion threat against the insured" (AIG)

"Covers money paid as the direct result of a threat made by someone to alter or destroy covered electronic business systems, commit a computer theft or to disseminate or improperly use any confidential information related to the insured's e-business activity or contained in their electronic data." (Zurich)

Rewards

"Coverage up to $50,000 (reward fund) available for information that leads to the arrest and conviction of individual(s) committing or attempting to commit a computer attack or other qualifying criminal acts. This coverage is provided with no applicable retention. (AIG)

"This coverage provides for the payment for information leading to the arrest and conviction of any individual committing, or trying to commit, any illegal act related to certain loss events." (Zurich)

D. Evaluation of the Cyber Insurance Market

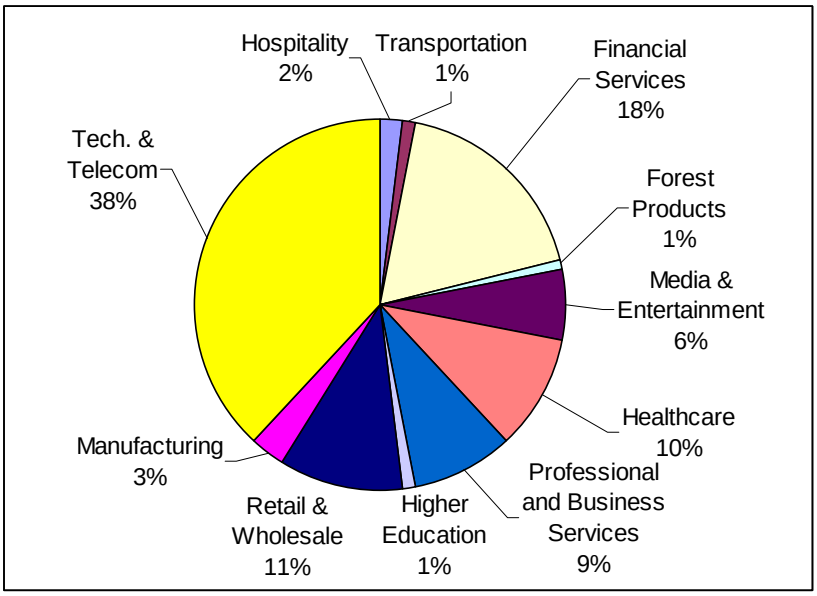
The types of cyber-incident risk coverage for businesses are in their initial stages of implementation. In order for a specialty product to become successful, it must have a few years of practical application to determine pricing, capacity, conditions for insurability, and other issues.

From 2000 to 2002, the number of cyber-incident policies issued in the U.S. grew by 30 to 40 percent. The increase in demand for this type of coverage is largely attributable to the impact of the 9/11 attacks on business and recognition and analysis of risk. As companies become more informed about cyber insurance, the market has the potential to

become one of the biggest growth areas for insurers over the next few years — one that could develop into a $3.6 billion U.S. market by 2005 (Insurance Information Institute, 2003).

As shown in Chart 4.1 below, the technology and telecommunications industry accounts for 38 percent of the cyber insurance policies being purchased in the U.S. by industry groups.

Chart 4.1 Purchases of Cyber Insurance by Industry Group, United States, 2003



Source: Marsh Inc. – Benchmarking August 2003.

E. Current Issues with Cyber Insurance

In this section, we describe current issues and sentiments connected with cyber insurance, as conveyed to us by senior officials of the insurance, reinsurance, and e-business solution industries during our consultation with industry stakeholders.

While our literature review indicated a sentiment that risk managers are looking toward the use of insurance to manage cyber-incident risk, our consultation with insurance, reinsurance, and e-business solution stakeholders did not point to the same conclusion. The discrepancy between these two sources is likely attributable to the "real world" impact of four prominent cyber insurance issues: price of insurance, lack of knowledge surrounding cyber-incident risks, self-insurance, and the use of risk management. Each of these is discussed, in turn, below.

Price of Insurance

Insurance companies that currently underwrite cyber-incident risks have noticed many challenges with this coverage. Many of the industry stakeholder respondents noted that one obstacle to getting businesses to purchase cyber insurance coverage is the lack of funds that senior management are willing to spend on insurance. One representative of a cyber insurance company observed that, while high premiums apply to cyber-incident coverage, these fees must be maintained until such a time as more data exist to permit more accurate price setting.

The Insurance Information Institute reports that small companies are foregoing cyber-incident coverage, not because of their lack of risk management, but because of a lack of funds. When asked why businesses are not investing in cyber-incident insurance, the majority of our insurance, reinsurance, and e-business solution industry stakeholder interviewees stated that most of their clients are too small to afford the cost of insuring for this risk. This same issue is apparent in the makeup of companies that seek e-business solutions for cyber-incident risks: the majority of e-business solution interviewees stated that their main clientele was comprised exclusively of Fortune 500 and large multi-national organizations.

