# Cyber Risks

## Implications for the Insurance Industry in Canada

EMERGING ISSUES
RESEARCH SERIES

Insurance Institute

# **Cyber Risks:**
Implications for the insurance industry in Canada

## Executive summary

The Canadian insurance industry ranked cyber security as third among the ten most important issues facing the property and casualty insurance industry at this time.

Cyber security incidents are in the news almost every day. Management of cyber risks has emerged as a major issue for the insurance industry and society. This report assesses cyber security from the perspective of the insurance industry in Canada. What is the threat? Who are the criminals? Why is there a growing concern about catastrophic incidents? How can property and casualty insurers reduce their risk of loss? What is the prospect for growth in the cyber insurance market? How will regulation of the Internet, disclosure, and privacy legislation evolve over the next five to ten years?

- Estimated global costs of cyber crime: Between $375 and $575 billion.
- Estimated global damage resulting from vehicle collisions: $518 billion.
- Estimated global cyber insurance premiums: less than one-half of one percent of the estimated cost of cyber crime.
- Estimated global auto insurance premiums exceed international estimates of vehicle collision damage.

A report by Intel's McAfee and the Center for Strategic and International Studies estimates that the global cost of cyber crime in 2013 was between $375 billion and $575 billion.[1] (All figures presented in this report are stated in U.S. dollars.) The global impact of cyber crime is similar to estimates by the United Nations of the international production, trafficking, and sales of illicit drugs ($400 billion)[2] and the worldwide damage resulting from vehicle collisions ($518 billion).[3] There is uncertainty over the precise extent of cyber crime, yet it is agreed that the impact is significant and growing.

The most recent KPMG survey of leaders in the Canadian insurance industry ranked cyber security as third among the ten most important issues facing the property and casualty insurance industry at this time.[4] Extensive personal information about customers attracts identity thieves, extortionists, and fraudsters. Advanced analytics, agency portals, online policy applications, and apps for filing claims provide new strategic capacity for insurers. These advances also increase the ways criminals can attack the insurance industry. Cyber incidents can result in significant damage, including the cost of response to the theft of consumer information, forensics, notification, fraud monitoring, crisis communications, and legal fees. Reputational risks may be more significant. Insurance is built on a foundation of trust. It is easy for insurance consumers to move their business if that trust is broken. A major cyber incident may erode consumer confidence, harm an insurer's reputation, and reduce the market value of the company.

There is considerable scope for insurance to penetrate into new fields of cyber security.

Cyber security is also a business opportunity for insurers. Presently, the majority of companies in Canada, including most insurers, do not purchase cyber insurance.[5] Over the next five to ten years, this is expected to change. Breach coverage is one of the fastest growing insurance markets in the United States, Europe, and Canada. Insurers also provide identity theft coverage for individuals.

[1] McAfee and Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, p. 2.

[2] Leduc and Lee, *Illegal Drug Trafficking*, p.1.

[3] Peden et al., *World Report on Road Traffic Injury Prevention*, p. 5.

[4] KPMG, "Canadian Insurance Industry Risks & Opportunities," forthcoming.

[5] A.M. Best, "Fall 2014 Insurance Industry Survey," p. 2.

However, most cyber risks are not insured. Global cyber insurance premiums, for example, are presently less than one-half of one percent of the estimated cost of cyber crime. In contrast, global auto insurance premiums exceed international estimates of vehicle collision damage. Beyond the insurance industry's success with breach and identity theft coverage, there is considerable scope for insurance to penetrate into new fields of cyber security. Current barriers to expansion include the difficultly in determining calculable risk due to the absence of information about the likelihood and consequences of cyber attacks seeking to steal trade secrets, and the accumulation risk if millions or perhaps hundreds of millions of policyholders experience loss from a single, catastrophic cyber incident.

*The insurance industry is well positioned to promote cyber security, just as the industry is a champion for road safety, crime prevention, and fire prevention.*

Despite barriers to the provision of insurance coverage for all cyber risks, the insurance industry is well positioned to promote cyber security, just as the industry is a champion for road safety, crime prevention, and fire prevention. Also, evolving federal and provincial privacy legislation will have a significant influence over insurance practices. Insurance companies providing cyber insurance may become more actively engaged in contributing to the federal government's cyber security strategy. There is scope for insurers to work with the government to secure increased information about the frequency and severity of cyber incidents, and to determine the role of the federal government if a catastrophic event should occur.

This is a critical time for the Canadian insurance industry to explore cyber security.

# Contents

# Foreword

The Insurance Institute is proud to publish this first of a series of reports on emerging issues impacting the property & casualty insurance industry in Canada.

Our intention is to provide research of value to our stakeholders. We are confident that this research report, and those to follow, will provide information and insights to enable insurance organizations to broaden their understanding of how emerging risks will impact the delivery of insurance products and services in Canada.

This report on Cyber Risks provides a significant launch to this Emerging Issues Research Series. The topic of cyber risks and cyber security seems omnipresent in the media but, for the most part, has an international focus. We saw an opportunity to research the topic from the perspective of our industry in Canada and particularly as it relates to the potential frequency and severity of cyber risks and security breaches.

We saw cyber space as the great unknown frontier that we – society in general and the insurance industry in Canada specifically – are engulfed in, but can't fully comprehend. The scope and potential capacity of cyber criminals is growing. Meanwhile, the capacity to defend and the capacity to transfer the risk may be limited.

This report provides a broad scope perspective to what is known about cyber crime today, and the current and potential cyber activities and events that could impact society in general and the insurance industry, in the near future.

It is our hope that you will find this research report interesting and insightful, with helpful resources and constructive recommendations.

Sincerely,

Peter Hohman

Peter Hohman, FCIP, MBA, ICD.d
President & CEO, Insurance Institute of Canada

# Introduction

Canada is one of the most wired countries in the world. Statistics Canada reports that in 2013, 89 percent of Canadian businesses used the Internet, and nearly every enterprise used some form of information technology.[6] The Canadian Internet Registration Authority found that 87 percent of Canadian households were connected to the Internet in 2013, the second highest rate among the G-7 nations.[7] The Authority also found that the number of web pages visited each month by Canadians is the highest in the world, and the average time spent online is second highest. Canadians use computers, phones, and other connected devices to conduct business, communicate, and entertain themselves. Over the last 25 years, cyberspace has reshaped how Canadians live, work, and socialize.

### Growth of Cyberspace Globally

| Year | Internet Users (millions) | Websites (thousands) |
|---|---|---|
| 1995 | 44.8 | 23.5 |
| 1996 | 77.4 | 257.6 |
| 1997 | 120.8 | 1,117.3 |
| 1998 | 188.0 | 2,410.1 |
| 1999 | 280.9 | 3,177.5 |
| 2000 | 413.4 | 17,087.2 |
| 2001 | 500.6 | 29,254.4 |
| 2002 | 662.7 | 38,760.4 |
| 2003 | 778.6 | 40,912.3 |
| 2004 | 910.1 | 51,611.6 |
| 2005 | 1,029.7 | 64,780.6 |
| 2006 | 1,157.5 | 85,507.3 |
| 2007 | 1,373.0 | 121,892.6 |
| 2008 | 1,562.1 | 172,338.7 |
| 2009 | 1,752.3 | 238,027.9 |
| 2010 | 2,034.3 | 206,956.7 |
| 2011 | 2,272.5 | 346,004.4 |
| 2012 | 2,511.6 | 697,089.5 |
| 2013 | 2,712.2 | 672,985.2 |
| 2014 | 2,925.2 | 968,882.5 |

Source: Internet Live Statistics

Worldwide, the number of people connected to the Internet tripled over the past decade from almost one billion in 2004 to almost three billion in 2014.[8] The number of people in the world is growing by 80 million a year, while the number of people connected to the Internet is growing by more than 200 million a year. Within the next five years, more than half of the people in the world will be connected to the Internet. There were 50 million websites in the world in 2004. There were almost one billion websites in 2014, a remarkable 20-fold increase over ten years. The rapid growth in Internet users and websites is expected to continue for the next five to ten years, particularly in emerging economies. Rich and poor, north and south, the Internet is bringing the world together, creating a global village. Cyberspace has become indispensible for commerce and communications.

This transformation has also been evident in the insurance industry. Digital technology is essential for the insurance industry in Canada and around the world to manage its business and interactions with consumers. The insurance industry uses computers to store consumer information, resolve and pay damage claims, and assess the risk of future losses. Consumers can go online to secure information about insurance products and pricing, purchase coverage, or make a claim. Insurance has gone digital.

Furthermore, some insurers provide cyber insurance. Recent surveys suggest that within the next five to ten years, most businesses will consider purchasing cyber insurance coverage.[9] The largest and fastest growing element of the cyber insurance market involves insuring the costs associated with a major data breach. In contrast, corporate espionage, catastrophic cyber incidents, and several other cyber risks are largely uninsurable at this time. For individuals, insurance is available to cover the costs associated with identity theft. Most other cyber threats are presently not insurable, such as insuring the cost of repairing or replacing an infected computer.

The Internet of tomorrow will almost certainly be less resilient, available, and robust than today.

[6] Statistics Canada, "Digital Technology and Internet Use," p. 3.
[7] Canadian Internet Registration Authority, "The Canadian Internet," p. 1.
[8] Accessed at www.internetlivestats.com.
[9] Munich Re, *Munich Re Cyber Risk Survey*, p. 1.

## More frequent and severe attacks are expected

A relatively stable environment has supported the remarkable expansion of cyberspace over the last 25 years. This is expected to change. Cyber crime is increasing, and experts warn that cyberspace will become much more dangerous over the next five to ten years.[10] Stories about disruption and loss from cyber events found in books, movies, and television are increasingly expected to become reality. The Internet of tomorrow will almost certainly be less resilient, available, and robust than today. Local cyber incidents may cascade into global shocks. Canadians and the Canadian insurance industry are particularly vulnerable because of heavy reliance on technology.[11]

The Internet may be the most complex system ever created by humankind, and humanity's track record of managing complex systems includes both successes and failures. Society's reliance on the Internet is growing exponentially, but the capacity for controlling developments in cyberspace has not been able to keep pace. Many technology experts and risk managers do not appear to recognize the risk of a major cyber shock over the next five to ten years. As a result, risk managers, corporate executives, and public officials may not be adequately preparing for a catastrophic incident. A focus on current and emerging threats to individual organizations has resulted in little attention on long-term, system-wide cyber threats. This report will explore how society is vulnerable to a catastrophic cascading cyber incident.

*This report will explore how society is vulnerable to a catastrophic cascading cyber incident.*

IBM reports that about half of the known cyber incidents to date have been directed toward manufacturing companies and financial service providers.[12] This includes the insurance industry. Most Canadians purchase property and liability insurance coverage for their businesses, homes, and vehicles. The insurance industry has information about tens of millions of customers, a large number compared to many other industries. Insurance consumer files include detailed information needed to assess the risk of loss.

However, the property and casualty insurance industry in Canada is very competitive, and this information is spread across more than 300 insurers and tens of thousands of brokerages. The amount of consumer information in each company is smaller than in Canada's largest manufacturers, banks, retailers, and communications companies. Moreover, criminals have more difficulty gaining financially from insurance data than from banking and manufacturing data. As a result, the Canadian property and casualty insurance industry has been a less attractive target for cyber criminals than large banks and manufacturers.

Reported cyber crime rates have been much lower in Canada than those in the United States and Europe. The difference in losses shows that the most attractive initial targets for casual hackers and cyber criminals have been located in the United States and Europe. Cyber security practices in Canada appear to be similar to those in other advanced countries, so fewer losses in Canada are not due to superior security practices. Nevertheless, there is an expectation that attacks on the insurance industry and other businesses around the world will increase in frequency and severity over the next five to ten years.[13]

*Nevertheless, there is an expectation that attacks on the insurance industry and other businesses around the world will increase in frequency and severity over the next five to ten years.*

The Internet has been an important contributor to many of the recent gains experienced by society. Moreover, much of the innovation and promise anticipated over the next few years is based on the assumption that society will become even

[10] World Economic Forum, "Global Risks 2014," and Zurich Insurance and Atlantic Council, "Beyond Data Breaches."

[11] Deloitte, "Global Cyber Executive Briefing," p. 2.

[12] IBM, *Security Services Cyber Security Intelligence Index*, p. 4.

[13] World Economic Forum, "Global Risks 2014," and Zurich Insurance and Atlantic Council, "Beyond Data Breaches."

more dependent on the Internet. Some of the expected changes include more flexible work arrangements, paperless offices, driverless cars, and low-cost communications. However, these innovations may be threatened because of cyber crime's potential to disrupt this essential foundation of modern society.

*Cyber security was identified as "the risk most underestimated by businesses."*

The Allianz Risk Barometer summarizes the responses from an annual survey of more than 500 risk managers and insurance experts in almost 50 countries.[14] Cyber security ranked fifteenth highest in 2013, eighth in 2014, and fifth in 2015 among the risks identified by international business leaders participating in the survey. Despite the increasing concern about cyber risks over the years, cyber security was identified in the 2015 Allianz survey as "the risk most underestimated by businesses."

The following chapters seek to address a number of important questions as Canada's insurance industry considers cyber security:

- What are the most common forms of attack?
- Who are the criminals and what are they after?
- What are the losses experienced in cyberspace?
- Why are severe disruptions expected to increase?
- How can insurers improve their cyber defenses?
- Why is the cyber insurance market now growing?
- How will evolving regulations affect cyberspace?

[14] Allianz, "Allianz Risk Barometer: Top Business Risks 2015," pp. 6 – 7.

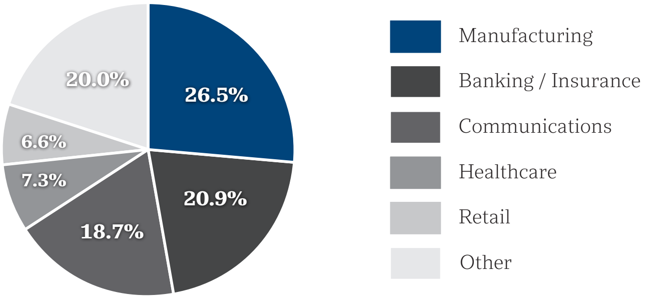
# What are the most common forms of attack?

### Common forms of cyber attacks

- Theft and other data attacks
- Malware (phishing and pharming)
- Mechanisms to infect computers

A complex array of cyber crimes has emerged over the past 25 years. These include attacks that seek to steal or corrupt data and actions that target computer systems to gain control over critical infrastructure. Data attacks that directly target computers include worms and viruses. Crimes that use computer networks include fraud (such as identity theft or phishing scams), harassment (such as stalking or bullying), and theft (such as stealing intellectual property or confidential consumer information).

Cyber Incidents by Industry



Source: IBM

Canada's insurance industry is primarily focused on attacks that steal or corrupt data and result in a data breach or identity theft. Over time, the nature of cyber attacks has changed. Initial attacks focused on system flaws and technological weaknesses. This included worms and viruses that spread without human direction to deliver malicious software. Increasingly, however, cyber risks also focus on human behaviour. Criminals seek to lure their victims with deception and carefully crafted schemes tailored to achieve a specific result. The particular elements of attacks are constantly evolving as new tools become available. Several common forms of cyber attack are explored below.

## Theft and other data attacks

The majority of cyber criminals seek to steal or corrupt personal and corporate data. In 2013, the 3,700 clients of IBM's Managed Security Services experienced seven or eight cyber incidents each month, on average. Half of these attacks were directed at the manufacturing (27 percent) and financial services (21 percent) industries.[15] These included scams to steal credit card information, website vandalism, corporate espionage, and denial-of-service attacks.

Data attacks are common because they are easy to conduct. Many people have the capacity to carry out these attacks. The tools are readily available

[15] IBM, *Security Services Cyber Security Intelligence Index*, p. 4.

and powerful. For example, an off-the-shelf computer can test millions of passwords per second. Most passwords can be cracked in less than a minute. The programs to conduct most attacks, including the tools to support sophisticated campaigns, are available online.

The majority of Canadians, including most employees, are highly vulnerable in cyberspace. Most Canadians have weak password protection on their computers, do not use password protection on their mobile devices, use the same password for multiple applications, and seldom change their passwords. Canadians may make themselves more vulnerable when they use aids to remember passwords, credit card information, billing addresses, and other data.

## Malware

Most of the early infectious software programs were written as pranks or experiments. The objective of many hackers in the 1990s, for example, was to explore weaknesses in computer systems to demonstrate what was possible in cyberspace through innovative programming. Today, malicious software (malware) is the tool most frequently used by cyber criminals to achieve financial gain. Criminals use malware to steal personal, financial, and business information, or disrupt computer networks. Hackers and other cyber criminals use malicious software for the most common forms of attack in cyberspace.

*Criminals use malware to steal personal, financial, and business information, or disrupt computer networks.*

### Denial-of-service attacks

Malware can be used to create botnets to build a network of computers that can be hijacked and controlled remotely. These servers and personal computers operate normally until a controller takes charge. A remote network will typically involve thousands of computers scattered over a broad geographic area, but may include more than one million computers. In a distributed denial-of-service attack, many computers are directed to overwhelm an Internet site, disrupting or shutting down operations.

Candid Wueest, a cyber security expert at Symantec, estimates that about 10 percent of distributed denial-of-service attacks are directed at banks and other financial institutions.[16] Sometimes a small attack is used to gain the attention of the institution. These attacks may include a request for payment to prevent a larger attack. The extortion requests are sometimes small, perhaps less than $300, to determine the victim's willingness to pay. There have been reports of demands in excess of $100,000. Sometimes denial-of-service attacks are used to mask incidents whose purpose is to steal personal or corporate information.

Symantec reports that almost half of denial-of-service attacks involve gaming. Some gamers use targeted denial-of-service attacks to enhance the likelihood of winning a competition or to escalate a dispute. Attackers can purchase a brief attack lasting a few minutes for as little as $5. An extensive attack lasting several days costs a few thousand dollars. The Symantec report references a study by Prolexic, a denial-of-service mitigation provider, which found that the average denial-of-service attack lasts 17 hours. Symantec reports that attackers have recently begun using shorter but more intense attacks, using amplification tools to increase the impact of the attack.

*In 2013, phishing of a contractor led to the theft of millions of customer files from Target. In 2014, phishing was used to steal personal and credit card information from millions of shoppers at Home Depot.*

### Phishing and pharming

An email that appears to be from a trusted source may include a compelling request for the user to share confidential information such as their social insurance number, date of birth, mother's maiden name, personal identification numbers,

[16] Wueest, "The Continued Rise in DDoS Attacks."

credit card information, or sensitive corporate information. Phishing is a broad request asking many users to share confidential information. Spear phishing is a focused request targeting specific users. Pharming also seeks to obtain personal information, but rather than exchanging data through email, the user is directed to a false website to submit information.

To get confidential information, criminals may send the user upsetting or exciting information designed to trigger an urgent response. Some users act before taking the time to think about the situation. The target may be asked to update, validate, or confirm information, a request designed to create the sense that the inquiry is legitimate because the user had previously shared these data. Some criminals follow up with a phone call to further increase the apparent validity of the request and gather additional information.

Email Spear Fishing Campaigns
(globally, on average, per day)

| | |
|---|---|
| 2011 | 165 |
| 2012 | 408 |
| 2013 | 779 |

Source: Symantec

Having obtained this personal information, criminals may be able to access bank accounts, open new accounts, transfer funds, apply for a loan, create a credit card, make purchases, receive government benefits, obtain a passport, or secure a driver's licence. The criminal may use sensitive corporate information to access personal and corporate data. In 2013, phishing of a contractor led to the theft of millions of customer files from Target. In 2014, phishing was used to steal personal and credit card information from millions of shoppers at Home Depot.

## Watering holes and social engineering

Cyber criminals often use psychological manipulation to achieve their goals. In addition to phishing attacks, some common scams include watering holes, pretexting, baiting, and quid pro quo. These techniques are used to deceive users into sharing sensitive information, like passwords and banking information, with a criminal masquerading as a trusted entity.

Watering holes are an emerging technique criminals are using to launch cyber attacks.[17] Specific individuals are identified as worthwhile targets. The criminals identify and infest websites that are likely to be visited by the targeted individuals. The attackers then wait for the targets to visit the website (the watering hole). During the visit, malware is sent to the computer of the target. Typically, the goal is to obtain remote control over the target's computer to support the theft of corporate and personal information. Individuals who are resilient to attacks using phishing and spear phishing have fallen victim to watering hole attacks.

A growing field of cyber security research is focused on social engineering—that is, how to protect people from being manipulated into inadvertently assisting cyber criminals. Because of the escalating use of social engineering by attackers, companies are encouraged to establish a culture of security. These organizations work to build understanding and awareness throughout the company about the threat of attack and best practices to minimize the risk of loss. Social engineering focuses on human behaviour and decision-making designed to complement and work with investments in technical security systems.

*Because of the escalating use of social engineering by attackers, companies are encouraged to establish a culture of security. These organizations work to build understanding and awareness throughout the company about the threat of attack and best practices to minimize the risk of loss.*

[17] Symantec, *Internet Security Threat Report* 2014, p. 6.

### Ransomware

A ransomware scam begins when a user opens a downloaded file and infects their computer. When the file is opened the malware is released and it locks the computer. A message is displayed demanding a payment of a few hundred dollars to unlock the computer. Payment of the ransom, however, does not restore the computer. The first ransomware scams posted a notice that a software licence with Microsoft had expired, and the computer would become functional again when a licensing fee was paid.[18] These scams have evolved. Now they frequently include a notice from what appears to be local law enforcement requesting that a fine be paid because the user has been caught with pirated software or downloaded pornography. These scams generate millions of dollars of revenue for criminals.

## Mechanisms to infect computers

An ongoing challenge for casual hackers and cyber criminals is to get their malware installed on computers. Many mechanisms have emerged. The most common are viruses, worms, and Trojan horses.

### Viruses and worms

Most of the earliest attacks in cyber space involved viruses and worms. These are stand-alone malware programs that self-replicate and automatically spread to other computers. They are designed to exploit vulnerabilities in network server programs. A computer virus infects executable applications, including the operating system. A worm infects documents and other non-executable files. Viruses and worms transmit themselves from computer to computer through networks.

Web Attacks Blocked
(globally, per day)

| | |
|---|---|
| 2011 | 190,000 |
| 2012 | 464,100 |
| 2013 | 568,700 |

Source: Symantec

Viruses and worms scan the available networks and replicate in vulnerable computers. Because they need no human intervention they can spread quickly and to a large number of unprotected computers. In 1988, for example, Robert Morris, a graduate student at Cornell University, released a worm that ultimately infected between five and ten percent of the servers in the world. The Morris worm was one of the first known cyber attacks. It is also one of the most widespread attacks on record. In 2003, one of the fastest attacks, the Slammer worm, spread to 75,000 computers in less than ten minutes.

Viruses and worms can be designed to provide a back door to an infected computer, permitting remote access and supporting denial-of-service attacks. Some programs have the capacity to delete, encrypt, or transmit files from an infected system. These programs can be used by criminals to steal personal and corporate data, or may be part of an extortion scheme.

> One attack targeting a major bank resulted in the theft of personally identifiable information for millions of customers. Debit cards and personal identification numbers were stolen. This information was used to create phony debit cards with stolen data embedded on the cards. The cards were then used to withdraw several million dollars in cash from automatic bank machines around the world.

[18] O'Gorman and McDonald, "Ransomware: A Growing Menace."

### Trojan horse

Most malicious programs are designed to operate with minimal risk of detection. They are typically disguised as something normal or desirable, so users are tricked into loading the program on their computer. With a Trojan horse, a user is enticed to run a program. The program is described in terms that are easily misunderstood and in a way that conceals its harmful effects. A Trojan horse may be designed to encrypt files, or download and execute malicious functions. Spyware and adware, for example, deceive the user into providing consent, allowing attackers to argue that they are not in breach of privacy laws.

A Trojan horse is not self-replicating like a computer virus or worm, but it can be programmed to achieve similar objectives. In particular, a Trojan horse can be used to create a back door and allow an infested computer to be controlled remotely. Trojan horses account for the majority of new infections of computers.[19]

### Cyber security terms

A variety of terms and expressions are used to describe cyber issues. These terms change frequently as new threats emerge and attacks evolve. The Government of Canada provides a useful source of information about cyber expressions through Public Safety Canada's Get Cyber Safe program. This can be accessed at: http://www.getcybersafe.gc.ca/cnt/rsrcs/glssr-eng.aspx.

Two other sources of information about cyber terminology include the Glossary of Security Terms provided by the SANS Institute (http://www.sans.org/security-resources/glossary-of-terms/) and Techterms.com (http://techterms.com). The SANS Institute is the largest organization in the world providing security training and certification. Techterms.com is an online dictionary of computer and technology terms.

## Supervisory control and data acquisition systems (SCADA)

Over the past 25 years, computer-based control systems have been introduced to monitor and remotely control critical infrastructure.[20] These systems are commonly used across Canada's critical infrastructure, including electric power generation and transmission, oil and gas refining and pipelines, water treatment and distribution, and railways and mass transit systems. Cyber attacks could be used to disable or to gain control over these systems. Increasing connectivity means that the failure of one critical component may have far-reaching effects over large geographic areas. Disruptions may have serious commercial and societal consequences that cascade across sectors and jurisdictions.

Attackers with basic skills have the potential to cause significant harm, while sophisticated attackers have the potential to cause catastrophic damage. Persistent actions often begin with probes to determine the specific nature of the control systems and the security in place. This may be followed by spear phishing, watering holes, and other attacks seeking to gain remote control over the computers of some key individuals who have internal control over the system. A major attack will require financial resources, skilled programmers, and patience. Attacks on control systems and critical infrastructure will likely focus on sabotage that causes physical damage, disruption, and threats to public safety, rather than espionage that steals information and trade secrets.

*Persistent actions often begin with probes to determine the specific nature of the control systems and the security in place. This may be followed by spear phishing, watering holes, and other attacks seeking to gain remote control over the computers of some key individuals who have internal control over the system.*

[19] Doherty, Krysiuk and Wueest, *The State of Financial Trojans 2013.*
[20] Shaw, "SCADA System Vulnerabilities to Cyber Attack."

A 2014 report on cyber threats to Canada's critical infrastructure describes how systems depend on secure Internet communications and are vulnerable to attack.[21] The banking, insurance, and other financial services industries account for 20 percent of Canada's annual production and are the largest sector in the country. Banks and the other financial institutions are heavily dependent on information technology and communications. This report notes that oil and gas industry leaders have expressed fears that cyber attacks could destroy facilities or severely disrupt production and deliveries to Canadian and export markets. Canada's mass transit system may soon become much more dependent on the Internet. For example, the report describes Bombardier's Primove as a fully integrated urban public transit system. Wireless technology would be used to recharge batteries, schedule transit routes, manage ticketing, and many other functions. Canada's critical infrastructure depends on secure Internet communications and is vulnerable to cyber attacks.

> In 2001, 800,000 litres of untreated sanitary waste was released into the rivers and coastal waters as the result of a cyber attack in Queensland, Australia.[22] An individual decided to attack the waste treatment facility. He was frustrated with his former employer and unable to secure full-time employment with the local government that owned the facility. While working with his former employer, the attacker helped to install the control system for the treatment facility. He gained considerable knowledge about the controls. On at least 46 occasions over a two-month period he directed radio commands to the sewage equipment controls, eventually resulting in the release of untreated sanitary waste into local parks, rivers, and the grounds of a Hyatt Regency hotel.

Admiral Michael Rogers, head of the National Security Agency and the top cyber security official in the United States, issued a warning in late 2014 that three countries may now have the capacity to remotely shut down the national power grid and other critical infrastructure in the United States.[23] In his view, the regular reconnaissance of hackers is a warning that it is only a matter of time until there is a major attack. NATO organized war games in which member countries responded to simulated cyber attacks on critical infrastructure. This was the largest known digital warfare exercise to date. On a smaller scale, attackers could take control of a railroad system and order two trains onto the same track. The resulting collision could significantly erode public confidence in the safety of the transportation network.

Those managing critical infrastructure have made significant investments in security, including systems to manage the risk of physical and cyber attacks. Nevertheless, the risk of attacks to gain remote control over critical infrastructure remains a serious concern.

## IN SUMMARY

***Infections by malicious software (malware) using Trojan horses and phishing have replaced self-replicating viruses and worms as the most common forms of attack by cyber criminals. Attackers design strategies and schemes using social engineering to entice users to download malware. The strategies used by cyber criminals shift and evolve quickly, seeking to stay a step ahead of security systems. Some current threats, such as Trojan horses and watering holes, did not exist a few years ago. New threats will emerge over the next five to ten years, likely targeting cloud computing, cell phones, and other devices connected to the Internet. An effective cyber security strategy must be flexible to evolve with the changing threat.***

[21] Gendron and Rudner, *Assessing Threats to Canadian Infrastructure*, pp. 14 – 16.

[22] Abrams and Weiss, "Malicious Control System Cyber Security Attack," p. 1.

[23] Rogers, "Cybersecurity Threats," pp. 12 – 13.

# Who are the criminals and what are they after?

**Many different kinds of people use cyberspace to commit crimes**

- Digital natives
- Disgruntled insiders
- Professional criminals
- State-sponsored attackers

Many different kinds of people are using cyberspace to commit crimes. The motivation for most cyber crimes can be clustered into four broad areas:

- Stealing or destroying information
- Exploiting victims through bullying or stalking
- Stealing corporate knowledge and trade secrets
- Attaining political goals through state-sponsored and terrorist attacks

Those exploiting the Internet range from joy seekers to terrorists. They include adventurers, cyber pirates, bullies, hackers, stalkers, pedophiles, fraudsters, extortionists, organized criminals, state-sponsored corporate spies, and terrorists. Four groups are explored below: digital natives, disgruntled insiders, professional criminals, and state-sponsored attackers.

The threat to Canada's insurance industry includes casual hackers, insiders, and cyber criminals. Casual hackers account for the largest number of attacks on the insurance industry. Most are testing their ability to break into computer systems and they do not intend to cause harm. However, some hackers are policyholders using their computer skills to secure justice for a perceived mistreatment by their insurer. Insider attacks are rare, but these individuals have knowledge that can cause great harm to the operations and reputation of their victims. Cyber criminals have primarily focused on the banking, manufacturing, and retail industries, but when they turn their attention to insurers they have the skills to cause considerable damage. Cyber criminals seek to steal private personal information about consumers and sell it for financial gain or use it for extortion purposes.

## Digital natives

Most people working in the Canadian insurance industry remember milestones when digital technologies, like computers and cell phones, were introduced into workplaces and homes. Some individuals, however, have grown up in a world that always had the Internet. Marc Prensky has written extensively about learning and education. He describes people born before 1980 as digital immigrants, and those born after 1980 as digital natives. Most digital natives are fluent and comfortable using technology at school, home, and work.[24] Cyberspace is a world that digital natives have known for their entire lives.

Some hackers are policyholders using their computer skills to secure justice for a perceived mistreatment by their insurer.

Statistics Canada reports almost 85 percent of Canadians between the ages of 16 and 24, but less than 9 percent of Canadians over the age of 65, accessed the Internet using mobile devices in 2012.[25] Digital natives spend more time than older Canadians on the Internet. Most activities are legal, but some are not.

[24] Prensky, "Digital Natives, Digital Immigrants," pp. 1 – 2.
[25] Statistics Canada, "Canadian Internet Use Survey."

The Recording Industry Association of America cites a NPD Group report that in 2009 consumers paid for only 37 percent of the music downloaded in the United States.[26] In 2013, V.I. Labs reported that 43 percent of the software operating in the world was unlicensed.[27] V.I. Labs also cited CodeAmour Intelligence reports that in 2011 the countries with the most illegal software were China, Russia, Taiwan, and the United States, while Canada was ranked ninth. GO-Gulf reports that 70 percent of individuals see nothing wrong with downloading pirated music and films.[28] The use of technology to bully others may contravene emerging provincial legislation, yet it remains disturbingly commonplace. Most Internet users explore cyberspace, and some gain access to private and confidential corporate or personal information. Some Canadians use the Internet to pursue political objectives like civil disobedience, protests, and activism. This may include illegal activities, like attacks that contribute to denial-of-service.

The number of digital natives in Canada with the skills to exploit the Internet will increase over time. The required equipment – a connected laptop, tablet, desktop computer, or phone – is becoming more affordable every year. The software to conduct attacks can often be freely downloaded. In addition, relatively few resources have been invested in law enforcement to detect and catch cyber criminals, so there appears to be little prospect of punishment, particularly for cross-border attacks. There are no firm data on illegal behaviour by digital natives, particularly for casual hackers, but it appears to be growing.

*The required equipment – a connected laptop, tablet, desktop computer, or phone – is becoming more affordable every year. The software to conduct attacks can often be freely downloaded. In addition, relatively few resources have been invested in law enforcement to detect and catch cyber criminals, so there appears to be little prospect of punishment, particularly for cross-border attacks.*

From the perspective of the insurance industry in Canada, attacks by casual hackers must be addressed due to their frequency. These include hackers exploring their capacity to break into an insurer's systems, and policyholders seeking justice for perceived wrongful action. Casual hackers account for the majority of attacks on the insurance industry (See Appendix II), and these are expected to increase in frequency over time. The potential consequences of these attacks will grow as the tools to cause disruption become increasingly available.

## Disgruntled insiders and inadvertent actors

IBM reports that most cyber attacks begin outside of the target company, but estimates that 20 percent of incidents involve malicious insiders.[29] A further five percent involve insiders who participate unwittingly. Focusing on data breach attacks, Verizon reports that deliberate, accidental, or unintentional actions by insiders account for five to ten percent of breaches.[30] Verizon reports that only 21 percent of insider breach compromises in 2013 involved remote access and "the majority of employees perpetrated their acts while in the office right under the noses of their co-workers, rather than hopping through proxies from the relative safety of their house."[31] Some employees, consultants, and former employees know where the most valuable information is stored. Insiders and former insiders have the potential to carry out highly damaging and potentially prolonged attacks, without arousing suspicion until the damage is done.

[26] Recording Industry Association of America, "Scope of the Problem."
[27] Accessed at http://www.vilabs.com/resource-section/stat-watch .
[28] GO-Gulf, "Online Piracy in Numbers."
[29] IBM, *Security Services Cyber Security Intelligence Index*, p. 6.
[30] Verizon, *2014 Data Breach Investigations Report*, figure 5, p. 8.
[31] Ibid., p. 24.