Lack of Knowledge Surrounding Cyber-Incident Risks

The existing knowledge of cyber insurance is extremely low. For example, the Assurex *E-Risk Survey* states that more than 80 percent of respondents either do not have cyber insurance or are unaware of their company's existing insurance policy protection against such losses (Assurex International, 2000).

Insurance company interviewees cited senior management's lack of knowledge regarding cyber-incident risks as another cause of business' apparent reluctance to purchase cyber insurance. With the exception of businesses that currently have cyber-incident risk coverage, most small- to mid-sized companies are said to lack a risk manager and some businesses are said to lack an IT department for even a preliminary risk assessment.

It was suggested during stakeholder interviews that the larger Fortune 500 companies rely heavily on the knowledge of their IT departments to control risk (with a common sentiment being that IT professionals are often reluctant to have their systems perceived as vulnerable, such that they often report to senior management that their systems are "secure", even when they may not be). One insurer representative asserted that if a company believes that it is not vulnerable to these types of risk, it will not inquire about specific insurance to protect against these events.

A representative of an insurer that provides cyber insurance coverage made mention of the ambiguity of the term, "cyber", and noted a preference for another term, "network security risk". This insurer representative asserted that if senior management do not understand exactly what they are spending money on (that is, in the circumstance when

the term, "cyber", is used), there is a greater risk that they will not think that "cyber" insurance applies to them.

Self-Insurance

Insurance Canada reports that more than one-third of the world's leading companies are not sufficiently prepared to protect their top revenue sources (Insurance-Canada.ca, 2003). They believe that the majority of businesses are looking beyond insurance to protect their assets and are spending to protect revenue sources through business continuity planning and contingency planning measures. Companies have begun to look inward to self-insure their organizations because of rising premiums associated with cyber insurance.

Our literature review indicated that some businesses are self-insuring against cyber-incident risk through improvements in computer software and hardware, and without the aid of cyber insurance coverage. E-business solution interviewees reported that cyber-incident risks are increasing and they ranked their own ability to identify their clients' risks at a "good" or an "excellent" level. While these e-business solution providers strive to remain a "step ahead" of technology — and while they also acknowledge that it is difficult to anticipate the next potential cyber-incident — they do not believe that insurance is required to protect against these threats. Indeed, one of the stakeholder interviewees stated that "if our business went down on a Friday afternoon, our first response would not be to call our insurance broker, but would be to fix the problem and get back up and running again." While there are major difficulties in assessing the risks posed by technology, these respondents asserted that there are unknown circumstances that surround computer and cyber-incidents — indefinite circumstances that even insurance companies would have difficulty responding to.

Use of Risk Management

There was agreement between e-business solution interviewees that they must review their own exposure to cyber-incident risk (although there was a difference of opinion concerning the method of risk management that they should implement). All of the companies that were interviewed had recently audited the security of their systems, installed viruses to protect against intrusion, and established some form of employee training program to better manage their risks (albeit that stakeholder interviewees were not aware of their own insurance coverage for cyber-incident risk). While few industry stakeholder interviewees had experienced any malicious attacks or virus intrusions in the past 12 months, they still believe that cyber-incident risks are real and will continue to increase. Even with their belief that cyber-incidents will increase, e-business solution interviewees think that the remedy is the identification and management of risk through business continuity plans and investments in more secure hardware and software — options that e-business solution interviewees regard as more economically feasible for their clients than insurance.

E-business solution providers believe that they are aware of the risks to which companies are vulnerable and they offer services to prevent these losses from occurring. E-business solution interviewees noted that their companies provide services to firms at risk for business continuity — providing support such as data recovery, and mitigating software and hardware products that secure the system prior to an attack. E-business solution interviewees observed that all of the businesses that employ their services have an existing structure in place (such as a risk manager) to identify the need for these services.

Risk managers are beginning to see an increase in corporate reliance on computer systems to connect their offices with both suppliers and customers. They have begun investing in risk management practices to protect their organization. "A global survey released in September 2002 by the National Association of Manufacturers, Redsiren Technologies and the Internet Security Alliance found that 88 percent of respondents said that their firms now recognize information security as an issue essential to the survivability of their business." (Willis, 2003). To maintain a level of security in their respective companies, risk managers must apply a risk management model that includes risk identification, mitigation, and monitoring.

The use of risk managers is low in small- to mid-size companies, while larger multi-national companies are better able to support a risk management staff. While large corporations, such as Fortune 500 companies, are able to identify and manage their cyber-incident risks through the use of mitigation and loss prevention methods, small- to mid-sized companies have fewer remedies available. These companies typically manage their risks through the purchase of software and hardware products to secure their systems against malicious attacks, viruses, and theft of proprietary data. (Risk management practices are discussed later in this paper.)