Some examples illustrate insider cyber incidents:

- An employee of L'Hôpital Montfort in Ottawa lost a memory stick with records for 25,692 patients, and the hospital is presently subject to a $40 million class action lawsuit.[32]
- A Lockheed Martin employee used his company authorization to download hundreds of documents with confidential trade secrets before resigning and giving the documents to a competitor.[33]
- An employee resigned who was responsible for identifying acquisition targets for International Airport Centers. Before he returned his laptop, a secure-delete program wiped the memory. The employer could not undelete files and investigate if the employee had done anything wrong.[34]
- A temporary computer technician terminated by Forbes erased all the data on five of the publisher's eight servers, and no data could be restored.[35]
- A temporary employee in the anti-fraud department of the Korea Credit Bureau collected personal information on a memory stick for more than 20 million individuals over a 15-month period, and then sold the data to telemarketers.[36]

Inadvertent actors comprise a small part of the attacker population. These insiders have the potential to cause significant losses. Company insiders who are unwittingly recruited to aid criminals with malicious intent can contribute to highly damaging attacks without arousing suspicion. This may involve information stolen from a laptop, tablet, or cell phone. The stolen information appears to offer authorized outside access to corporate information systems. A major concern is that attacks may be successfully sustained over a prolonged period of time.

## Professional criminals

Cyberspace provides a livelihood for a growing number of criminals. In the past, a few skilled individuals committed most professional cyber crimes. This is changing. Criminal organizations now frequently work with teams of technology professionals to plan and commit crimes. Cyber crimes are an element of a range of traditional illegal activities that include theft, fraud, and illegal gambling. The crimes are not new, but they are evolving to take advantage of new technologies. They are also becoming more widespread and damaging. International criminal networks sometimes bring together individuals from around the world to commit crimes on an unprecedented scale. Determining attribution is difficult with cyber attacks, particularly with large, complex attacks across national borders.

*For example, before the high-profile 2014 attacks on Sony Pictures, the attackers warned Sony that the company would be "bombarded" unless it paid monetary compensation for perceived damage that had been inflicted.*[37]

Many cyber criminals are highly skilled. This is their chosen profession, and they have learned how to acquire and apply the most effective tools of the trade. They are strongly motivated to avoid detection. Professional criminals spend time practicing and honing their skills in a way that most casual hackers do not. Moreover, their motivation is to secure financial gain through theft and extortion, so few barriers constrain their attacks. The exploitation of unwitting insiders, for example, may be one step in a larger attack, with little thought about the impact on the individuals involved.

[32] Meckbach, "OIAA Speaker Explains How Ontario Civil Law on Privacy Affects Cyber Liability Exposure," p. 2.
[33] Lemley, "When Disgruntled Employees Attack."
[34] McCullagh, "Police Blotter: Ex-employee Faces Suit over File Deletion," p. 2.
[35] Harvey, "Battling Employee Sabotage in the Wired Workplace," p. 2.
[36] Osborne, "South Korean Credit Card Firms Suspended over Data Breach."

Professional criminals often seek to steal personal data and corporate secrets. This information has value and can be sold to others. It can also be used to extort money from corporate victims. For example, before the high-profile 2014 attacks on Sony Pictures, the attackers warned Sony that the company would be "bombarded" unless it paid monetary compensation for perceived damage that had been inflicted.[37]

Criminals can secure financial gain by selling the information. SecureWorks, the information security subsidiary of Dell Computers, estimates that for bulk orders of 2,000 or more, high-quality stolen credit cards can be purchased for $9 each. Some orders include a complementary training tutorial for hackers and a "100% satisfaction guarantee or the cards will be replaced."[38] Shear and Stewart, writing for SecureWorks, report that the personal information needed to create a new identity can be purchased for $250 to $350. This would include a working social insurance card with a matching name and address. This is the information needed to obtain a driver's licence, birth certificate, or passport. Alternatively, counterfeit foreign passports can be purchased for between $200 and $500, and a driver's licence for between $100 and $150. This may be a small amount of money for each transaction, but the values accumulate when the information is sold in volume.

*For example, JPMorgan Chase Bank responded to the 2013 attacks on its systems with a public commitment to spend $250 million a year and maintain a staff of more than 100 individuals to protect itself from cyber crimes.*

A distributed denial-of-service attack is designed to flood a website with so much traffic that the website must go offline and become inaccessible to users. Symantec, a leading supplier of cyber security services for corporations and Norton products for individuals, estimates that the going rate for a denial-of-service attack ranges from $5 to over $1,000.[39] In contrast, the loss experienced by the company attacked can be significant. This may include sales lost while a website is not operating, and sales lost over the long-term if consumers move their business to another company.

The financial gains for criminals are small for a single piece of information but can be significant when large volumes of information are secured. Moreover, the greatest value for the stolen data is often found with the company that has been attacked, so extortion is a growing cyber crime. The proceeds also appear small when compared to the cost of defending against criminal attacks. For example, JPMorgan Chase Bank responded to the 2013 attacks on its systems with a public commitment to spend $250 million a year and maintain a staff of more than 100 individuals to protect itself from cyber crimes.

*McAfee identified one study of the cost of cyber crime in Italy that found actual losses of $875 million, but recovery and opportunity costs for the victims of these attacks was almost 10-fold higher, at $8.5 billion.*

A report by Intel Security's McAfee observes that a criminal may expect to gain $50 if they steal and sell a bicycle that is a $500 loss for the owner.[40] There is a large difference between the gain made by a criminal and the loss experienced by a victim in the physical world and also in cyberspace. McAfee identified one study of the cost of cyber crime in Italy that found actual losses of $875 million, but recovery and opportunity costs for the victims of these attacks was almost 10-fold higher, at $8.5 billion.[41]

## State-sponsored attackers

State-sponsored cyber attacks are an emerging means to achieve political, military, and economic objectives. Most countries, including Canada, have established active defences against cyber threats. Several countries are now also engaged in attacks. These countries view cyber attacks as a low-cost, high-payoff way to achieve national goals. This may involve crippling

[37] Byford, "Sony Pictures Hackers Sent Ominous Email to Executives Warning of Attack."

[38] Shear and Stewart, *Underground Hacker Markets*, pp. 5 – 6.

[39] Wueest, "The Continued Rise of DDoS Attacks," p. 12.

[40] McAfee and Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, p. 6.

[41] Ibid., p. 18.

foreign financial institutions, stealing military secrets, or disrupting commerce in a rival nation. For example, Appendix III describes an attack on the chemical industry. There is the potential for state-sponsored attacks on the insurance industry.

With a few exceptions, nation-states are the only organizations with the capacity to conduct large-scale and persistent cyber attacks. The attacks should not be viewed as ends in themselves, rather they are a means to achieve a variety of political goals. State-sponsored cyber attacks tend to have a clear motive, and determination of the motive can be essential in determining who the attackers are and the best defence to mitigate losses.

Attribution of responsibility for cyber attacks is difficult, particularly for state-sponsored incidents. Many attacks are designed to be covert and these are not visible for the public. Effective attacks include many layers of secrecy. Attacks can be run through third-party systems or sympathetic arm's-length organizations. In this way the state that was directing the attack could deny its involvement. One of the greatest challenges involved in defending against cyber attacks is the problem of correctly identifying the perpetrator.

Cyber security experts, like Kenneth Geer and others at FireEye, believe that the determination of the most likely source of a state-sponsored attack should be based on understanding the unique history and political system of each country.[42] The distinctive characteristics of state-sponsored attacks frequently reflect the essential qualities of the sponsor nation. As discussed below, forensic experts at FireEye argue that this is evident in the attacks that appear to have been directed by a number of countries, including the United States, Russia, and China.

## United States

Several leaders from Europe have foresworn the use of cyber attacks, but the United States government appears to have sponsored several of the most sophisticated cyber attacks. This includes Stuxnet, Duqu, Flame, Gauss, and perhaps Regin. Stuxnet, for example, is a malware program designed to disrupt Iran's nuclear enrichment program. The attack was narrowly focused on a few critical computers, and concealed within apparently legitimate operational data. The program included many innovative elements that had never been used before (zero-day exploits) and significantly raised the bar in terms of understanding what is possible to achieve in a cyber attack. Ultimately, the malware destroyed Iran's centrifuges. Moreover, Stuxnet has unfortunately become widely available and could be used to support attacks by others, including nation-states and perhaps terrorists. The experts at FireEye believe that attacks directed by the United States would showcase cutting-edge programming and creativity, require a high level of financial investment, and have significant legal oversight.

## Russia

Many Russian criminals use the Internet, but the extent of state-sponsored attacks by Russia is unclear. Computer experts in Russia are known for their technical skills, capacity for innovation, and ability to remain undetected. The government appears to have used cyber attacks to shut down Chechen protests. FireEye and others believe that Russia participated in the infamous denial-of-service attack on Estonia, although the Government of Russia denies any involvement. FireEye believes that the Red October campaign, spying on millions of Russians, may have involved the government monitoring its own people. And Russia is thought to be creating chaos in government information systems in Ukraine. Nevertheless, experts at FireEye are surprised that Russia has not been implicated in more cyber attacks to steal military secrets or disrupt foreign economies.

## China

The Chinese have been implicated in hundreds of cyber attacks on a broad range of targets around the world. This includes hacking financial institutions, absconding with military technology, stealing manufacturing and communication trade secrets, and gaining control over critical infrastructure. Chinese attacks often emphasize quantity over quality, often using brute force attacks in contrast to the more elegant and innovative attacks of the United States and Russia. FireEye reports

[42] Geers et al., "World War C."

that the vast majority of the state-sponsored cyber incidents appear to involve China, and these attacks are expected to increase. Chinese malware is often not the most advanced or creative, but it has been effective due to the volume of attacks and seeming indifference to being caught.

## IN SUMMARY

*The number of potential cyber attackers is growing each year, and they are becoming more skilled. Attackers include casual hackers, insiders, professional cyber criminals, and state-sponsored organizations. One of the challenges for Canada's insurance industry and others in defending against cyber attacks involves identification of the perpetrator. Attribution of cyber attacks is notoriously difficult.*

- *Casual hackers, insiders, cyber criminals, and state-sponsored attackers typically design their attacks to allow deniability.*
- *Attacks may operate through a network of remotely controlled computers, helping to hide the location where the attack is initiated and controlled.*
- *Criminal organizations can be hired to conduct an attack, masking the identity of the perpetrator behind the attack.*
- *Some cyber criminals use false flag attacks designed to mislead forensic investigators by including clues implicating someone that is not part of the attack.*[43]

[43] Geers et al., "World War C."

# What are the losses experienced in cyberspace?

### Costs for Businesses

- Estimated cost of cyber crime globally: $375 to $575 billion
- Estimated cost of cyber crime in Canada: $3 to $4 billion
- Additional costs that are hard to quantify: damage to company reputation, erosion of consumer confidence, immediate and future lost sales as well as subsequent and necessary sercurity enhancements

Canadians are among the world's leaders in embracing the Internet and reaping its benefits. At the same time, Canadians have not been as enthusiastic in understanding the vulnerabilities of cyberspace and implementing secure operating procedures. This combination leaves individuals and businesses in Canada, including the insurance industry, vulnerable to attack due to the relative absence of security in the present system.

Each year, more businesses and individuals in Canada experience losses through cyber crime. This includes the insurance industry. Cyber experts predict that the losses will grow. They expect that there will be an escalation in the frequency and severity of loss events. Experts warn of the potential for catastrophic cyber events resulting in widespread and prolonged disruption and losses.[44]

## The costs for businesses

Evidence of damage is clear following a vehicle collision or residential fire. The damage from a cyber crime, however, can be difficult to see and measure. It takes time before businesses learn that they are victims of a cyber crime. When an incident is detected, most companies do not report the losses, unless required by law. Moreover, it is difficult to put a value on the loss experienced. Nevertheless, Intel's McAfee and the Center for Strategic and International Studies estimate the global cost of cyber crime in 2013 was between $375 billion and $575 billion.[45]

The global impact of cyber crime is similar to estimates by the United Nations of the international production, trafficking, and sales of illicit drugs ($400 billion)[46] and the worldwide damage resulting from vehicle collisions ($518 billion).[47] Cyber losses are significant and warrant increasing attention from businesses, individuals, and policy makers. But cyber losses do not yet appear to be a large enough threat to result in a major counter-offensive.

Cyber Crimes Rates
(precent of GDP)

| | |
|---|---|
| Japan | 0.02% |
| United Kingdom | 0.16% |
| Canada | 0.17% |
| EU | 0.41% |
| China | 0.63% |
| United States | 0.64% |

Source: McAfee

McAfee and the Center for Strategic and International Studies estimate that cyber crime rates in Canada are well below the international average. Estimated cyber losses in Canada are $3 billion to $4 billion a year or 0.2 percent of the Gross Domestic Product, while the global rate is four times higher, at 0.8 percent.[48] The estimated cost of cyber crime in Canada is much lower than that in the United States, Germany, and China; similar to the United Kingdom; and much higher than that in Japan. International variation in losses appears primarily to reflect differences in the frequency and severity of attacks, rather than differences in defensive capacity.

[44] Deibert, "Distributed Security as Cyber Strategy," p. 23.

[45] McAfee and Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, p. 2.

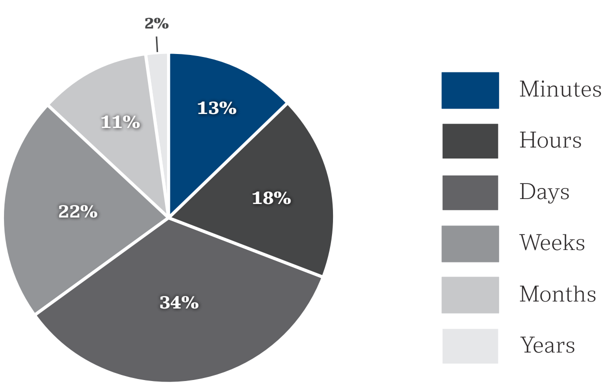
[46] Leduc and Lee, *Illegal Drugs and Drug Trafficking*, p.1.

[47] Peden et al., *World Report on Road Traffic Injury Prevention*, p. 5.

[48] McAfee and Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, p. 21.

Estimates of the cost of cyber crime tend to focus on short-term direct damage. The full consequences are difficult to quantify but are greater than those included in these measurements. For example, the theft of confidential consumer information can harm the reputation of a company, erode consumer confidence, and result in lost sales. The long-term impacts are typically excluded from loss estimates, as these losses are hard to quantify. Attacks can steal intellectual property and other trade secrets, and cyber attacks have the potential to erode success in the marketplace. Service disruptions that prevent sales, result in downtime, and reduce employee productivity are costs that are difficult to measure.

Insider Attack Discovery Time



Source: Verizon

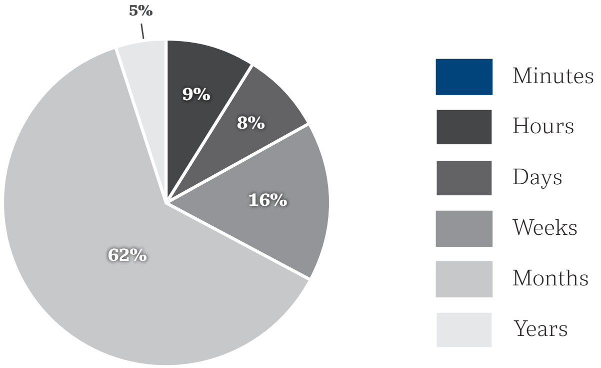
Information has become increasingly available about data breach attacks that result in the theft or loss of personal consumer information. A 2014 study by the Ponemon Institute and Hewlett-Packard Enterprise Security found that it took, on average, 170 days before a data breach was discovered.[49] If the attack involved an insider, the time was nearly twice as long. A further 45 days, on average, is required for the clean up. As a result, it typically takes seven months between the initiation of an attack and the recovery. Some data breach attacks take a year or more to resolve.

A 2014 Ponemon Institute study sponsored by IBM found that for the companies that experienced a data breach the average cost per record stolen or lost in 2013 was $145.[50] The cost was highest in the health sector ($359). Financial sector costs were also above average ($206). Costs in the retail sector were much lower ($104).

In 2007, TJX announced that personal consumer information for more than 45 million credit and debit cards holders had been compromised. Early estimates suggested that the breach might cost the company more than $1 billion, including one estimate of $4.5 billion.[51] In 2014, 25 class action lawsuits were settled and the retailer ultimately paid out $177 million dollars.[52] This case demonstrates the significant challenges associated with assessing the financial impact of a cyber attack.

Sony suffered a breach of its PlayStation network in 2011. This resulted in the possible exposure of the personal data for all of its customers. Sony announced costs of ¥14 billion ($170 million).[53] The PlayStation network was shut down for almost one month. The Information

Cyber Espionage Discovery Time



Source: Verizon

[49] Ponemon Institute, *2014 Global Report on the Cost of Cyber Crime*.
[50] Ponemon Institute, *2014 Cost of Data Breach Study*, p. 8.
[51] Dignan, "The TJX Data Breach: Why Loss Estimates Are Overblown."
[52] Hartwig and Wilkinson, *Cyber Risks: The Growing Threat*, p. 17.
[53] Tassi, "Sony Pegs PSN Attack Costs at $170 Million."

Commissioner's Office in the United Kingdom fined Sony £250,000 ($400,000) for exposing the personal data of about 100 million accounts.[54] The Deputy Commissioner David Smith criticized Sony's cyber security practices including the comment, "The security measures in place were simply not good enough."

In 2013, Target experienced a data breach involving information for more than 100 million customers, including 40 million credit cards. Target is facing more than 70 class action lawsuits.[55] The company estimates that the breach may cost $148 million,[56] some of which will be recovered from a $100 million cyber insurance policy. Costs included reimbursement to financial institutions for issuing new credit cards, retrofitting their security systems, and reduced sales. The CEO and CIO both are no longer with Target, at least in part due to the incident. The impact on the reputation of Target is hard to quantify, but may be material and sustained.