Privacy Issues

Cyber incidents may impinge on the privacy of personal information, which is now protected by legislation in a number of countries. In Canada, the federal government passed the Personal Information Protection and Electronic Document Act (PIPEDA). This legislation applies to third-party personal data, not employee data, and includes non-compliance penalties such as public disclosure of information practices, fines, and court-ordered damages. Effective in 2004, the law regulates all personal information collected, used, or disclosed in the course of commercial activity. In reaction to the law, cyber insurance providers expect that their clients will seek coverage against breaches in third-party personal data. Provincial governments have not been as active in adopting their own legislation.

5.0 Loss Prevention and Mitigation

The insurance industry has an important role to play in the promotion of loss prevention and mitigation. By writing policies to insure against cyber-incidents, insurers provide risk transfer for cyber exposure, including incentives to employ best practices and improved mitigation strategies for managing these risks. While insurance can be an efficient method of risk transfer, it is not the only way for businesses to protect themselves from losses due to cyber incidents — these organizations can also focus attention on mitigation techniques to assess and reduce their vulnerability to cyber-incident risk. Certainly, growing dependence on information networks and changes in technology make it critical for businesses to adopt effective techniques to mitigate information security risks and to prevent losses. Information that flows freely over networks can be intercepted by outside sources, which make businesses vulnerable to copyright and other violations.

The insurance industry believes that mitigation techniques (for example, risk avoidance, deterrence, prevention, detection, recovery, and transfer) are essential toward improving the insurability of businesses and government agencies against cyber-incident risk (Gordon, et. al., 2003). In our consultations with insurance, reinsurance, and e-business solution stakeholders, we heard a sentiment that businesses need to recognize that risk mitigation has a powerful influence on spending for information security solutions, and that businesses must be able to identify what risks exist in relation to their critical information. By quantifying risks, businesses are in a better position to address those cyber-incidents that are expected to have the greatest potential impact.

A. A Cyber-Incident Risk Management Framework

Gordon, Loeb and Sohail describe a cyber-incident risk management framework for information security. Figure 5.1 illustrates the authors' risk management framework to reduce and maintain risk at an appropriate level.

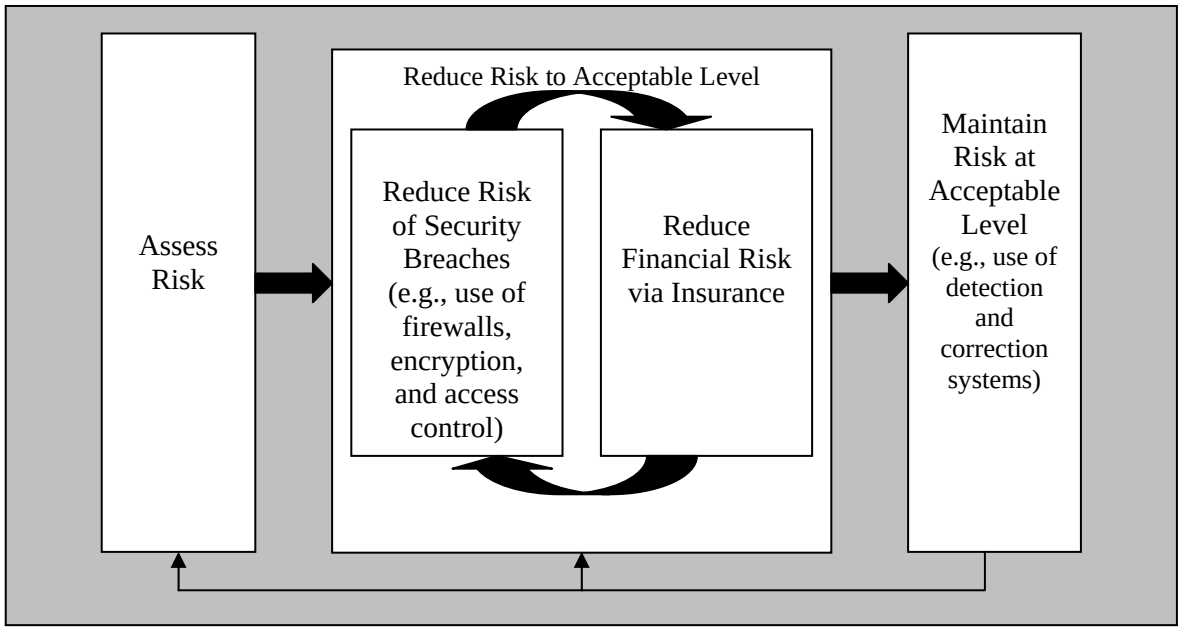
As shown in Figure 5.1, the authors' risk management framework involves a three-step process:

1. **Assess risks**. This requires companies to determine their own risk exposure and true costs. They must determine what their current level of insurance covers, including existing computer systems and the level of maintenance required.

2. **Reduce risks**. There are several techniques that can be employed to reduce risk, such as employee education, upgrades to anti-virus software and operating systems, increased security protocol, improvements in monitoring systems to detect intrusions, and the use of firewalls, encryption, and access control.

3. **Maintain an acceptable level of risk**. This can be achieved by determining the type of insurance policy required for each particular company, including the methods employed to reduce potential losses and increase security measures.

Figure 5.1 A Cyber-Incident Risk Management Framework



Source: Gordon, Loeb and Sohail, 2003.

6.0 Conclusion

This paper has described the costs and vulnerabilities associated with, and the ability of insurance to provide coverage for, cyber-incident risk, including hacking or unauthorized use of computer systems, denial of service, theft of proprietary information, and virus distribution. The research has indicated clearly that:

- cyber-incidents are pervasive, costly, and escalating;
- the insurance industry has a meaningful role to play in cyber-risk transfer and loss prevention;
- risk reduction and mitigation strategies play a critical function in securing systems; and
- cyber-incident statistics need to improve.

We discuss these, in turn, below.

Cyber-incidents have become quite extensive in the business community, with roughly 90 percent of U.S. companies currently reporting unauthorized system access, and cyber-incident losses shared roughly one-third each between denial of service, theft of private information, and virus distribution and other attacks. Considering virus attacks alone, some measures of the annual global financial impact of such strikes indicate a twenty-fold to forty-fold increase over the period from 1995 to 2003. Cyber-incidents are increasing in scale and expense.

Despite challenges, insurance can play a meaningful role in cyber-risk transfer and loss prevention. While standard insurance policies do not cover cyber-incident risk exposure, the insurance industry has designed a cyber-incident insurance product that responds to consumer needs. Recent (2002) estimates place business purchases of cyber-incident insurance coverage at $150 million to $300 million with the technology and telecommunications industry being the largest purchaser of cyber insurance policies in the U.S. With estimates of potential cyber-related losses in the billions of dollars, the insurance industry believes that mitigation techniques (for example, risk avoidance, deterrence, prevention, detection, recovery, and transfer) are essential toward improving the insurability of businesses and government agencies against cyber-incident risk. By writing cyber insurance policies, insurers provide risk transfer for cyber exposure, including incentives to employ best practices and improved mitigation strategies for managing these risks.

There exists a perception that cyber-incident risks are more significant for large multi-national firms because of their exposure and their capacity to afford insurance. Cyber premiums range from $7,000 to $85,000 per $1.5 million worth of coverage, depending on the size and exposure of each company to online or electronic risk. Consequently, many companies look inward and self-insure their organizations. In this regard, risk

reduction and mitigation strategies (including the purchase of software and hardware products, such as upgrades to anti-virus software and operating systems, increased security protocol, improvements in monitoring systems to detect intrusions, and the use of firewalls, encryption, and access control) play a critical function in securing systems.

Cyber-incident statistics need to improve. The insurance industry is currently confronted by a dearth of cyber-incident data and insurers have been obligated to price cyber-incident coverage without being able to completely quantify risks. Additionally, cyber-incident crime may be one of the most under-reported forms of criminal behaviour in Canada. Because of the under-reporting of cyber-incident attacks (businesses are reluctant to report incidents for fear of economic losses), historical data on which to base cyber insurance premiums are limited.

After only a few years of experience with cyber-incident insurance coverage, it is clear that a sizeable market for the product has yet to emerge. Initial pricing for the coverage is material, and reinsurers continue to exclude it from their policies. Large amounts of new capital are not currently available to property-casualty insurers to fund cyber-incident risks. While the inability of insurers to fully fund such high-severity events may cause businesses to question the value of cyber-incident risk coverage, given time, awareness, and the prospect of additional cyber-incident attacks, more businesses are expected to seek insurance coverage.

7.0 References/Bibliography

Aarsteinsen, Barbara. (2002). "Cyber Threat." http://www.insurance-canada.ca/ ebusiness/canada/ciBACyber200208.php (25 July 2003).

American International Group. (2002). "Incidents: Internet Liability, Cyber-Crimes, and EBusiness Interruptions." http://www.aignetadvantage.com/bp/servlet/ unprotected/claims.examples (27 August 2003).

Assurex International. (2000). "E-Risk and E-Insurance Fact Sheet." http://www.assurex.com/Admin/eriskfact.asp (18 June 2003).

Brush, Colleen. (2001). "Cyber insurance." http://infosecuritymag.techtarget.com/articles/ november01/industry_cyber insurance.shtml (25 July 2003).

Cantanese, Joseph. (2003). "Insurance: New Coverage on the Block." http://wasteage.com/ar/waste_new_coverage_block/index.htm (27 August 2003).

Cisco Systems. (2001). "Economic Impact of Network Security Threats." http://www.cisco.com/warp/public/cc/so/neso/sqso/roi1_wp.pdf (28 August 2003).

Click for Cover. (2003). "Esurance." http:www.clickforcover.com/products/ esurance.html (14 August 2003).

Computer Economics. (2004). *Virus Attack Costs on the Rise – 2004 Update*. California: Computer Economics, March 2004.