JPMorgan Chase Bank had the records of 76 million customers compromised in 2013.[57] The bank previously made significant investments in information security; nevertheless, many of its servers were accessed. The bank replaced much of its information technology infrastructure after the attack, a process that took several months. As a result of the attack, JPMorgan Chase Bank made a public commitment to a significant and ongoing investment in cyber security.[58]

Home Depot experienced a breach in 2014 that compromised 56 million credit cards and stole 53 million email addresses.[59] The hackers initially accessed the company network in April 2014 with the username and password of a third-party vendor. Between April and September, the attackers were able to access credit card information from customers shopping at Home Depot stores in the United States and Canada. The company reported $27 million in related expenses in 2014. Further expenses in 2015 will result from at least 44 lawsuits. Home Depot has $100 million in cyber insurance coverage, with a $7.5 million deductible.

Sony was hit again in late 2014 through its film division. The group responsible threatened to release data and secrets. Sony refused to meet the ransom demands and the hackers released confidential internal communications and four films. At the time of writing this report the situation at Sony is still not resolved, and costs continue to mount. The Sony attack is likely the most costly cyber breach incident to date.

## Corporate espionage

While considerable information is available about major data breaches, there is much less information about the frequency and cost of attacks that seek to steal corporate trade secrets and other confidential company information. Companies generally choose not to release this kind of information, increasing the challenge of estimating the frequency, severity, and consequences of these attacks. Some cyber espionage victims are government agencies. The insurance industry is likely more interested in the risk of corporate espionage in terms of the potential to provide coverage than in the risk that trade secrets owned by an insurance company would be stolen. In part this reflects extensive regulation of automobile insurance.

### National Research Council

In the summer of 2014, the Government of Canada's National Research Council (NRC) was forced to shut down its computer network to stop hackers from stealing sensitive information from the Council and its industrial

[54] Toor, "UK Regulators Fine Sony for 'Preventable' 2011 PSN Hack."
[55] Hartwig and Wilkinson, *Cyber Risks: The Growing Threat*, p. 16.
[56] Kedmey, "Target Expects $148 Million Loss from Data Breach."
[57] Santus, "What You Need to Know About the JPMorgan Chase Cyberattack," p. 2.
[58] Snyder, "Wall Street Admits That a Cyberattack Could Crash Our Banking System at Any Time."
[59] Associated Press, "Home Depot Faces Dozens of Lawsuits after Massive Security Breach."

partners.[60] NRC is the mechanism the federal government uses to partner with private companies to support industrial research.

The attack began with spear-phishing emails targeting NRC employees.[61] The email included malicious links disguised as safe information. Users who opened the attachments triggered malware that was downloaded using a vulnerable version of Internet Explorer. The malware allowed the hackers to steal usernames and passwords to the corporate network. The criminals then sought to steal intellectual property, trade secrets, and other sensitive information. It remains unclear what was done with the information stolen from the National Research Council.

### Nortel

For the majority of 114 years, between 1895 and 2009, Nortel was the largest and most successful technology company in Canada. In 2004, it was discovered that malicious hackers had gained almost complete access to the company's communications systems. The attack likely began in 2000 and was still operating ten years later when Nortel declared bankruptcy in 2009. Hackers working from Chinese addresses were using passwords from Nortel executives, including a former CEO, to access emails, research, and business plans. Brian Shields, who led the internal Nortel investigation of the breach, believes that attacks by criminals working for China's Huawei Technologies accessed the CEO's files and ultimately contributed to the insolvency of Nortel.[62] Today, Bell Canada and many other former Nortel customers purchase telecommunications equipment from Huawei Technologies.

## IN SUMMARY

*While cyber attacks are less visible than other losses, they are significant. International estimates of the cost of cyber crime are similar in size to the illegal drug industry and the damage from vehicle collisions. Losses in Canada are lower than in many other countries, but are a serious and growing threat. These include insurable risks, such as identity theft and data breach attacks on banks and retail companies. The majority of cyber losses, however, are not presently insurable, including cyber espionage. The strong dependency of Canadians and Canadian businesses on the Internet increases Canada's vulnerability to future cyber attacks.*

[60] CTV News, "Chinese Cyberattack Forces Computer Shutdown at National Research Council."

[61] Bronskill, "Chinese Hackers Attacked National Research Council Computers."

[62] Berkow, "Nortel Hacked to Pieces," pp. 1 – 2.

## Why are severe disruptions expected to increase?

### The major risk of loss

- Theft of intellectual property
- Theft of funds
- Theft of confidential information
- Opportunity cost

Cyberspace has proven to be surprisingly resilient to disruptions. The losses experienced have been large, but are less significant than expected. Over the past 25 years, experts predicted a major increase in the frequency and severity of disruptions. Fortunately this did not occur. Nevertheless, predictions of increased difficulties in cyberspace remain. In recent years, a consensus has emerged that cyberspace will become less open, less resilient, and less valuable than the current system.[63]

Terms like digital disintegration, cyber hurricane, and cybergeddon have emerged to describe the prospect of extensive, widespread, and persistent problems. The descriptions of potentially catastrophic cyber incidents are frequently compared with hurricanes, earthquakes, and other natural hazards that are having a significant impact on the insurance industry. Some technology experts predict that the current system is doomed to collapse. They are encouraging efforts to build new support systems for international commerce and communications to replace the current ones. At a minimum, the experts anticipate reduced public confidence and trust in the Internet over the next five to ten years as a place for secure communications and commerce.

*Organizations under attack may experience a very difficult week or two, but they generally have been able to execute continuity plans, rebuild information systems, and get back to business. The system has been resilient, but it is not secure.*

The threat of harm appears to be building faster than the capacity to prevent and mitigate catastrophic cyber incidents.

There have been disruptions in the past. Some were widespread and affected many connected to the global system (like the Morris Worm). These occurred several years ago, did not last long, and did not have major consequences. Most recent disruptions have been relatively narrow, sometimes inflicting serious losses on those affected (like Nortel), but affecting a relatively small portion of the user community. Organizations under attack may experience a very difficult week or two, but they generally have been able to execute continuity plans, rebuild information systems, and get back to business. The system has been resilient, but it is not secure.

Widespread, prolonged disruptions in global communications and commercial networks have not occurred. However, cyber experts believe that these attacks will come in the next five to ten years.[64] Many anticipate that the first cyber crisis

[63] Deibert, "Distributed Security as Cyber Strategy," p. 23.
[64] Zurich Insurance and Atlantic Council, "Beyond Data Breaches," p. 3.

will involve an attack on the critical infrastructure of a major economy, such as shutting down the power grid in the United States. A prolonged attack could have global consequences. Several countries, a few criminal organizations, and perhaps some terrorist groups have the ability to mount a major, sustained attack. The threat of harm appears to be building faster than the capacity to prevent and mitigate catastrophic cyber incidents.

An issue of growing concern involves systemic threats in cyberspace. Cyber attacks with catastrophic consequences were inconceivable to most people a few years ago, but are now seen as inevitable by a growing number of experts.[65] Concepts like interdependence and cascading events have recently entered into the discussions about cyber security. While the Internet has been resilient over the past 25 years, there is a growing sense that the system supporting global communications and commerce is vulnerable.

Several elements have been identified warning that the resilience of cyberspace is gradually being undermined, increasing the vulnerability of the Internet and the communications and commerce that it supports:[66]

- In cyberspace it is easier to attack than defend. The defender must protect all vulnerable points, while the attacker needs to find one way through the defences.
- Defenders often underestimate the risk of loss. Attackers are learning that the profits from cyber crime are high and rising, and there is little risk of being caught.
- Many of the tools required to build an attack on global networks are readily available. The key elements can be downloaded from the Internet and tailored to support a specific attack.
- There continues to be rapid growth in the number of individuals capable of launching an attack. This includes people, organizations, and countries with the necessary equipment and knowledge.
- The potential rewards from cyber crime continue to grow rapidly, while there is relatively little cost in terms of people and equipment required to mount an attack.
- Growth in the Internet of things means that billions of devices are being connected online. There are more entry points to the system and more parts of life that are vulnerable to disruption.
- The interconnectedness and complexity of cyberspace increases the difficulty of identifying attackers and holding them responsible.
- Cyber warfare is an emerging risk to the critical infrastructure that is essential to support society. This includes the threat of attack by foreign governments or terrorists.

Cyberspace is increasingly vulnerable to a catastrophic attack that may undermine the gains made over the last 25 years and block the advancements expected over the next five to ten years. A foundation for the success of the Internet has been trust. Unfortunately, gains built on trust can unwind and be lost quickly when that trust is threatened. Individual participants, like insurance companies, are actively working to protect the trust that they have built with their customers and other stakeholders, but it is unclear who, if anyone, is working to preserve public trust in the Internet as a whole, or how this can be accomplished.

> *A foundation for the success of the Internet has been trust. Unfortunately, gains built on trust can unwind and be lost quickly when that trust is threatened. Individual participants, like insurance companies, are actively working to protect the trust that they have built with their customers and other stakeholders.*

[65] Rogers, "Cybersecurity Threats," pp. 2 – 4.

[66] World Economic Forum, "Global Risks 2014."

## The major risk of loss

Intel's McAfee and the Center for Strategic and International Studies estimate that the Internet generates between $2 trillion and $3 trillion in economic activity around the world each year.[67] The McAfee study found that cyber crime extracts between 15 percent and 20 percent of the value generated by the Internet. They report four major types of cyber losses – theft of intellectual property, theft of funds, theft of confidential information, and opportunity cost. Each of these aspects of the McAfee report is explored briefly below.

### Theft of intellectual property

The largest source of loss from cyber crime involves the theft of trade secrets and other intellectual property. The actions of some individuals, companies, and countries to steal intellectual knowledge is an issue that has affected society for many generations, but the importance of this problem is increasing in the digital world. The threat of cyber theft is forcing companies to redirect scarce resources to protect existing corporate knowledge.

*Canadian economic prosperity is fundamentally reliant on an open network of global communications, and there will be a cost to the quality of life if Canadians are unable to sustain the security of cyberspace.*

### Theft of funds

Financial crime is the second largest source of direct losses from cyber crime. Criminals use data breach attacks on retailers and direct attacks on financial institutions to secure personal information about tens of millions of people that can be used to extract money from automatic bank machines, transfer funds between accounts, and support other methods to steal large sums of money. The theft of financial assets can be readily monetized and used to build on existing criminal activities.

### Theft of confidential information

The theft of confidential business and consumer information is the third major source of direct losses. This includes investment information, exploration findings, and sensitive negotiations data. Some experts anticipate that cyber attacks will be increasingly used for stock market manipulations through the theft of insider information, acquisition plans, and other information that could affect company stock prices. Financial manipulation is difficult to detect and can be very lucrative for criminals.

### Opportunity cost

Opportunity cost is the fourth largest consequence of cyber crime. If confidence erodes in the Internet as a trusted place for commerce and communications, companies and individuals may choose to invest less in research, adopt increasingly risk-averse behaviour, and direct more resources to cyber defence. The world may become a less dynamic and innovative place, and turn into a place driven more by fear than opportunity. There is a trade-off between risk and reward for individuals and businesses. Canadian economic prosperity is fundamentally reliant on an open network of global communications, and there will be a cost to the quality of life if Canadians are unable to sustain the security of cyberspace.

## Breach attacks are rising

Research by the Ponemon Institute commissioned by IBM found that 42 percent of data breach events involve malicious or criminal attacks.[68] Malicious attacks are the main cause of breaches. This may involve casual hackers or criminal groups. There continues to be growth around the globe in the number of disenfranchised people that become hackers. Potential hackers include individuals with little prospect for meaningful employment, strong computer literacy, and access to the basic tools needed to conduct an attack on the Internet. Hackers also include a growing number of criminals who are motivated by

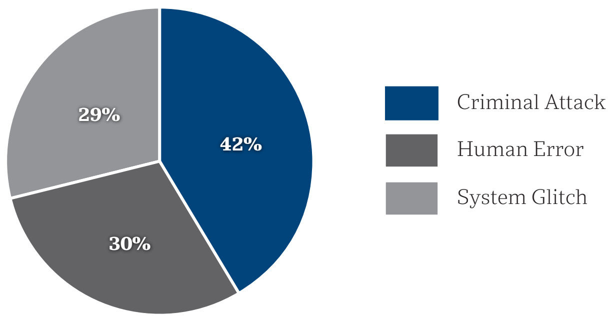
[67] McAfee and Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, p. 7.

[68] Ponemon Institute, *2014 Cost of Data Breach Study*, p. 9.

lucrative rewards and small risk of penalties. The expectation is that cyber attacks will grow in frequency and severity over the next five to ten years.

About 30 percent of data breach events in the Ponemon study involve human error. This includes negligent employees and contractors. Increasingly, staff members connect their own laptops, phones, and tablets to the workplace system, yet fail to follow proper security protocol. This offers an opening for criminals and casual hackers to access corporate information. The overall trend has been toward a growing number of devices connected to the system, increasing the risk of disruption. Efforts to establish a stronger corporate culture of security has not kept pace with actions to make it easier for employees to connect to the workplace, further increasing the risk of attacks.

Main Causes of Data Breaches



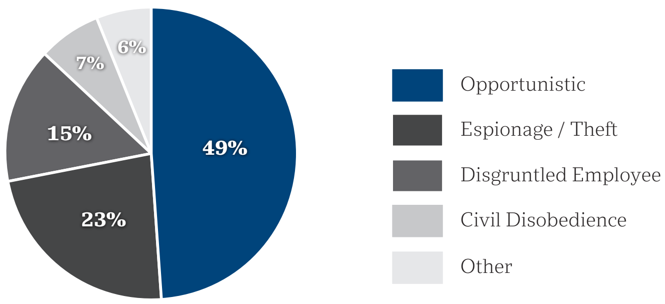
Source: Ponemon (Cost of Data Breach)

*Efforts to establish a stronger corporate culture of security has not kept pace with actions to make it easier for employees to connect to the workplace, further increasing the risk of attacks.*

The remaining 29 percent of data breach events involve system glitches. This may involve information technology or business process failures that are found to leave the system open to attack. Older, legacy systems were often not designed to provide high levels of security. Also, large organizations operate multiple systems, and some parts may be difficult to bring up to the security standards applied elsewhere in the company. Company actions to modernize information technology do not appear able to keep up with the actions of persistent attackers. For example, companies that seek to patch application and system software within 48 hours of a new security release may find it difficult to get timely patches for legacy systems.

An assessment of thousands of breach incidents by IBM found that half of the time (49 percent) the motivation of attackers is opportunistic.[69] Hackers take advantage of existing vulnerabilities without any specific motivation or objective. While these attacks are relatively easy to detect and seldom result in serious harm, they occur with great frequency so they need to be addressed. Almost one quarter of the time (23 percent), criminal attackers are seeking to steal trade secrets, financial assets, or consumer data. These organized criminal efforts can be very dangerous and often require the greatest effort to prevent. And one-sixth of the time (15 percent) the attacker is an employee who is angry with the company. Attacks by disgruntled employees are uncommon, but have the potential to do great long-term harm to the company and its reputation.

Motivation Behind Breach Attacks



Source: IBM

[69] IBM, *Security Services Cyber Security Intelligence Index*, p. 6.

## Who governs the Internet?

Many years ago, the initial connections that grew into the Internet involved trusted colleagues in academic and government research laboratories seeking to work together. Each system was distinct and developed independently. Cyberspace evolved from techniques introduced to facilitate communications and sharing of knowledge between the systems of trusted colleagues. During its formative years, the objective of cyberspace was to facilitate communications between independent systems. Security was not a priority. Protection against hostile attackers was not designed into the early systems.[70]

Over time, private corporations accelerated the development of the Internet. Presently billions of people and devices can now interact. Cyberspace may appear to be a single, global network, but in practice it is a patchwork of systems that can communicate and transfer information. Many groups are beginning to impose regulations on the Internet, both at the national and international levels, but no organization is in charge. The Internet has emerged as a public good, like fresh air and clean water, where the use by one individual does not diminish its availability and value to others. Like most public goods, however, most people assume that cyberspace will always be available, until difficulties arise.

Management of cyber security for the system, when it was considered, has been viewed as the responsibility of the individual participants.[71] Corporations are expected to protect their intellectual property and consumer information. Individuals are expected to protect their personal information. Public agencies protect the extensive information they have acquired. The accumulation of the actions of many participants was seen as the foundation for security of the system. It has been assumed that the system would be safe if each participant was serious about security. Moreover, there has been a sense that the failure to address security issues by some of the participants would present a risk for those companies and individuals, but that the system as a whole would not be at risk.

*The Internet has emerged as a public good, like fresh air and clean water, where the use by one individual does not diminish its availability and value to others. Like most public goods, however, most people assume that cyberspace will always be available, until difficulties arise.*

This approach has been largely successful over the past 25 years, a period when the Internet was less significant and less complex than it is now. Moreover, the security interests of individuals, corporations, and governments were largely converging over most of this period, and the Internet was not essential to support daily needs. Recently, however, the various stakeholders are increasingly seen as holding diverging interests that are sometimes in conflict.[72] For example, Internet providers have protected the privacy of users, but recently law enforcement officials have presented compelling arguments that this information should be accessible to prevent or resolve crimes. Is the protection of society from crime more or less important than the value of personal privacy? Conflicting objectives that were absent or trivial in the past are growing in importance as various stakeholders explore the security of the system.

*It has been argued that the current system is unmanageable given its size and complexity.*

An important risk to the system is the absence of global governance. Cyberspace has largely grown through the networking of a diverse set of services developed by private corporations. Public regulation has emerged in recent years at the national level and is expected to increase, but the system as a whole is not managed or regulated. Indeed, it has been argued that the current system is unmanageable given its size and complexity.

[70] Deibert, "Distributed Security as Cyber Strategy."

[71] World Economic Forum, "Global Risks 2014."

[72] Deibert, "Distributed Security as Cyber Strategy."