Computer Security Institute. (2003). "CSI/FBI Computer Crime and Security Survey." http://www.gocsi.com/forms/fbi/pdf.jhtml (14 August 2003).

Denning, Dorothy. (2000). "Cyberterrorism." http://www.cs.georgetown.edu/~denning/ infosec/cyberterror.html (June 16 2003).

Ernst & Young Assurance and Advisory Business Services. (2003). "Global Information Security Survey 2003." http://www.ey.com/global/download.nsf/International/ TSRS_-_Global_Information_Security_Survey_2003/$file/TSRS_-_Global_Information_Security_Survey_2003.pdf (28 August 2003).

Globe Advisor. (2003). Top Tech Companies. http://www.globeinvestor.com/series/ top1000/tables/tech/2003/?ga (23 September 2003).

Gordon, Lawrence A., Martin P. Loeb, and Tashfeen Sohail. (2003). A Framework for Using Insurance for Cyber-Risk Management. Communications of the ACM. Vol. 46, No. 3: 81-85.

IBC. (1999). Insurance and the Year 2000. Insurance Bureau of Canada.

IBC. (2003). "General Insurance Industry." http://www.ibc.ca/gii.asp (9 October 2003).

IBM Global Services. (2003). "Business Continuity and Security." http://www-1.ibm.com/services/feature/security_replay.html (15 August 2003).

ICD. (2003). "Worldwide Internet Security Software Market Forecast and Analysis 2002-2006: Vendor Views." http://www.idcresearch.com/en_US/commerce/idcStore.jhtml (15 August 2003).

Insurance-Canada.ca. (2003). Insurance Marketing Information from Around the World. http://www.insurance-canada.ca/market/other/FMGlobal200304.php (28 August 2003).

Insurance Information Institute. (2003). "Cyber Insurance." http://www.iii.org/media/hottopics/insurance/cyber insurance/content.print/ (10 September 2003).

Insurance Information Institute. (2003). "Most Companies Have Cyber-Gaps in Their Insurance Coverage." http://www.iii.org/media/updates/press.735620_content.print/ (18 August 2003).

International Information Industry Congress. (2000). "Cyber Crime." http://www.iiicongress.org/ accepted/ap00-itac.pdf (15 August 2003).

Kelly, Susan. (2003). "Cyber Insurance Still Rare." http://www.treasuryandrisk.com/article.asp?ID=141 (13 August 2003).

Kolodzinski, Oscar. (2002). "Cyber Insurance Issues: Managing Risk by Tying Network Security to Business Goals." *The CPA Journal*. http//www.nysscpa.org/cpajournal/2002/1102/nv/nv4.htm (27 August 2003).

Kowalski, Melanie. (2002). Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics. Ottawa: Statistics Canada.

Kunreuther, Howard. (1998). "Insurability Conditions and the Supply of Coverage." Paying the Price: The Status and Role of Insurance Against Natural Disasters in the United States. Ed. Howard Kunreuther, and Richard J. Roth Sr. John Henry Press, Washington, D.C. 17-50.

Lewis, James A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington: Centre for Strategic and International Studies.

Marsh Inc. (2003). "Benchmarking August 2003." http:// www.marsh.com/MarshPortal/PortalMain?PID=AppPublicHomePage (8 October 2003).

McAfee Security. (2003). "New Cyber Coverage on the Block." http://dispatch.mcafee.com.esecuritynews/juns2003/news_cybercoverage.asp (27 August 2003).

Pethia, Richard D. (2003). "Cyber Security – Growing Risk from Growing Vulnerability" http://www.cert.org/congressional_testimony/Pethia_testimony_06-25-03.html (24 November 2003).

Purdy, Margaret (2001). "Speeches." Office of Critical Infrastructure Protection and Emergency Preparedness. http://www.ocipep.gc.ca/whoweare/speeches/ mp_ciss_e.asp (18 August 2003).

RIMS. (2003). http://www.rims.org/Content/NavigationMenu/AboutRIMS/ Whats_a_risk_manager_/Whats_a_risk_manager_.htm (8 October 2003).

Rossi, Michael A. (2002). "Stand-Alone E-business Insurance: Who's Buying It, Who's Selling It, and Why?" http://www.irmi.com/expert/articles/rossi012.asp. (30 October 2003).

Royal Canadian Mounted Police. (2001). "Hackers: a Canadian police perspective." http://www.rcmp-grc.gc.ca/crim_int/ hackers_e.htm (19 August 2003).

Sagalow, Ty R. (2001). Insurance Coverage Evaluation for Cyber-Risks. European American Business Journal. Spring 2001.

Schneier, Bruce. (2001). Insurance and the Computer Industry. Communications of the ACM. Vol. 44, No. 3: 114-115.

Senate Committee on Security and Intelligence. (1999). "The Report of the Special Senate Committee on Security and Intelligence." http://www.parl.gc.ca/36/1/ parlbus/commbus/senate/com-e/secu-e/rep-e/repsecintjan99-e.htm (9 September 2003).