Zurich Insurance, the Atlantic Council, the World Economic Forum, and others have proposed that lessons learned from the recent global crisis in the financial sector can provide a possible solution for addressing aspects of the risk of catastrophic failure that is now present in cyberspace.[73] The self-interest of individual financial institutions reduced the risk of bank failures, but a few institutions have the potential to disrupt the entire financial system. Systemically important financial institutions are now subject to special regulatory attention. Similarly, there are a few organizations that are essential to the success of Internet. These organizations could be subject to public supervision. The goal would be to establish regulations to ensure that the system itself is not at risk, while retaining relatively little regulation for most participants as a means to encourage innovation.

## IN SUMMARY

*A future where hackers, organized crime, or state-sponsored attackers have an overwhelming advantage over defenders could be just one technological advance away. The expert consensus is that cyberspace will become a less secure place for communications and commerce over the next five to ten years, despite the expectation of increasing attention to build greater cyber security at the corporate and personal level, perhaps with special attention on systemically important institutions.*[74] *In particular, there is growing concern about the risk of catastrophic cyber incidents.*

[73] Zurich Insurance and Atlantic Council, "Beyond Data Breaches," and World Economic Forum, "Global Risks 2014."

[74] Deibert, "Distributed Security as Cyber Strategy."

# How can insurers improve their cyber defenses?

### Improving cyber defenses

- Assess current levels of preparedness and develop effective cyber security practices
- Determine accountability and ownership
- Evaluate vulnerabilities of current security systems on a regular basis
- Conduct a situational analysis to understand and describe the current cyber security state
- Identify, prioritize and protect essential corporate data
- Develop an incident management system including documentation and response plans
- Adopt an enterprise-wide cyber security policy

Some companies have been employing hackers for more than 40 years to test the risk of others penetrating their computer security systems. These tests typically demonstrate that contemporary security controls and practices increase the difficulty for casual hackers and cyber criminals to penetrate the defenses. Nevertheless, most systems can be breached by a serious and sustained attack. Even the best systems are vulnerable.[75] Attackers hold an advantage in cyberspace. How can insurance companies, brokers, and others in the insurance industry best defend themselves against attacks and minimize losses?

The Canadian Cyber Incident Response Centre (CCIRC) has identified four strategies that will prevent up to 85 percent of the targeted cyber attacks:[76]

- Use application whitelisting to prevent unapproved programs from running
- Update application software with the most recent security releases
- Update operating system software with the most recent security releases
- Reduce the number of users with administrative privileges

These are technical elements of cyber security strategy. Most importantly, insurers must establish a company-wide commitment to information security, including a better cyber risk awareness throughout the organization.[77]

For most individual users, improvements, such as using strong passwords, regularly changing passwords for each device, and prompt updating of software, may address up to 80 percent of the risk of compromises due to cyber attacks.[78]

For most individual users, improvements, such as using strong passwords, regularly changing passwords for each device, and prompt updating of software, may address up to 80 percent of the risk of compromises due to cyber attacks.

To better defend against attack, businesses and individuals need to focus on understanding how human behaviour can affect the risk of loss from cyber attacks. In the past, attacks focused on system flaws and technological weaknesses. Presently, criminals focus on tricking victims into giving access or sharing sensitive information. Security will be enhanced if everyone pauses to think before responding to requests for personal information.

Corporate risk managers have moved away from focusing primarily on preventing cyber incidents and toward minimizing the risk of loss. The PricewaterhouseCoopers (PwC) 2015 report *Managing cyber risks in an*

[75] World Economic Forum, "Global Risks 2014," p. 39.
[76] Public Safety Canada, "Top 4 Strategies to Mitigate Targeted Cyber Intrusions."
[77] U.S. Department of Homeland Security, *Cyber Risk Culture Roundtable Readout Report*.
[78] Zurich Insurance and the Atlantic Council, "Beyond Data Breaches."

*interconnected world* assesses the responses from a survey of 9,700 international business leaders. PwC include the finding that "today's interconnected business ecosystem requires a shift from security that focuses on prevention and controls to a risk-based approach that prioritizes an organization's most valuable assets and its most relevant threats."[79]

Attacks have become, and will remain, so commonplace that the objective should be to manage regular attacks to minimize the consequences, rather than seek to achieve the unattainable goal of eliminating the risk of attack. Security practices must at least match, if not exceed, those of a company's peers to ensure that the company does not become a target of choice.

> *The four actions that should be taken by an organization that is "early in the transformation process" toward more aggressive and proactive management of cyber security. First, put a senior executive in charge. Second, map threats to the business assets that really matter. Third, launch priority projects for early wins. And fourth, accelerate behaviour through incentives and experience-based awareness.*

Cyber security is not a one-size-fits-all approach. Organizations have unique risks and different tolerances for loss. To address the specific circumstances of each organization, security practices will and should differ between organizations and over time. There is no agreement about cyber best practices that should be applied in all situations.

*Changing the Game on Cyber Risk*, a 2014 report by Deloitte, sets out the four actions that should be taken by an organization that is "early in the transformation process" toward more aggressive and proactive management of cyber security. First, put a senior executive in charge. Second, map threats to the business assets that really matter. Third, launch priority projects for early wins. And fourth, accelerate behaviour through incentives and experience-based awareness.[80]

There are several initiatives that provide useful direction for the management and governance of cyber risk. Among them are the guidance issued in 2013 by the Office of the Superintendent of Financial Institutions (OSFI)[81] and the 2014 *Framework for Improving Critical Infrastructure Cybersecurity* issued by the National Institute of Standards and Technology in the United States.[82] These are explored below.

## A brief history of cyber security

The protection of consumer and company information is a long-standing issue for insurers, both pre-Internet and now. Procedures once included maintaining hard copies and secondary disk copies of all data, restricting access to sensitive materials, and generally keeping computers clean to ensure smooth running and prevent inadvertent loss of information.

For many years, information technology professionals managed the detection, response, and threat of cyber attacks. Technology experts managed the threat that technology might disrupt corporate activity. The threat has evolved from casual hackers sending infectious worms and viruses to cyber criminals seeking to steal or destroy personal data and corporate information. The emerging threats were security attacks using technology, such as spear phishing and watering holes, in addition to the earlier technology attacks using worms and viruses. Many companies developed an approach that combined the expertise of security specialists and information technology experts.

The introduction of enterprise risk management has been an important recent development to better integrate cyber security into the mainstream of corporate management and governance. Most banks and insurance companies now use enterprise risk management, but studies suggest that perhaps 90 percent of the non-financial companies in North America do not use enterprise risk management, including most small and mid-sized companies.

[79] PricewaterhouseCoopers, *Managing Cyber Risks in an Interconnected World*, p. 31.

[80] Deloitte, *Changing the Game on Cyber Risk*, p. 6.

[81] Office of the Superintendent of Financial Institutions, "Cyber Security Self-Assessment Guidance."

[82] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*.

With enterprise risk management, technology and security professionals no longer manage cyber risk in isolation. Cyber risks are assessed in relation to the other risks facing the company. This integration supports a better evaluation of the resources that should be devoted to detecting and mitigating the consequences of attacks. The governance of corporate risk management can be used to bring cyber issues to senior management and the board of directors in a consistent and timely manner. Risk management also encourages strategies for managing the peril, rather than reacting to attacks.

*With enterprise risk management, technology and security professionals no longer manage cyber risk in isolation. Cyber risks are assessed in relation to the other risks facing the company. This integration supports a better evaluation of the resources that should be devoted to detecting and mitigating the consequences of attacks.*

The 2014 cyber security framework published in the United States by the National Institute of Standards and Technology provides a risk management framework for organizations to do the following:

- Understand and describe their current cyber security state
- Determine their target state for cyber security
- Identify and prioritize opportunities for improvement
- Assess progress toward the target state
- Communicate among stakeholders about cyber security[83]

This voluntary framework is designed to enable organizations to apply risk management best practices to improve the security and resilience of critical infrastructure. The framework was designed to be applied regardless of the size, degree of risk, or extent of technical sophistication of the organization. Moreover, the framework is a living document that will evolve over time.

## OSFI Guidance for assessing cyber security

In October 2013, the Office of the Superintendent of Financial Institutions (OSFI) issued the *Cyber Security Self-Assessment Guidance*.[84] This template was designed to help banks, insurers, and other financial institutions to assess their current level of preparedness and develop effective cyber security practices. The voluntary OSFI Guidance includes 89 questions about the state of cyber security for banks, insurers, and other financial institutions. These questions are organized into six groups that are explored below:

- Organization and resources
- Cyber risk and control assessment
- Situational awareness
- Threat and vulnerability risk management
- Cyber security incident management
- Cyber security governance

[83] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*.

[84] Office of the Superintendent of Financial Institutions, "Cyber Security Self-Assessment Guidance."

## Organization and resources

OSFI's Guidance begins with an assessment of accountability and ownership. The company should have a cyber security framework. The framework should set out who is accountable for maintaining and implementing the plan. The company should set out the financial and human resources, and authority to do this work. In particular, there should be a group responsible for threat detection, management, and response. The group members should have sufficient skills and access to training. Security training and awareness training should be provided to all staff, both new and existing.

OSFI's Guidance sets out basic questions to assess the company's capacity to address cyber risks. The questions apply to any insurance company regardless of the specific circumstances – large or small, Canadian or branch, regional or national, broker or direct. The company needs to have a plan and the people to implement the plan.

A number of studies show that the frequency of attacks and the severity of losses are reduced for companies that demonstrate a healthy risk culture with respect to cyber security.[85] OSFI's Guidance sets out the issues that should be addressed to establish a healthy risk culture, and allows for variation in practices between institutions, based on the risk of loss.

## Cyber risk and control assessment

The cyber security system needs to be regularly evaluated, seeking to identify and address potential vulnerability both within the company and from outside. The evaluation should include the use of third parties to assess the risk of attack, review risks from outsourcing, and evaluate the vulnerability of critical information technology service providers. Some practices should include regular penetration tests to identify security control gaps in the network infrastructure, testing with third-party mitigation service providers, and attack simulations.

*Since 2008 the Cyber Incident Response Centre has published 40 to 90 advisories each year and issued one to eight alerts.*

Within the company there is the potential for human error, vulnerabilities in legacy systems, and lax security behaviour by employees. Poor behaviour would include carelessness, perhaps by new employees unaware of security expectations, and the risk of sabotage by disgruntled employees. Outside the company, contractors, service providers, and outsourcers all have access to company data. It is important to evaluate the company's vulnerability to internal and external threats on a regular basis. In addition, regular testing of software and other processes is important to effectively manage the risk of loss.

## Situational awareness

It is essential to understand the cyber risks facing the insurance industry and the circumstances of the insurance company. This can begin with a comprehensive inventory of the software and hardware used by the company, network maps, and performance data. The company may maintain a history of security events, including severe and minor events. The history should also include near misses where some information is available about an attack, even if a loss did not occur. Larger events should include a detailed evaluation, perhaps with a third-party expert analysis of lessons learned. Insurers should monitor public warnings and industry research on cyber security. For example, since 2008 the Cyber Incident Response Centre has published 40 to 90 advisories each year and issued one to eight alerts.

## Threat and vulnerability risk management

When considering the nature of cyber attack risk and theft of data, it might be useful to think back to pre-Internet days, when protecting a company's corporate information was a matter of placing sensitive papers in locked cabinets and instituting strict rules as to who had access to the data and under what circumstances. Today, the nature of the safes and

[85] U.S. Department of Homeland Security, *Cybersecurity Insurance Workshop Readout Report*, p. 32.

locked cabinets has shifted to cyberspace. Protecting essential corporate data remains a priority and will determine the consequences for the company when a theft is attempted. Modern information security programs define categories of sensitivity and provide the greatest protection to the "crown jewels" – that is, information with the greatest risk of causing significant harm if stolen or destroyed.

OSFI's Guidance on threat and vulnerability risk management includes 30 detailed questions on the current industry best practices. The major issues include data loss detection and prevention, cyber incident detection and mitigation, software security, network infrastructure, security configuration and management, network access control, outsourcing, and communications with customers.

## Cyber security incident management

The consequences of an attack can be significantly mitigated through a rapid and effective response to an incident. The company should have a documented incident response plan. Appropriate authorities should be designated to ensure appropriate command over the response. This may include delegated expenditure authority for minor and severe attacks, and established criteria for escalation. Procedures should be documented to monitor, analyze, and respond to attacks. There should be an approved communications plan for key internal stakeholders, including senior management, risk managers, and the board of directors. There should also be a plan for informing key external stakeholders, such as consumers, regulators, the media, and critical service providers.

A comprehensive incident management system needs to be implemented quickly to be effective, but it also must be sustained over a lengthy period of time. With many significant data breach events, the company may need months to recover from an attack. Simulations can be powerful tools to test and evaluate the system. The incident management plan should also include a post-event evaluation process of lessons learned in order to improve the company's capacity to address future incidents.

*With many significant data breach events, the company may need months to recover from an attack. Simulations can be powerful tools to test and evaluate the system.*

## Cyber security governance

The final section of OSFI's Guidance stresses the importance of governance in the effective management of cyber security. It includes more than two dozen questions probing to ensure that the insurer has an enterprise-wide cyber security policy. The company needs to ensure that the cyber security policy is consistent with policies dealing with information security, business continuity, outsourcing, and the company's overall risk appetite. Appropriate management and board oversight is needed to support implementation of the cyber security policy. Ideally, the insurer's cyber security policy should be benchmarked against that of its peers.

## IN SUMMARY

***OSFI's Guidance provides a framework for insurance companies in Canada to assess their preparedness for cyber attacks and to identify any gaps that should be addressed in their cyber security policy. The Guidance covers six elements that should be considered in a comprehensive cyber security policy. Each insurer has unique needs and requirements when it comes to cyber security, and OSFI's Guidance provides a flexible yet comprehensive framework for this important work.***

# Why is the cyber insurance market now growing?

### Current coverage available

- Cyber breach
- Identity theft

### Barriers to expanding coverage

- Determining calculable losses
- Determining accumulated risk from catastrophic incidents

Complete protection from cyber attacks is unachievable. Cyber insurance can provide financial protection against some residual risks. Similar to other perils, companies and individuals work to mitigate the likelihood and consequences of attacks, and then consider paying a premium to transfer part of the remaining risk to an insurer. Policyholders expect insurance practices that reward sound risk mitigation with lower prices and better coverage terms. Consumers also expect that insurance will be available to cover most of the residual threat of loss from a broad range of cyber attacks.

Over the next five to ten years, cyber insurance will likely become a standard purchase for most businesses concerned about data breaches.[86] Insurance will also be important to help individuals manage the threat of identity theft. However, the market for cyber insurance is very small in relation to the extent of cyber crime. Cyber insurance premiums presently are less than one-half of one percent of the estimated $375 billion to $575 billion in annual cyber crime losses. In contrast, global vehicle and fire insurance premiums are greater than annual damage from collisions and fire. Most cyber risks are uninsured or presently uninsurable. The role of insurance to help society manage cyber security is not comparable to that for perils like vehicle collisions, fire losses, and theft.

Many companies would like to purchase insurance coverage against cyber attacks that seek to steal corporate secrets, but this is not insurable because of the absence of information about the frequency, severity, and consequences of losses. The insurance industry in the United States, in partnership with government, has begun exploring the idea of insuring against the risk of a catastrophic cyber attack, but this coverage is presently not available due to lack of information about attacks and concern about accumulation risk.[87]

## A brief history of cyber insurance

Cyber insurance has been available since the late 1970s. The first insurer offered information and communications technology coverage.[88] In the 1980s, coverage expanded to include cyber security insurance marketed primarily to banks and other blue chip corporations. In the 1990s, the cyber insurance market grew from one insurance company to a few insurers. This was a very small, specialized market during this formative period.

Breach coverage is the cyber success story of the insurance industry over the past ten years.

The market changed in the late 1990s due to concerns about Y2K, and in the early 2000s with the 9/11 attacks. These events increased awareness across the business community about cyber vulnerabilities and the limited protection provided by traditional insurance coverage. Despite growing interest, virtually all of the corporate expenditures for cyber security over this period were

[86] Hartwig and Wilkinson, *Cyber Risks: The Growing Threat*, p. 21.
[87] U.S. Department of Homeland Security, various reports.
[88] U.S. Department of Homeland Security, *Cybersecurity Insurance Workshop Readout Report*, pp. 8 – 10.

invested in loss mitigation and avoidance, not insurance. The cyber insurance market remained small, and did not meet the expectations of consumers and the industry.