Smith, David M. (2000). "The Cost of Lost Data." *Storage Management Solutions.* http://www.wwpi.com/Archive/show_article.asp?ArticleID=616 (28 August 2003).

Spagnuolo, John. (2003) "Cyber Terrorism: Is the Insurance Industry Prepared?" *The National Underwriter Company.* http://www.nationalunderwriter.com/tech/news/ viewFeatures.asp?articleID=466 (25 July 2003).

Tapia, Catherine. (2000). "Cyber Insurance Policies Require Careful Examination." http://www.brownandriding.com/ financial_3e.htm (19 June 2003).

Vatis, Michael A. (1999). "NIPC Cyber Threat Assessment, Statement by Director, National Infrastructure Protection Center, FBI." http://www.fbi.gov/congress/congress99/nipc10-6.htm (25 August 2003).

Willis. Market Realities and Risk Management Solutions. Global Solutions. (2003). http://www.willis.com/adviser/news/adv_news.nsf/(Threads)/EF9C07E9A481F1CA80256CB50051D879/$FILE/Marketplace_Realities.pdf. (31 October 2003).

Yu, Peter K. (2002). "What Businesses Should Know About Cyberterrorism". *Computer Crime Research Centre*. http://www.crime-research.org/eng/library/Peter.htm (17 June 2003).

Appendix A – Interviewees

Insurance and reinsurance companies interviewed:

American International Group (AIG)
AON Re Canada Inc.
Aviva Canada Inc.
Chubb Insurance Company of Canada
The Co-operators General Insurance Company
The Dominion of Canada General Insurance Company
ING Canada
Munich Reinsurance Company of Canada
TOA Reinsurance Company
The Wawanesa Mutual Insurance Company
Zurich North America Canada

E-business solution providers interviewed:

Cognos Inc.
EDS Canada
Entrust
IBM Canada

Appendix B – Insurer Interview Questions

Respondent Name: _____

Title: _____

Company Name: _____

Telephone Number: _____

Interviewer Name: _____ Date: _____

Start Time: _____ am/pm

Introduction

Hello, my name is _____, from the Institute for Catastrophic Loss Reduction. The ICLR is currently involved in a federal government initiative to research the insurance industry and its role in cyber-risk transfer and loss prevention. We're conducting a survey of risk managers and insurance providers to identify what you and other insurance companies believe are the current issues affecting your clients and the demands that they are requiring to protect against these losses. This study will be used to determine the current risks facing e-business companies and how these risks are affecting insurance coverage. Your answers will be kept completely confidential.

Main Questionnaire

1. How many years have you worked in insurance and risk management?

   _____ Years

   Not Sure

2. Looking forward to the next couple of years, what would you say are the three or four most important areas of risk that your company will be dealing with?

   Employment Risks – employee liability
   Computer/Internet Risks
   Product Liability
   Operational/Business Risks
   Energy/Pollution Risks
   Weather Related Risks
   Security Risks
   Health Care/Public Health Risks

3. Companies today are increasingly relying upon sophisticated computer hardware, networks and software, in order to use and store important company data. In your view how great are the risks and liabilities that your clients' companies face from technology in today's economy? Please use a 1 – 10 scale, where 10 means that your company faces major risks and 1 means you face virtually no risk at all.

   _____ (1-10) Not Sure

4. With an increase in computer related business, how great do you think your clients' risks will be in the near future? Please use a scale of 1 – 10 again. 10 meaning that your clients will face major risks in the near future and 1 meaning you will face virtually no risk.

   _____ (1-10) Not Sure

5. How good of a job would you say that your clients are doing in identifying potential risks and liabilities arising from Internet technology and e-commerce activities?

   Excellent
   Good
   Fair
   Poor
   Not Sure

6. How good of an understanding do you feel that you have of the technology risks that your clients' companies may be facing?

   Excellent
   Good
   Fair
   Poor
   Not Sure

7. What are the most difficult aspects of assessing the risks posed by technology to your clients' companies?

   Unknown or unforeseen circumstances
   Understanding of current insurance policies
   Staying informed and updated to current risks, issues and insurance policies
   Lack of information about risk and insurance
   Difficulty and uncertainty with properly identifying risks and hazards
   Communication barriers
   Lack of security
   Lack of historical data on risks
   Other: _____

8. How good of an understanding would you say that each of the following groups in your clients' companies has about technology risks and how to minimize them?

   Company's employees in general
   The IT of MIS department
   Company's top management, such as the CEO

9. Have your clients' companies taken any of the following steps in reviewing their exposure to and coverage for technological risk?

   Reviewed existing insurance coverage to determine which cyber-incident risks are covered
   Inventoried and quantified the types and extent of risks vulnerable to
   Added new coverage to cover these risks
   Worked with insurer to identify risks
   Retain a consultant to identify cyber-incident risks

10. How adequately do your company's current property-casualty insurance program offerings cover the various liabilities arising from technology?