*63 percent of corporate decision makers were concerned about the risk of security breach of customer or employee data, and 97 percent were directing similar or increasing resources to defend against attacks, but only 36 percent chose to purchase cyber insurance.*

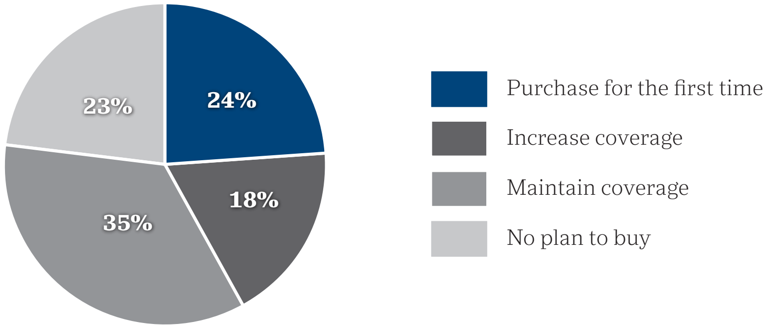
Insurance companies responded to Y2K, 9/11, and emerging information about the likelihood and potential severity of losses. Caps and limits on coverage were introduced to control the risk of accumulation, and insurance companies began to revise wordings to exclude the risk of many losses from cyber attacks from most general coverages. For example, the Insurance Services Office's standard wording for a commercial general liability policy now excludes cyber risk. Considerable effort in the insurance industry was directed to the management of cyber issues during this period, but this did not result in any meaningful expansion of the cyber insurance market, or to the development of coverages that appealed to corporate consumers. In 2002, the global cyber insurance market generated $150 million to $300 million dollars in annual revenues.[89]

The current cyber insurance products have largely emerged over the past decade. The market is now growing quickly from a small base. A 2012 survey by Chubb found that 63 percent of corporate decision makers were concerned about the risk of security breach of customer or employee data, and 97 percent were directing similar or increasing resources to defend against attacks, but only 36 percent chose to purchase cyber insurance.[90]

A 2014 survey by Partner Re found that the cyber insurance market grew five-fold between 2006 and 2013, an average annual rate of growth of almost 30 percent.[91] The survey found that more than 90 percent of brokers and underwriters expect that demand for cyber insurance will increase somewhat or increase significantly. The major drivers for increased demand are news of cyber related losses, increased awareness of the threat, and a requirement for coverage by a third party.[92]

A 2014 survey of 100 risk managers by Munich Re found that 82 percent of corporations were able to find cyber insurance coverage that met their needs.[93] Of the risk managers responding to the survey, 23 percent do not plan to purchase cyber insurance, 35 percent will maintain their current coverage, 18 percent plan to increase their cyber insurance coverage, and 24 percent plan to purchase coverage for the first time. This is a strong foundation for sustained growth of the cyber insurance market.

Cyber Insurance Plans



Source: Munich Re Cyber Risk Survey

Using reports from a variety of sources, it appears that global sales of cyber insurance premiums were near $0.2 billion in 2002. Over the past decade, the market grew at an average annual rate of about 20 percent to reach $1.5 billion in 2013. If this market sustains growth of 15 to 20 percent a year, then global cyber insurance premiums will reach $3.5 billion to $4.5 billion by 2020, and $7.0 billion to $11.1 billion by 2025. There is significant potential for even faster growth.

[89] Kovacs, Markham, and Sweeting, "Cyber-Incident Risk in Canada and the Role of Insurance," p. 23.
[90] Chubb, "Public Companies' Perceptions of Risk," pp. 14 – 15.
[91] Partner Re, *Cyber Liability Insurance Market Trends*, pp. 2 – 4.
[92] Canadian Press, "Cyber Insurance in Demand after Recent Data Breaches," pp. 1 – 2.
[93] Munich Re, *Munich Re Cyber Risk Survey*, p. 1.

## Cyber breach coverage

Cyber insurance helped Target and Home Depot significantly lower their breach-related expenses. Breach coverage is the cyber success story of the insurance industry over the past ten years. Insurance companies active in this market are growing increasingly comfortable with estimating the likelihood, severity, and consequences of attacks seeking to steal or destroy personal information. Companies that explored but did not purchase this coverage five years ago are now finding that the current coverage better meets their needs, and the product has become more affordable.[94] Major corporations in some industries, such as banking, online retail, hotels, restaurants, and healthcare providers, are driving the expansion of the cyber breach insurance market. Simplified products are now also widely available for most small- and mid-sized companies.

There are large variations from company to company in the specific insurance coverage presently available.[95] Most cyber breach insurance covers losses associated with the following:

- Disclosure injury
- Reputational injury
- Litigation defence costs and regulatory penalties
- Privacy notification expenses and credit monitoring
- Crisis management, including forensics and public relations
- Income lost due to business interruption
- Professional negotiations and funds to pay extortion costs

Insurance does not eliminate the harm experienced by cyber victims; rather, insurance works to reimburse some of the financial losses. Insurance coverage is designed to encourage actions by policyholders to reduce their risk of loss from cyber attacks. In particular, the cost to purchase coverage is based on the specific security actions taken by policyholders, so cyber insurance encourages increased investments in protection from attacks.

## Identity theft coverage

Over the past few years, many insurance companies in Canada have begun offering identity theft coverage. This coverage may be added to home, condominium, or tenant insurance policies. Identity theft coverage has been included at no charge by some insurance companies or offered as an inexpensive endorsement.

This coverage often includes reimbursement for identity restoration expenses, professional advice, and reimbursement of lost income resulting from the time required to speak with the police and credit agencies. Policies typically include a cap on the maximum payment. There are differences in the coverage offered by insurance companies, particularly in the maximum payment, but the differences are relatively small for a coverage that is new in the market.

## Barriers to expanding insurance coverage

If the insurance industry is to expand coverage to presently uninsurable losses, insurers need to know more about the incidents that are occurring, how to value them, and how to measure the effectiveness of security strategies designed to prevent and minimize them. The insurance industry is providing coverage to help society better manage the risk of loss from data breaches and identity theft, but insurance remains largely absent in addressing most other cyber perils. Adverse selection and moral hazard are long-standing issues that increase the difficulty of providing some insurance coverages, such as overland flooding, but these are not as significant for cyber insurance. The major obstacles to the development of insurance coverage for other cyber perils involve difficulties in determining calculable loss and the accumulation risks associated with catastrophic events, as explored below.

[94] Armerding, "Cyber insurance: Worth It but Beware of the Exclusions," p. 1.

[95] Burke, "The Future of Cyber Insurance," p. 4.

## Sufficient information to determine calculable loss

A barrier to insuring a broader range of cyber risks is the determination of the calculable loss. Unlike most fire losses and vehicle collisions that are observed and recorded by public officials, similar information is not available about the vast majority of cyber incidents. Many businesses would like to purchase insurance against losses from corporate espionage. Businesses would also like to insure against the risk of losses that may occur if cyber criminals gain remote control over the operating systems of critical infrastructure. However, these perils are largely uninsurable. The vast majority of incidents of this nature are not reported. Because insurers cannot anticipate with confidence the chance of a loss, this risk cannot be transferred.

Beyond the need for information about the frequency of penetrations are concerns about severity. Due to a lack of reporting, the insurance industry does not have reliable information about the severity of cyber incidents. The theft of a laptop from an employee may reveal a few company secrets, for example, but the theft would be a less severe loss than if a disgruntled employee downloaded and shared hundreds of sensitive documents with a competitor. A hacker who gains remote control over the lighting system would be a less significant threat than an extortionist who gains control over the national power grid.

*A specific objective would be to spur the development of broadly accessible cyber risk actuarial data needed to advance the cyber security insurance market more comprehensively.*

Perhaps the greatest challenge involves quantifying the consequences of the attack. The cost of replacing a laptop is easy to estimate, but it is difficult to put a value on the stolen corporate information on the computer. The costs may eventually be revealed in terms of lost future sales, but these are difficult to determine at the time of the incident. The concept of calculable loss is essential for insurability. The risk of cyber attacks to steal intellectual property or gain remote control over operating systems is largely uninsurable at this time due to the absence of data about the frequency, severity, and value of the losses.

Some insurance companies provide cyber insurance coverage using manuscripted policies. These client-specific agreements are custom drafted to address the specific needs of a policyholder. Coverages may include otherwise uninsurable risks, because the insurance company is able to secure sufficient information from the client and to consider the risk, but similar coverage cannot be offered to other companies.

The cyber security strategy for the United States has included a provision since 2010 for the federal government to explore collecting and sharing information about the frequency and severity of cyber attacks.[96] Homeland Security held a series of meetings with insurance and risk management experts to identify and address barriers to the provision of insurance, including the idea of establishing a data repository. A specific objective would be to spur the development of broadly accessible cyber risk actuarial data needed to advance the cyber security insurance market more comprehensively. The group is exploring how to pool and share cyber incident information, on an anonymized basis, and make it accessible to insurance carriers and other risk management professionals.

A repository may also provide a benchmark for organizations to assess their current cyber risk management performance against their peers, inform cyber security best practices, and better support the assessment of risk accumulation. Much insurance work revolves around predicting future losses – specifically the likelihood of events and their associated damages. A repository of cyber incident information would build a history of loss events that can be assessed over time.

*A repository of cyber incident information would build a history of loss events that can be assessed over time.*

[96] White House, "Presidential Executive Order 13549" in 2010, "Executive Order 13636" in 2013, and the Cybersecurity Framework in 2014 are some elements of long-standing commitment to increase the volume, timeliness and quality of cyber threat information sharing as a foundation of cyber security policy in the United States.

The lack of available data about the frequency, severity, and consequences of cyber attacks is a barrier to the expansion of the cyber insurance market beyond breach attacks and identity theft. Insurance companies need to determine the calculable loss if they are to consider accepting the transfer of the residual risk from consumers, and an absence of data prevents insurers from assuming this role for many aspects of cyber risk.

*A cyber attack capable of taking down the national power grid, disrupting air and rail traffic, shutting down the water supply, bringing chaos to communications systems, or otherwise threatening critical infrastructure would create severe disruptions for society. This kind of catastrophic incident is presently uninsurable.*

### Sufficient information to determine the accumulated risk from catastrophic incidents

A second barrier involves accumulation risk. A cyber attack capable of taking down the national power grid, disrupting air and rail traffic, shutting down the water supply, bringing chaos to communications systems, or otherwise threatening critical infrastructure would create severe disruptions for society. This kind of catastrophic incident is presently uninsurable. Insurance companies do not have sufficient information to assess the likelihood and consequences of a serious attack. Moreover, while insurance may be sufficient to cover the individual risks of loss, the industry may be unable to cover the accumulation of losses across society. For a catastrophic cyber attack, it is recognized that the risk of loss is not independent, although the extent of the correlation may not be fully understood at this time.

Insurance coverage is possible for some large, correlated loss events, like a major urban earthquake, if the probable maximum loss can be estimated and managed. The key to insurability is information about the likelihood and potential consequences of a catastrophic loss event.

Insurance companies have struggled to estimate the probable effects of a cyber attack on critical infrastructure – key information needed to extend and price first-party coverage. Cyber incident models and simulations would help insurance companies understand the potential loss from attacks on critical infrastructure and determine who would be responsible for paying the cost to restore it. The components that present the greatest concern from a business interruption perspective can be tested in models, helping to identify the controls that would have the greatest mitigation effect.

*Major attacks on the power grid or the Internet itself are examples of perils with widespread implications that are poorly understood at present in terms of likelihood, consequence, and accumulation.*

A major obstacle to advance first-party cyber insurance arises from the ongoing uncertainty about how large cyber-related critical infrastructure losses may become. The industry needs a better understanding of what losses could be anticipated. Insurance companies need to know more about the potential for cascading effects to better understand risk accumulation. A tabletop exercise where public and private sector stakeholders jointly respond to a simulated major cyber attack could provide a useful starting point for cyber incident consequence analysis.

In situations where the potential loss exceeds the capacity of the insurance industry, insurers may provide coverage if the federal government is willing to provide a backstop by agreeing to act as the insurer of last resort. This may involve a situation where a very large number of policyholders are impacted by a single event. Development of an insurance market for catastrophic cyber risks may require information about the probable maximum loss, but may also require the creation of a backstop.

Insurers are confident that they have the funds to pay the losses from cyber attacks when there are few cyber victims, but the companies need to understand the potential consequences of a cyber incident that could result in claims from tens of millions or perhaps hundreds of millions of customers simultaneously. Major attacks on the power grid or the Internet itself are examples of perils with widespread implications that are poorly understood at present in terms of likelihood, consequence, and accumulation.

## IN SUMMARY

*Insurance coverage for cyber breach attacks and identity theft are recent successes of the insurance industry. Over the next five to ten years, cyber breach coverage is expected to extend to companies, large and small, across North America and Europe. The size of the cyber breach and identity theft insurance market may increase by more than five-fold over the next decade. The coverage is useful for companies and individuals and has become more affordable. Some insurance companies in Canada currently purchase cyber coverage and most are expected to explore the idea of purchasing coverage over the next five to ten years.*

*Most other cyber perils are presently uninsurable. These perils include the risk of attacks to steal corporate secrets or to gain remote control over the operations of a company. Another peril is the risk of catastrophic attacks to disrupt or destroy a society's critical infrastructure. Over time, some of these risks may become insurable. A barrier to the expansion of cyber insurance markets involves the lack of information about the likelihood, severity, and consequences of major attacks needed to determine the calculable loss. A second barrier to the expansion of cyber insurance markets involves accumulation risk associated with catastrophic attacks that must be managed to ensure that they do not overwhelm the financial capacity of insurance companies.*

*Insurance support for society's management of many other perils – vehicle collisions, fire, and theft – evolved over many decades. When a serious effort is made to collect data about the likelihood and consequences of cyber attacks, it will likely take more than a decade until sufficient information is available to support a rigorous actuarial analysis of the risks. Insurability will likely extend to a variety of cyber risks over the long term, but the primary focus of cyber insurance over the next five to ten years is expected to remain on data breach and identity theft.*

# How will evolving regulations affect cyberspace?

### Canada's cyber security strategy

- Securing government systems
- Partnering with private sector to secure other vital systems
- Helping Canadians to be safe online

Cyberspace is a complex web of private and public responsibility subject to growing attention from government regulatory agencies. Several national and international organizations are working to address cyber security, but the many actors involved are not in agreement about the objectives. The cyber security effort has been described by Ron Deibert, Director of the Canadian Centre for Global Security Studies, as one of "intense contestation."[97] Many participants have an interest in shaping the future of cyberspace to secure a strategic advantage for their organization or nation.

Some, like Lloyd's, have been encouraging the insurance industry to become active in the national and global discussions about cyberspace.[98] Others, such as the World Economic Forum, have been describing specific ideas insurers and other corporations should promote concerning international regulation of the Internet.[99] A natural role for the insurance industry would involve partnering with government agencies to promote safe cyber practices, just as the industry has been a champion for fire prevention, road safety, and crime prevention.

A natural role for the insurance industry would involve partnering with government agencies to promote safe cyber practices, just as the industry has been a champion for fire prevention, road safety, and crime prevention.

The Internet has emerged as an essential foundation supporting communications and commerce in market economies. Cyberspace also facilitates the free exchange of ideas and knowledge, a system that is critical to the support of successful democracies. In market-based democracies, Internet reform efforts focus on the introduction of legislative and enforcement protection for specific needs, like the protection of intellectual property, privacy, and the rights of children. Some countries, like the United States, speak openly about their view that cyberspace should support the expansion of market-based democratic approaches around the world, with minimal regulation.[100]

However, many countries are not market-based democracies, and they are pursuing reforms in cyberspace to advance a different agenda. Some countries seek to secure the right to monitor communications as a tool to manage dissent. State-sponsored agencies may be directed to secure intellectual knowledge that can advance the capacity of local producers. Moreover, establishing a global leadership organization for managing cyber security may be an approach that serves to diminish the overall influence of the United States and Europe in global economic affairs.

"In hindsight, it was folly to examine [financial solvency] risks one organization at a time, while ignoring the interconnections. Yet this is how cyber attacks are looked at today."

The complexity of the issues in cyberspace is much more intractable than the debate between two points of view. For example, the United States has been outspoken about the value of private sector leadership continuing for the management of cyberspace and the importance of protecting privacy and

[97] Deibert, "Distributed Security as Cyber Strategy," p. 1.
[98] Lloyd's, "Digital Risks: Views of a Changing Risk Landscape," p. 5.
[99] World Economic Forum, "Global Risks 2014."
[100] President of the United States, *International Strategy for Cyberspace*, p. 22.

intellectual property, yet they have introduced an aggressive system of monitoring communications within the context of national security. The Internet was established and initially governed by a small group of like-minded computer engineers. Today, there are many actors interested in cyberspace governance, and the stakeholders have complex and conflicting objectives.

The Internet has its roots in Europe and the United States, and its early development reflects the values of western industrial countries. However, the majority of Internet users are now located elsewhere in the world. Moreover, developing countries will continue to experience the fastest growth in the number of users. People in these countries seek to ensure that their values are reflected in emerging reforms. For example, most communication in cyberspace is in English, but Russian authorities have been providing a Cyrillic top-level domain since 2010, while Chinese authorities control the provision of Chinese language services. For better or worse, cyberspace is becoming more complex.

Beyond actions to encourage linguistic communities to express themselves online, there are less visible efforts underway to use cyberspace to impose social and political norms. For example, the OpenNet Initiative reported that more than 40 countries now engage in Internet content filtering to some extent.[101] The Initiative calculated that 47 percent of global Internet users are now subject to some degree of censorship. Certain countries are using censorship to control dissent and confront opposition. Democratic countries justify filtering as a mechanism to protect intellectual property, confront sexual exploitation of children, and tackle hate crimes.

*The difference between cyber security and information security is an important distinction that helps to explain the impasse between western nations and countries such as Russia and China. Cyber security focuses on the technical security of hardware, software, and data and its transmission.*

The difference between cyber security and information security is an important distinction that helps to explain the impasse between western nations and countries such as Russia and China. Cyber security focuses on the technical security of hardware, software, and data and its transmission. The United States, Canada, and many of the countries in Europe would like international discussions to focus exclusively on these issues. Information security includes all aspects of technical security, but also the content of the cyber data – usually for the purposes of censorship. China and many other countries would like to explore this broader set of issues.

Some in the business community, as articulated by Zurich Insurance and the Atlantic Council, propose that regulation of cyberspace should be viewed as primarily an economic issue.[102] They acknowledge the complexity and difficulty in finding solutions to the systemic risk of Internet security, nevertheless they identify solutions found in economic policy that could be adapted to address the challenges in cyberspace. These include efforts to protect property rights, promote free trade, and minimize regulation. Several of these efforts have been sustained over many decades, across many nations.