    Very adequate
    Somewhat adequate
    Not very adequate
    Not adequate at all
    Not Sure

11. Do your existing insurance product offerings cover any of the following types of technology risks?

    Damage or destruction of data by employees or hackers caused by malicious acts
    Unauthorized access to computer systems and misappropriation of data
    Access to and misappropriation of your clients' intellectual property
    Computer Fraud
    Errors and omissions resulting from your clients' services or products

12. Are any of your clients adding insurance for these types of loss? Approximately what percentage of companies?

    _____ 0-4
    _____ 5-24
    _____ 25-49
    _____ 50-100

13. Have your clients' companies experienced losses from any of the following in the past 12 months or so?

    Yes
    No
    Not Sure

14. Did their property-casualty insurance cover this monetary loss, or not?

    Yes
    No
    Not Sure

List of Cyber-Incident Issues (for Questions 13-14)
Denial of service problems
Computer virus infestation, such as the Love Bug
Customer data privacy breaches
Employee data privacy breaches
Any type of malicious act to the computer system
Other problems related to technology: _____

15. Is there specific coverage for technological risk that you feel that your clients should have, but don't have now?

    Yes
    No
    Not Sure

    If yes, what types of coverage do you think these companies are missing?

    _____
    _____

16. What are the main reasons for these companies to overlook this insurance coverage?

    Believe they have cyber-incident coverage through existing insurance
    They have not fully assessed their cyber risks and exposures
    Coverage for cyber-incident is too expensive
    Their insurance broker has not offered them this coverage
    The underwriting of this insurance is not well established
    They do not experience major cyber-incident losses

17. Who in your clients' companies has the primary responsibility for identifying and monitoring risks from technology?

    Risk Manager
    IT Department
    Other: _____

18. Do your clients have risk management committees or other structures to identify and monitor technological risk?

    Yes
    No
    Not Sure

19. What types of information exist to determine cyber-incident risk, including the cost of insuring for this risk?

    _____
    _____

20. How is this loss shared and what role does it play in the underwriting of cyber risk insurance?

    _____
    _____

21. What is the nature of the cyber insurance market?

    National
    Global

22. What is the role of reinsurance and other methods of risk transfer?

    _____
    _____

23. Are there differences in the nature and extent of cyber-incident risk in different industrial sectors? For example, are energy and utilities services, transportation, communications, government and private industry differentially exposed to cyber-incident risk?

    _____
    _____

24. Are those sectors also differentially served by the insurance industry in addressing this exposure?

_____

25. What are your companies practices in terms of the following:

a) What kinds of cyber-risks are insurable and which are not?

_____

b) What are the criteria for insurability?

_____

c) What is the scope of products available for this risk?

_____

d) What new product developments are emerging?

_____

e) What do insurers require from insureds in the way of loss prevention and mitigation to qualify for insurance?

_____

Thank You for your Participation!

End Time: _____ am/pm

Appendix C – E-Business Solution Provider Interview Questions

Respondent Name: _____

Title: _____

Company Name: _____

Telephone Number: _____

Interviewer Name: _____ Date: _____

Start Time: _____ am/pm

Introduction

Hello, my name is _____, from the Institute for Catastrophic Loss Reduction. The ICLR is currently involved in a federal government initiative to research the insurance industry and its role in cyber-risk transfer and loss prevention. We're conducting a survey of risk managers and insurance providers to identify what you and other e-business companies believe are the current issues affecting your clients and the demands that they are requiring to protect against these losses. The study will be used to determine the current risks facing e-business companies and how these risks are changing. Your answers will be kept completely confidential.

Main Questionnaire

1. How many years have you worked in e-business and risk management?

   _____ Years

   Not Sure

2. Looking forward to the next couple of years, what would you say are the three or four most important areas of risk that your company will be dealing with?

3. Companies today are increasingly relying upon sophisticated computer hardware, networks and software, in order to use and store important company data. In your view how great are the risks and liabilities that your company faces from technology in today's economy? Please use a 1 – 10 scale, where 10 means that your company faces major risks and 1 means you face virtually no risk at all.

   _____ (1-10) Not Sure

4. With the increase in computer related business, how great do you think your risks will be in the near future? Please use a scale of 1 – 10 again. 10 meaning that your company will face major risks in the near future and 1 meaning you will face virtually no risk.

   _____ (1-10) Not Sure

5. Does your company currently engage in any e-business or e-commerce, such as selling products over the Internet or provide e-services for other businesses?

   Yes, does engage in e-business or e-commerce
   No, does not engage in e-business or e-commerce
   Not Sure

   a) If no, are you planning on beginning any e-business in the near future?

   Yes
   No
   Not Sure

6. How effective do you think your company is in identifying potential risks and liabilities arising from Internet technology and e-commerce activities, either in your company or with your clients systems?