*Information security includes all aspects of technical security, but also the content of the cyber data – usually for the purposes of censorship.*

The World Economic Forum identifies the 2008 financial crisis as a learning opportunity to guide the discussion about cyber security.[103] Prior to the financial crisis, security in the international banking system was based primarily on the independent actions of many participants. Recently regulations have been introduced to address systemic risks. In particular, greater regulatory attention has focused on the extensive interconnections of systemically important institutions – those banks and insurance companies that, if they should fail, could place the global financial system at risk. Zurich and the Atlantic

[101] Deibert, "Distributed Security as Cyber Strategy," p. 7.
[102] Zurich Insurance and the Atlantic Council, "Beyond Data Breaches."
[103] World Economic Forum, "Global Risks 2014."

Council observe, “In hindsight, it was folly to examine [financial solvency] risks one organization at a time, while ignoring the interconnections. Yet this is how cyber attacks are looked at today.”[104] Increased regulatory monitoring of the major participants supporting the Internet may reduce risks to the system and preserve the benefits of minimal regulation for most participants.

Risk management is emerging as an essential tool for managing issues in the private and public sectors. In particular, there is growing emphasis on integrating the management of a range of risks rather than technical planning for narrowly defined individual risks. This includes adopting an enterprise-wide perspective in private companies. A risk management perspective is also emerging in the public sector, where actions now are frequently developed to work across departments and agencies.

Risk appetite and risk tolerance are concepts that provide risk management goals for decision-makers. Many significant risks cannot be eliminated, but they can be reduced to an acceptable level. Accordingly, risk mitigation has begun to replace risk elimination as the objective of cyber risk management.

Most importantly, the risk management approach to addressing priority issues increasingly involves establishing a culture of long-term thinking. This can be challenging for private corporations, whose financial performance is subject to judgment and external review each quarter. Long-term thinking is also difficult in the public sector, with daily judgment offered by opposition parties and the media, and a short-term electoral cycle. Long-term thinking, however, is essential in order to confront risks like cyber security.

## Canada’s cyber security strategy

The Government of Canada joined the international discussion about cyber security in 2010 with the publication *Canada’s Cyber Security Strategy for a Stronger and More Prosperous Canada*.[105] The report set out a five-year plan of action in three areas: securing government systems, partnering with the private sector to secure other vital systems, and helping Canadians to be safe online.

Shared Services Canada, the Treasury Board, Public Works and Government Services Canada, and other federal agencies are working to consolidate information and technology services for the Government of Canada. The objective is to improve defensibility through built-in redundancies, and reduce the number of network connections to the Internet.

The initial five-year plan focuses on securing information managed by the Government of Canada. The legal mandate of Communications Security Establishment Canada, however, is to “provide advice, guidance and services to help ensure the protection of electronic information and the information infrastructure of importance to the Government of Canada.” That is to say that the Government of Canada has the legislative authority to extend its cyber security efforts to deal with critical infrastructure, and 85 percent of these systems are owned by the provinces or private industry.

The strategy sets out ten sectors where the Government of Canada seeks to partner with private industry in addressing cyber security issues. Finance Canada has the lead for dealing with banking and insurance companies, one of the ten critical sectors. The Office of the Superintendent of Financial Institutions issued cyber security self-assessment guidance in 2013 to the financial institutions that it regulates, and discusses security practices during on-site supervisory visits with each institution. Communications Security Establishment Canada is responsible for the Government of Canada’s incident response co-ordination.

*The Office of the Superintendent of Financial Institutions issued cyber security self-assessment guidance in 2013 to the financial institutions that it regulates, and discusses security practices during on-site supervisory visits with each institution.*

[104] Zurich Insurance and the Atlantic Council, “Beyond Data Breaches,” p. 1.
[105] Canada, *Canada’s Cyber Security Strategy.*

Public Safety Canada has been directed to help Canadians protect themselves and their personal information online. Primarily, this involves a national awareness campaign seeking to inform and empower Canadians about cyber security.

Public Safety Canada is also managing the national strategy for critical infrastructure. This includes the National Cross-Sector Forum where public and private sector leaders from the ten identified critical infrastructure sector networks work together and exchange ideas about cyber security. Public Safety Canada also manages the Cyber Incident Response Centre to co-ordinate federal responses to cyber security incidents and protect critical infrastructure. The Royal Canadian Mounted Police (RCMP) established a Critical Infrastructure Intelligence Team to examine physical and cyber threats, including a Suspicious Incident Reporting system. The RCMP report *Cybercrime: An Overview of Incidents and Issues* provides several case studies of incidents in Canada.[106]

> *The best defence involves a robust offence based on intelligence. According to CSIS, Canada should build its capacity to identify and forestall prospective threats. Canada should strive to deny terrorists and nation-states the means to conduct attacks within Canadian borders.*

A particularly bold initiative was set out by the Canadian Security and Intelligence Service (CSIS) in its 2012 report *Assessing Cyber Threats to Canadian Infrastructure*.[107] This paper for CSIS by Gendron and Rudner proposes a proactive intelligence approach to cyber security for critical infrastructure. The objective would be to detect and forestall cyber threats. This challenges the conventional view that cyber security must always be a defensive effort, with an emphasis on technical solutions.

Moving from the view of individual and corporate actions to defend digital assets to a national perspective of defending Canada's information-based society, CSIS brings forward the idea that the best defence involves a robust offence based on intelligence. According to CSIS, Canada should build its capacity to identify and forestall prospective threats. Canada should strive to deny terrorists and nation-states the means to conduct attacks within Canadian borders. A challenge is determining the means to harness this capacity and make it available to key decision-makers in the public and private sectors.

Canada's Cyber Security Strategy was generally well received and recognized as consistent with the strategies set out by the United States, the United Kingdom, Australia, and New Zealand. The Canadian strategy moves directly to commitments to act in the three areas – securing government systems, partnering with the private sector to secure other vital systems, and helping Canadians to be safe online. However, the strategy has been criticized for failing to explore the importance of cyberspace itself. Critics maintain that the strategy does not address the importance of open communication for achieving Canada's interests as a democratic, market-based economy. The strongest criticisms have been directed at the absence of details about international dimensions of cyberspace security. The risks to cyberspace in Canada will not be resolved in isolation and will require participation in global discussions.

> *The Canadian strategy moves directly to commitments to act in the three areas – securing government systems, partnering with the private sector to secure other vital systems, and helping Canadians to be safe online.*

The insurance industry may want to explore options with the federal government for expanding the role of cyber insurance in Canada. Increased use of insurance would help Canadians mitigate the losses from cyber incidents and enhance their resilience to future attacks. Promoting cyber insurance would increase the financial incentives for businesses to invest in cyber security as a means of managing the cost of coverage. A shared interest in loss mitigation and incident prevention suggests that the insurance industry and the federal government may be natural allies in promoting cyber security, sharing the desire to apply a risk management approach to security issues.

[106] Royal Canadian Mounted Police, *Cybercrime: An Overview of Incidents and Issues*.

[107] Gendron and Rudner, *Assessing Cyber Threats to Canadian Infrastructure*, p. 43.

Insurance companies providing cyber coverage should press for the government to provide more information about the frequency, severity, and consequences of attacks. There is scope for joint exercises simulating attacks on critical infrastructure to better understand the worst-case scenarios and best practices to mitigate the potential loss. Companies may even explore the idea of providing coverage for a catastrophic cyber incident if the government is willing to commit to a financial backstop.

## Privacy legislation and breach notification

The Canadian insurance industry, through the Insurance Bureau of Canada, has been an active participant for many years in the development of privacy legislation. Alberta and federal privacy legislation requires notification to consumers if there has been a breach of personal information.[108] Work is underway toward the introduction of mandatory disclosure requirements in the Quebec and Ontario privacy legislation. Mandatory breach disclosure requirements should be an essential component of Canada's cyber security strategy. Presently, most cyber incidents are not reported, or reports are incomplete and delayed. Canadians would benefit from a clear statement of expectations to ensure that their personal information is properly secure when it is shared with third parties. If a breach does occur, Canadians deserve timely and appropriate notification.

*Mandatory breach disclosure requirements should be an essential component of Canada's cyber security strategy. Presently, most cyber incidents are not reported, or reports are incomplete and delayed.*

A 2013 survey by Phoenix Strategic Perspectives, sponsored by the Office of the Privacy Commissioner of Canada, found that 97 percent of Canadians want to be notified if their personal information is accidentally or deliberately disclosed. However, an alarming 59 percent believe that they will not be notified if a breach does occur.[109] Consumer confidence that they will be notified is low. Canadians would like assurances that they will be informed if a breach does occur.

The 2014 report by the Office of the Privacy Commissioner, *Privacy and Cyber Security*, notes that "the interconnectivity and shared risks in cyberspace puts responsibility of all stakeholders to shape cyberspace and cyber security on a foundation of enduring trust." The report also indicates that "Undertaking preventative measures to ensure security – and informing consumers about the potential risks – can foster trust in individuals using the Internet."[110]

Breach notification and disclosure requirements are important drivers in the recent expansion of the cyber insurance market in the United States. Moreover, legislation and regulations should not be the primary drivers of disclosure practices. Good corporate practice should include a commitment to communicate with consumers after a breach.

Some jurisdictions around the world, like the United Kingdom, have introduced fines and regulatory charges for corporations that fail to adequately protect personal consumer information. Insurance companies should consider sharing their views about this approach when fines and penalties are considered by federal and provincial officials in Canada, and clarify the role of cyber insurance in covering this charge.

*Good corporate practice should include a commitment to communicate with consumers after a breach.*

[108] Tyndale and Morgan, "Cyber Liability," p. 11.

[109] Phoenix Strategic Perspectives, *Survey of Canadians on Privacy-Related Issues*, p. 14.

[110] Privacy Commissioner of Canada, *Privacy and Cyber Security*, pp. 8 - 9.

## Regulation of the Internet

There is also scope for the insurance industry to participate in the broader discussion about the future of cyberspace. Some questions that could be addressed include the following:

- Can the current largely unregulated system be sustained?
- Should control of cyberspace remain primarily in the private sector, with limited public regulation to deal with exploitation of children, bullying, and privacy of personal information?
- What role should be allowed for censorship by public agencies?
- Should there be special legal provisions for addressing the threat of terrorism and hate crimes?
- What powers, tools, and resources should be given to the police to combat cyber crime?
- How should cyber crime issues be best addressed at the local, national, and international level, given the significant differences in capacity and resources?
- Should Canada establish a national plan to prevent cyber attacks through intelligence?

### IN SUMMARY

*Over many decades, the insurance industry has become a leader in the promotion of road safety, crime prevention, and fire prevention. There is scope for the industry to play a similar role in promoting safe practices in cyberspace. The goals of the criminals are largely unchanged, with a focus on theft, fraud, and extortion, but the tools are constantly evolving. The insurance industry has the potential to build important partnerships in the emerging efforts to promote cyber security. Actions to promote cyber security would be consistent with the long-term objectives and practices of the insurance industry:*

- *Partner with the federal government's Get Cyber Safe public awareness campaign*
- *Support the proposal by the Canadian Association of Chiefs of Police to develop a national cyber crime strategy with enhanced interagency capacity, operational plans, and data collection*
- *Press for greater disclosure about the frequency and consequences of cyber attacks*
- *Sponsor simulations and research to assess the impact of large-scale incidents*

# Recommendations for the insurance industry

### Cyber risks are anticipated to increase over the next five to ten years

### Contributing factors

- Continued exponential growth of the Internet of things
- More and more communications and commerce online
- Ease and capacity to launch cyber attacks on individuals, corporations, countries and the Internet itself

### Consequences

- Cyber security now third most important issue facing p&c insurance industry
- Cyber security is identified as the most underestimated risk by business leaders
- Premiums for current levels of cyber coverage completely inadequate

Canadians have embraced cyberspace as a safe place for commerce and communications. Over the next five to ten years, the finance, transportation, communications, and retail industries are some sectors that plan to introduce new products and services that are dependent on the Internet.

Experts warn, however, that cyber attacks on individuals, corporations, and the Internet itself are going to increase in frequency and severity over the next five to ten years. Cyberspace is expected to become less resilient, available, and robust than what has been experienced over the past 25 years.

## Insurers resilient to cyber attacks

Cyber security was identified as the third most important issue facing the property and casualty insurance industry today in a recent KMPG survey of Canadian industry leaders. At the same time, cyber security was identified as the most underestimated risk in a recent Allianz survey of international business leaders. Customer information must be protected from cyber criminals. The use of technology to enhance relations with consumers and company operations must be secure. Insurers must protect their corporate knowledge and systems. Cyber security is important for the Canadian insurance industry.

Even the best security system can be overwhelmed by persistent attacks. Nevertheless, there are practices to increase resilience to attacks and limit the financial and reputational consequences when an incident does occur. OSFI has provided flexible and comprehensive guidance for insurance companies and other financial institutions to strengthen their cyber security plans. These plans should include technology and behavioural elements.

Three recommendations for the insurance industry in Canada to improve resilience to cyber attacks:

- Appoint a senior executive to develop and implement a comprehensive plan to manage and reduce the long-term consequences of cyber risks.
- Identify the consumer information and the corporate knowledge that matters most, and direct the highest protection effort to shield these critical assets.
- Build a corporate culture of cyber security that includes actions to address technological threats and security training for employees.

## Insurance solutions for society

Insurance is the business of risk management. Society benefits when insurers quantify the risk of loss, incentivize investments in mitigation, model catastrophic events, promote consumer awareness, and contribute to sound government regulation. Over the past decade, the insurance industry has begun to address the risk of identity theft for individuals and data breach attacks on corporations. Insurance coverage for these perils is expected to expand over the next five to ten years.

Most cyber risks, however, are presently not covered by insurance. Over the long term, cyber insurance markets should expand beyond the risk of identity theft and data breach. Insurers need to work with governments and other stakeholders to confront the major barriers to expansion:

- Determine calculable loss by securing data about the likelihood and consequences of cyber attacks.
- Understand accumulation risk, including the threat of catastrophic attacks on critical infrastructure.

Increasingly, the Canadian insurance industry should participate in the policy discussions about cyber security. The long-standing tradition of the insurance industry to champion road safety, crime prevention, and fire prevention provides a foundation for similar participation in efforts to promote safe practices online. The insurance industry should also develop views on breach notification, cyber defense through intelligence, and other cyber security issues.

Three recommendations for the insurance industry to provide solutions for cyber risks in Canada:

- Build the market over the next five to ten years until most businesses, homeowners, and tenants consider cyber insurance for the risk of loss from data breach and identity theft.
- Work with governments and other stakeholders to establish conditions over the medium and long term to expand insurance coverage to other cyber risks in Canada.
- Work with the federal and provincial governments, law enforcement officials, and other stakeholders to champion practices to keep Canadians safe online.

Despite the efforts of the insurance industry and others to address cyber risks, external forces are likely to bring great change in cyberspace over the next five to ten years. Experts warn that cyberspace will become increasing less reliable as a foundation for commerce and communications. In Canada and around the world, the frequency and consequences of cyber attacks are expected to increase. These expectations add to the importance of investing now to prepare for the risks ahead.

*This is a critical time for the Canadian insurance industry to explore cyber security.*

# Appendix I – Bibliography

A.M. Best Company. "Fall 2014 Insurance Industry Survey." *Best's Special Report*. 8 December 2014. http://africabusiness.com/wp-content/uploads/2014/12/A.M.-Best-Fall-2014-Insurance-Industry-Survey-Insurers-wrestle-with_-cyber-cover-and-social-media-strategy-December-8-2014.pdf

Abrams, Marshall, and Joe Weiss. "Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia." The MITRE Corporation, 2008. http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

Allianz. "Allianz Risk Barometer: Top Business Risks 2015." *Allianz Risk Pulse* (2015). https://www.allianz.com/v_1421228810000/media/press/document/Allianz_Risk_Barometer_2015_Jan_2015_final.pdf

Armerding, Taylor. "Cyber Insurance: Worth It, but Beware of the Exclusions." *Tech Page One*. Dell, 24 October 2014. http://www.techpageone.co.uk/en/technology/security-it/cyber-insurance-worth-beware-exclusions/

Associated Press. "Home Depot Faces Dozens of Lawsuits after Massive Security Breach." *CBC News*, 25 November 2014. http://www.cbc.ca/m/touch/business/story/1.2849810

Berkow, Jameson. "Nortel Hacked to Pieces." *National Post Online*, 25 February 2012. http://business.financialpost.com/2012/02/25/nortel-hacked-to-pieces/?__lsa=3b87-b412

Bronskill, Jim. "Chinese Hackers Attacked National Research Council Computers." *CTV News Online*, 13 December 2014. http://www.ctvnews.ca/canada/chinese-hackers-attacked-national-research-council-computers-1.2146400

Burke, Benedict. "The Future of Cyber Insurance." Crawford & Company, 2014. http://ca.crawfordandcompany.com/media/1614470/2014-06-13-cyberinsurance.pdf

Byford, Sam. "Sony Pictures Hackers Sent Ominous Email to Executives Warning of Attack." *The Verge*, 8 December 2014. http://www.theverge.com/2014/12/8/7356575/sony-pictures-hack-extortion-email

Canada. *Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada*. Government of Canada, 2010. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

Canadian Internet Registration Authority. "The Canadian Internet." *The 2014 CIRA Factbook*, 2014. http://www.cira.ca/factbook/2014/index.html

Canadian Press. "Cyber Insurance in Demand after Recent Data Breaches." *CBC News*, 28 July 2013. http://www.cbc.ca/m/touch/news/story/1.1396187

Chien, Eric, and Gavin O'Gorman. "The Nitro Attacks: Stealing Secrets from the Chemical Industry." *Symantec Security Response*, 2011. http://securityresponse.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

Chubb. "Public Companies' Perceptions of Risk and Their Risk Mitigation Strategies." Chubb Group Insurance Companies, 2012. http://www.chubb.com/businesses/csi/chubb15930.pdf

CTV News. "Chinese Cyberattack Forces Computer Shutdown at National Research Council." *CTV News Online*, 28 July 2014. http://www.ctvnews.ca/canada/chinese-cyberattack-forces-computer-shutdown-at-national-research-council-1.1936483

Deibert, Ron. "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace." *Canadian Defense & Foreign Affairs Institute Research Paper*, August 2012. http://www.cdfai.org.previewmysite.com/PDF/Distributed%20Security%20as%20Cyber%20Strategy.pdf

Deloitte. *Changing the Game on Cyber Risk: The Imperative to Be Secure, Vigilant, and Resilient*. Deloitte Development, 2014. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-deloitte-cyber-risk-pov-secure-vigilant-resilient.pdf

Deloitte. "Global Cyber Executive Briefing: Insurance." *Deloitte Case Studies*, 2015. http://www2.deloitte.com/be/en/pages/risk/articles/insurance.html

Dignan, Larry. "The TJX Data Breach: Why Loss Estimates Are Overblown." *ZDNet*, 8 May 2007. http://www.zdnet.com/article/the-tjx-data-breach-why-loss-estimates-are-overblown/

Doherty, Stephen, Piotr Krysiuk, and Candid Wueest. *The State of Financial Trojans 2013*. Symantec, 2013. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_state_of_financial_trojans_2013.pdf

Geers, Kenneth, Darien Kindlund, Ned Moran, and Rob Rachwald. "World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks." *FireEye Labs White Paper*, 2013. http://bp.softline.kiev.ua/attachments/article/30/fireeye-wwc-report.pdf

Gendron, Angela, and Martin Rudner. *Assessing Cyber Threats to Canadian Infrastructure*. Canadian Security Intelligence Service, March 2012. http://publications.gc.ca/collections/collection_2013/scrs-csis/PS74-1-2012-eng.pdf

Go-Gulf. "Online Piracy in Numbers – Facts and Statistics." *Go-Gulf Blog*, 1 November 2011. http://www.go-gulf.com/blog/online-piracy/

Hartwig, Robert P., and Claire Wilkinson. *Cyber Risks: The Growing Threat*. Insurance Information Institute, June 2014. http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf

Harvey, Thomas J. "Battling Employee Sabotage in the Wired Workplace." *American Society of Association Executives White Paper*, 2001. http://www.asaecenter.org/Resources/whitepaperdetail.cfm?ItemNumber=12167

IBM. *Security Services Cyber Security Intelligence Index: Analysis of Cyber Security Attack and Incident Data from IBM's Worldwide Security Operations*. IBM, July 2013. https://www.ibm.com/developeorks/community/files/form/anonymous/api/library/7c2de643-a72b-429f-a473-c77be1e9035a/document/399520ae-1898-4479-9eeb-68c5478ae4e1/media/IBM%20Security%20Services.pdf

Kedmey, Dan. "Target Expects $148 Million Loss from Data Breach." *Time Online*, 6 August 2014. http://time.com/3086359/target-data-breach-loss/

Kovacs, Paul, Melissa Markham, and Robert Sweeting. "Cyber Incident Risk in Canada and the Role of Insurance." *Institute for Catastrophic Loss Reduction Research Paper Series 38* (April 2004). http://www.iclr.org/images/Cyber-Incident_Risk_in_Canada_and_the_Role_of_Insurance.pdf

KPMG. "Canadian Insurance Industry Risks and Opportunities. Survey." 2015 (forthcoming).

Leduc, Diane and James Lee. *Illegal Drugs and Drug Trafficking*. BP-435E. Parliament of Canada, November 1996 (rev. February 2003). http://www.parl.gc.ca/content/lop/researchpublications/bp435-e.htm

Lemley, Brandon K. "When Disgruntled Employees Attack: The Computer Fraud and Abuse Act and the Problem of Authorized Access." Querrey & Harrow, November 2014. http://www.querrey.com/index.php/news-knowledge/publications/472-when-disgruntled-employees-attack-the-computer-fraud-and-abuse-act-and-the-problem-of-authorized-access

Lloyd's. "Digital Risks: Views of a Changing Risk Landscape." *Lloyd's Emerging Risks Team Report*, October 2009. http://www.lloyds.com/~/media/lloyds/reports/emerging%20risk%20reports/digitalrisksreport_october2009v2.pdf

McAfee, Inc., and Center for Strategic and International Studies. *Net Losses: Estimating the Global Cost of Cybercrime*. Intel Security, 2014. http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf

McCullagh, Declan. "Police Blotter: Ex-employee Faces Suit over File Deletion." *CNET*, 10 March 2006. http://news.cnet.com/Police-blotter-Ex-employee-faces-suit-over-file-deletion/2100-1030_3-6048449.html

McGrath, Maggie. "Home Depot Confirms Data Breach, Investigating Transactions from April Onward." *Forbes Online*, 9 August 2014. http://www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets/

Meckbach, Greg. "OIAA Speaker Explains How Ontario Civil Law on Privacy Affects Cyber Liability Exposure." *Canadian Underwriter*, 5 February 2015. http://www.canadianunderwriter.ca/news/oiaa-speaker-explains-how-ontario-civil-law-on-privacy-affects-cyber-liability-exposure/1003465430/?&er=NA

Munich Re. *Munich Re Cyber Risk Survey*. Munich Reinsurance America, 2014. http://www.munichre.com/site/mram/get/documents_E-293280320/mram/assetpool.mr_america/PDFs/5_Press_News/Press/2014_cyber_survey_report.pdf

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

New York State Department of Financial Services. *Report on Cyber Security in the Insurance Sector*. 2015. http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf

Office of the Superintendent of Financial Institutions. "Cyber Security Self-Assessment Guidance." (October 2013). http://osfi-bsif.gc.ca/eng/docs/cbrsk.pdf

O'Gorman, Gavin, and Geoff McDonald. "Ransomware: A Growing Menace." *Symantec Security Response*, 2012. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf

Osborne, Charlie. "South Korean Credit Card Firms Suspended over Data Breach." *ZDnet*, 17 February 2014. http://www.zdnet.com/article/south-korean-credit-card-firms-suspended-over-data-breach/

Partner Re with Advisen. *Cyber Liability Insurance Market Trends: Survey*. 24 October 2014. http://www.partnerre.com/assets/uploads/docs/cyber-survey-results.pdf

Peden, Margie, Richard Scurfield, David Sleet, Dinesh Mohan, Adnan A. Hyder, Eva Jarawan, and Colin Mathers, eds. *World Report on Road Traffic Injury Prevention*. World Health Organization 2004. http://whqlibdoc.who.int/publications/2004/9241562609.pdf

Phoenix Strategic Perspectives. *Survey of Canadians on Privacy-Related Issues: Final Report Prepared for the Privacy Commissioner of Canada*. January 2013. https://www.priv.gc.ca/information/por-rop/2013/por_2013_01_e.pdf

Ponemon Institute. *2014 Cost of Data Breach Study: Global Analysis*. May 2014. http://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03027usen/SEL03027USEN.PDF

Ponemon Institute. *2014 Global Report on the Cost of Cyber Crime*. October 2014.
http://h20195.www2.hp.com/v2/getpdf.aspx/4AA5-5207ENW.pdf?ver=1.0

Prensky, Marc. "Digital Natives, Digital Immigrants," *On the Horizon* 9, no. 5, MCB University Press, 2001.
http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

President of the United States. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. The White House, May 2011.
http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

PricewaterhouseCoopers. *Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015*. 30 September 2014.
http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

Privacy Commissioner of Canada. *Privacy and Cyber Security: Emphasizing Privacy Protection in Cyber Security Activities*. December 2014.
https://www.priv.gc.ca/information/research-recherche/2014/cs_201412_e.pdf

Public Safety Canada. "Top 4 Strategies to Mitigate Targeted Cyber Intrusions." March 2015.
http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tp-strtgs-eng.aspx

Recording Industry Association of America. "Scope of the Problem." *Piracy Online*, 2015.
http://www.riaa.com/physicalpiracy.php?content_selector=piracy-online-scope-of-the-problem

Rogers, Michael. "Cybersecurity Threats: The Way Forward." *Hearing of the House (Select) Intelligence Committee*, 20 November 2014.
https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf

Royal Canadian Mounted Police. *Cybercrime: An Overview of Incidents and Issues in Canada*. 2014.
http://www.rcmp-grc.gc.ca/pubc/cc-report-rapport-cc-eng.htm

Santus, Rex. "What You Need to Know About the JPMorgan Chase Cyberattack." *Mashable*. 3 October 2014.
http://mashable.com/2014/10/03/need-to-know-jpmorgan-chase

Shaw, William T. "SCADA System Vulnerabilities to Cyber Attack." *Electric Energy Online*. Jaguar Media, 2014. Originally published in Electric T&D (September-October 2004).
http://www.electricenergyonline.com/show_article.php?mag=&article=181

Shear, David, and Joe Stewart. *Underground Hacker Markets*. Dell SecureWorks, December 2014.
http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf

Snyder, Michael. "Wall Street Admits That a Cyberattack Could Crash Our Banking System at Any Time." *The Economic Collapse Blog*, 28 August 2014.
http://theeconomiccollapseblog.com/archives/wall-street-admits-that-a-cyberattack-could-crash-our-banking-system-at-any-time

Statistics Canada. "Canadian Internet Use Survey, Internet Use, by Location of Use, Household Income and Age Group for Canada and Regions." *CANSIM* Data. 28 October 2013.
http://www5.statcan.gc.ca/cansim/pick-choisir?lang=eng&p2=33&id=3580154

Statistics Canada. "Digital Technology and Internet Use, 2013." *CANSIM* Data. 11 June 2014.
http://www.statcan.gc.ca/daily-quotidien/140611/dq140611a-eng.htm

Symantec. *Internet Security Threat Report 2014*. April 2014.
https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Tassi, Paul. "Sony Pegs PSN Attack Costs at $170 Million, $3.1B Total Loss for 2011." *Forbes Online*, 23 May 2011.
http://www.forbes.com/sites/insertcoin/2011/05/23/sony-pegs-psn-attack-costs-at-170-million/

Toor, Amar. "UK Regulators Fine Sony for 'Preventable' 2011 PSN Hack." *The Verge*, 24 January 2013.
http://www.theverge.com/2013/1/24/3910538/uk-government-fines-sony-for-preventable-psn-data-breach

Tyndale, Catherine, and John P. Morgan. "Cyber Liability – What Risk Managers Need to Know." RIMS Canada Conference, Victoria, BC, 2013.
http://www.rimscanada.ca/clients/c/ce/ce8fb48b94af85570b01427e6ccf5ad1/File/3D%20-%20Cyber%20Liability%20-%20What%20Risk%20Managers%20Need%20to%20Know.pdf

U.S. Department of Homeland Security, National Protection and Programs Directorate. *Cyber Risk Culture Roundtable Readout Report*, May 2013.
http://www.dhs.gov/sites/default/files/publications/cyber-risk-culture-roundtable-readout_0.pdf

U.S. Department of Homeland Security, National Protection and Programs Directorate. *Cybersecurity Insurance Workshop Readout Report*, November 2012.
https://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf

U.S. Department of Homeland Security, National Protection and Programs Directorate. *Cyber Insurance Roundtable Readout Report: Health Care and Cyber Risk Management: Cost/Benefit Approaches*, February 2014.
http://www.dhs.gov/sites/default/files/publications/February%202014%20Cyber%20Insurance%20Health%20Care%20Use%20Case%20Roundtable.pdf

U.S. Department of Homeland Security, National Protection and Programs Directorate. *Insurance Industry Working Session Readout Report: Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues*, July 2014.
http://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf

Verizon. *2014 Data Breach Investigations Report*. 2014.
http://www.verizonenterprise.com/DBIR/2014

Verizon RISK Team with cooperation from Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service. *2012 Data Breach Investigations Report*. 2012.
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

White House, Office of the Press Secretary. "Executive Order 13549 -- Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities." 18 August 2010.
http://www.whitehouse.gov/the-press-office/2010/08/18/executive-order-classified-national-security-information-programs-state-

White House, Office of the Press Secretary. "Executive Order 13636 – Improving Critical Infrastructure Cybersecurity." 12 February 2013.
https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

White House, Office of the Press Secretary. "Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience." 12 February 2013."
https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

World Economic Forum. "Global Risks 2014." *Insight Report*, Ninth Edition, 2014.
http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

Wueest, Candid. "The Continued Rise of DDoS Attacks." *Symantec Security Response*, October 2014.
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf

Zurich Insurance Company and Atlantic Council of the United States. "Beyond Data Breaches: Global Interconnections of Cyber Risk." *Risk Nexus*, 2014.
https://www.zurich.com/_/media/dbe/corporate/docs/whitepapers/risk-nexus-beyond-data-breaches-global-interconnections-of-cyber-risk%202014.pdf

## Other Internet Resources

Internet Live Stats is a site that provides live updates of statistics pertaining to global internet use. The statistics provided in this paper were up to date as of 1 March 2015, but will have changed since then.
www.internetlivestats.com

V.I. Labs' Software Piracy Stat Watch is a site that provides statistics pertaining to software piracy. The statistics provided in this paper were up to date as of 1 March 2015, but will have changed since then.
http://www.vilabs.com/resource-section/stat-watch

# Appendix II – A survey of cyber security practices by insurers

In February 2015, the New York State Department of Financial Services released the results of a survey of cyber security practices in the insurance sector.[111] Twelve property and casualty insurers responded to the regulator's survey on cyber security. Some highlights include:

## Data breach incidents for insurers

One of the 12 insurers reported more than ten successful breach attacks over the last three years.
Five of the 12 insurers reported between one and five successful breach attacks over the last three years.
Six of the 12 insurers reported no successful breach attacks over the last three years.
Techniques used for breach attacks on insurers
Malware (58%), phishing (33%), botnets (33%), pharming (25%), and other (33%).

## Consequences of attacks on insurers

One of the 12 insurers reported a financial loss of between $6 million and $10 million.
One of the 12 insurers reported a financial loss of between $250,000 and $500,000.
Two of the 12 insurers reported a financial loss of less than $250,000.
Seven of the 12 insurers reported no financial losses over the past three years.

## Information security framework

Eleven of the 12 insurers have an information security framework in place. This includes a written information security policy, a designated communications officer for breach-related inquires, incident monitoring, an incident reporting system, information security audits, and training for employees.
Ten of the 12 insurers have a communications plan for informing stakeholders affected by a breach.
Nine of the 12 insurers have a designated information security executive, often reporting to the CIO.

## Cyber security defense

All of the 12 insurers use anti-virus software, malicious code detection software, firewalls, intrusion detection tools, encryption for data in transit, and login passwords.
All of the 12 insurers use penetration testing (44% annual, 19% quarterly, 30% monthly).
All of the 12 insurers have policies in place for the use of mobile devices.
Nine of the 12 insurers have policies to mitigate the security risks associated with cloud computing.
Three of the 12 insurers use biometrics, such as fingerprints and retinal scans.

## Cyber security budget

Eight of the 12 insurers report information security spending is 3% to 5% of their overall budget.
Two of the 12 insurers report information security spending is 1% to 2% of their overall budget.
Two of the 12 insurers report information security spending is less than 1% of their budget.

[111] New York State Department of Financial Services, *Report on Cyber Security in the Insurance Sector.*

# Appendix III – A case study from the chemical industry

Most cyber attacks target individual companies but this case study warns that criminals can attack an industry, such as the insurance industry. Symantec, the information technology security company, published a report in 2012 describing a cyber attack directed at companies involved in the chemical industry.[112] The case study below shares highlights from the Symantec report.

The purpose of the campaign was industrial espionage. The attacker was collecting intellectual property that could be sold for financial gain to help clients secure commercial advantage in the chemical industry. The attacker sought design documents, formulas, and information about manufacturing processes.

The attack covered a two-and-a-half month period in 2011, although preparations began more than four months earlier. At least 48 companies were targeted as part of this campaign, including 29 in the chemical industry and 19 in the defence sector and elsewhere. About 100 unique Internet Protocol addresses appear to have been infected and subject to remote control.

The attacker identified desired targets and sent a customized email to each person. Most organizations would have received only a handful of emails, but three companies had more than 100 targets selected. The emails typically claimed to be meeting invitations from established business partners. In some circumstances, an email was sent to many recipients with an attachment promising to be a security update. If the meeting invitation or security update attachment was opened by the targeted user a Poison Ivey remote access tool was installed. The malware established remote control over the user's infected computer.

(Poison Ivy is a remote access tool (RAT) used to infect computers. It is widely used for criminal attacks. In particular, Poison Ivey RATs are frequently used in cyber espionage attacks. The malware is available for free download on the Internet. A number of plug-ins can be used to give the attacker control over the compromised computer.)

The attackers began using the infected computers to search the internal networks for intellectual property. The criminals also sought to obtain domain administrator credentials to gain access to systems storing intellectual property and other sensitive information. Once files had been identified, this information was transferred to internal staging servers, then, ultimately, uploaded to a remote site to complete the attack. Symantec speculate that the stolen information may have been sold to a company seeking to strengthen its position in the international chemical industry.

## IN SUMMARY

***This attack illustrates how attackers could threaten to steal intellectual property from manufacturing and processing industries. The case study warns that cyber criminals could target other industries, such as the insurance industry.***

[112] Chien and O'Gorman, "The Nitro Attacks: Stealing Secrets from the Chemical Industry."