   Excellent job
   Good
   Fair
   Poor
   Not Sure

7. What are the more difficult aspects, if any, of assessing the risks posed by technology?

   For Example:
   Unknown or unforeseen circumstances
   Understanding fully current insurance policies
   Staying informed and updated to current risks, issues, and insurance policies
   Lack of information about risk and insurance
   Difficulty and uncertainty with properly identifying risks and hazards
   Communication barriers
   Lack of security
   Lack of historical data on risks
   Other (specify): _____

8. How good an understanding would you say that each of the following groups has regarding technological risks,

	Excellent	Good	Fair	Not Very Good	Unsure
Company's employees					
Your IT department					
Your company's top management, such as the CEO					

9. Has your company taken any of the following steps in reviewing your exposure to and coverage for technological risk?

    a. Reviewed existing insurance coverages to determine the extent to which it covers risks from technology
    b. Inventoried and quantified the types and extent of risks resulting from technology
    c. Considered adding new types of policies that cover risks from technology
    d. Worked with your IT, legal and security departments to identify emergency risks
    e. Worked with your insurer or broker to identify possible risks
    f. Retained a consultant to conduct an audit of technology risks

10. Has your company done any of the following:

    a. Audited the security of your systems
    b. Installed anti-virus software
    c. Installed firewalls to protect against hackers
    d. Established standard security procedures
    e. Implemented employee training programs to better manage technology risk
    f. Other: _____

11. How adequately does your current property-casualty insurance program cover the various liabilities arising from technology?

    Very adequate
    Somewhat adequate
    Not very adequate
    Not adequate at all
    Not sure

12. Do your existing insurance policies cover any of the following cyber-incident risks?

    Damage or destruction of data by employees or hackers caused by malicious acts
    Unauthorized access to computer systems and misappropriation of data
    Access to and misappropriation of your company's intellectual property
    Computer fraud
    Errors and omissions resulting from your services or products
    Unintentional infringement of the intellectual property of others' (copyright, trademark, and patent infringement
    Product liability insurance for software and hardware products
    Sexual harassment resulting from inappropriate e-mail from a company employee
    Telecommunications theft

13. Has your company experienced losses from any of the following in the past 12 months or so?

    Yes
    No
    Not Sure

14. If you were to experience a loss, do you believe your current insurance policies largely cover the monetary loss, or not?

    Yes
    No
    Not Sure

15. Did your property-casualty insurance largely cover this monetary loss, or not?

    Yes
    No
    Not Sure

Cyber-Incident Issues (for Questions 13-15)
Denial of Service Attacks (how many hours was service denied)
Computer Virus infestation, such as the Love Bug
Unauthorized intrusion into systems by hackers
Customer data privacy breaches
Employee data privacy breaches
Y2K problems
Unintentional infringement of intellectual property of others (copyright, trademark or patent infringement)
And type of malicious act to your computer system or systems you rely upon.

16. Who in your company has the primary responsibility for identifying and monitoring risks from technology?

    Risk Manager
    IT Department
    Other

17. What is the title of the person in your company who you would say is most responsible for identifying technological risk?

    _____
    _____

18. Who else is involved? What are their titles

    _____

19. Does your company have a risk management committee or any other formal structure to identify and monitor technological risk?

    Yes
    No
    Not Sure

20. How effective is this group in evaluating technological risks?

    Very effective
    Somewhat effective
    Not really effective
    Not effective at all
    Not Sure

21. Based upon your company's experience with issues, such as the Love Bug, Melissa Virus, W32.Blaster, are your clients more likely to seek out ways to identify and manage technological risk, less likely or they have had little impact?

    More likely
    Less likely
    Didn't have much impact
    Not Sure

22. Which are your most important sources for information about cyber-incident risks?

    Insurance Broker
    Insurers
    IT Department
    Consultants
    Seminars
    Trade Publications
    Other Risk Managers
    Media/News
    Legal Department
    Other

23. What would a company need to do in order to be perceived as a leader in the area of insuring technological risk?

    _____
    _____

    Anything else?

    _____

24. Has your executive management allocated a budget for e-commerce initiatives?

    Yes
    No
    Not Sure

25. What are your company's annual sales revenues? An estimate is fine.

    Less than $50 million
    $50 million - $99.9 million
    $100 million - $149.9 million
    $150 million - $199.9 million
    $200 million - $249.9 million
    $250 million - $499.9 million
    $500 million - $749.9 million
    $750 million - $999.9 million
    $1 billion - $4.9 billion
    $5 billion and above

26. Does your company conduct more than 25% of its business outside of Canada?

    Yes
    No
    Not Sure

27. How many full-time employees do you have at all of your locations?

    Less than 100
    100 – 249
    250 – 499
    500 – 999
    1,000 – 1,499
    1,500 – 1,999
    2,000 – 4,999
    5,000 – 9,999
    10,000 – 19,999
    20,000 and above

Thank You for your Participation!

End Time: _____ am/pm