Cyber Risks

2019: Implications for the Insurance Industry in Canada
About the author

Paul Kovacs is well known and respected in the industry as the founder and Executive Director of the Institute for Catastrophic Loss Reduction at Western University, and the former President and Chief Executive Officer of PACICC. For more than 35 years Paul has been a popular commentator on insurance, disaster safety and economic policy, and has written more than 200 publications and articles. Paul is Senior Researcher with the Insurance Institute, and has published four reports with us to date: on cyber risks (2015), automated vehicles (2016), the sharing economy (2017), and this cyber risks research update.

Table of Contents

Research Update .......................... 2

Introduction ................................ 4

Summary of 2015 Report ................. 7

Background ............................... 11

Three Key Findings ....................... 16

A threat ................................... 16

An opportunity ............................ 23

An issue ................................... 29

Copyright © 2019 by The Insurance Institute of Canada. All Rights Reserved.

This research paper is published in the public domain. When citing excerpts or the report in its entirety, please use the following citation: Cyber Risks 2019: Implications for the Insurance Industry in Canada.
Cyber Risks 2019: Implications for the insurance industry in Canada

Research Update

Executive Summary

*Cyber Risks: Implications for the insurance industry in Canada* is an important foundational study published in 2015 by the Insurance Institute of Canada.¹ This was the first of an ongoing series of publications by the Insurance Institute to identify and assess the impact of significant emerging issues for the property and casualty insurance industry. The report provides a comprehensive analysis of critical cyber security questions for the industry. It concludes with recommendations about how the insurance industry can improve its cyber security and expand the cyber insurance protection that it provides to Canadians.

This *Research Update* provides a current perspective on the earlier analysis and offers three findings:

1. **A threat — Protecting insurers and brokers from attacks**

   Insurance companies, brokers, agents, adjusters and other parties involved in the property and casualty insurance industry make extensive use of the Internet and digital technology to serve the risk management needs of Canadians. The digital age has resulted in extensive benefits for the insurance industry and its consumers, but has also introduced significant risks. In particular, the risk of malicious cyber attacks continues to grow in severity and complexity. The nature and volume of the attacks continue to evolve and escalate, representing a threat to society at large, including the operations of the insurance industry in Canada.

---

There is a growing understanding that disruptions will be experienced even with best protective efforts and it is essential for everyone involved in the insurance industry to plan for how to minimize the consequences of cyber attacks. The insurance industry can and must do more to protect itself and its customers.

2. **An opportunity — A growing market for cyber insurance**

The cyber insurance market remains relatively new and misunderstood in comparison to other lines of business. Cyber coverage is recognized as higher risk than established lines due to a lack of historic experience and the ever-changing nature of cyber attacks.

Commercial cyber coverage varies significantly in form and availability between insurers. Since the 1990s, most insurers have been working to exclude cyber risks from basic commercial liability and property coverage, and introducing standalone cyber coverage or package policies over the past decade. For insurers providing cyber insurance in Canada, coverage is shifting to offer broad spectrum protection against the loss, theft or destruction of a company’s digital assets. This coverage can extend to business interruption and supply chain disruption, and provide immediate and paid access to an incident-response team. There is a growing acceptance by businesses across Canada of cyber insurance as an effective risk transfer solution.

At the individual level, coverage for identity theft and fraud is offered as an optional endorsement or included in basic coverage for homeowners and tenants. It has been widely available for more than a decade.

Cyber insurance now generates considerable revenue and represents what may be the fastest sustained growth opportunity for any line of business.
3. **An issue — The uncertain role of insurance in policy**

Consumers and policymakers appear largely unaware of the identity and fraud protection available from personal lines insurers. Cyber security policymakers, cyber experts and consumer advocates appear unfamiliar with cyber insurance coverage available to businesses large and small. Moreover, the vast majority of cyber losses are presently uninsured.

Insurance is the business of managing risk and the insurance industry has the potential to play a much larger role in society’s management of cyber threats. Insurance is an essential part of how Canadians manage the risk of vehicle collisions and damage from fire and is recognized as critical for managing the risk of physical damage from flood, climate and seismic risks. Policymakers’ views about the role of insurance in cyber risk management is uncertain and missing in the current cyber security policy conversation.
Introduction

A 2018 report by McAfee found that the global economic impact of cybercrime increased to between C$600 billion and C$800 billion a year. The report states that cybercrime is “just too easy and too rewarding.” Many organizations and individuals fail to implement basic protective measures and lack adequate defenses. Cyber criminals use both simple and advanced tools to identify targets, automate attacks and monetize their gains. High-end cyber criminals have adopted cloud computing, artificial intelligence and other sophisticated tools found in the most advanced information technology companies. Cybercrime is described as “relentless, undiminished and unlikely to stop.”

---

Accenture Security estimates that the global values at risk of cyber attacks are C$7 trillion. Accenture found that the cost of cybercrime increased by 30 percent in 2018 in the United States, Japan and the United Kingdom. In 2018, insurance ranked fifth highest in the world in terms of the average annual cost of cybercrime by industry, reporting costs twice that of the public sector. Accenture noted that “threats are dramatically expanding, while becoming more complex...the subsequent cost to our organizations and economies is substantial — and growing.”

A survey conducted by Norton LifeLock found that more than 10 million Canadians were victims of cybercrime in 2017. These consumers reported total losses of C$2 billion representing an average direct loss of C$200. Norton observes that the six most common cybercrimes reported by consumers include having a device infected by a virus, credit card fraud, a compromised password, unauthorized hacking of an email or social media account, an online consumer scam or providing sensitive personal information in response to a fraudulent email. In summary, Norton found, “When it comes to cyber security, consumers are overconfident in their security prowess, leaving them vulnerable and enabling cybercriminals to up the ante this year, which has resulted in record attacks.”

Cyber experts are united in their view that cyber space is becoming more dangerous. All users — including Canada’s insurers, brokers, agents, adjusters — are increasingly vulnerable to cyber attack. This includes attacks seeking to access and steal personal information about policyholders and employees, destruction of company data, ransomware attacks and denial of service attacks. It is important to invest in protection, establish a culture of cyber security and minimize the consequences of successful attacks. The cyber environment is expected to become increasingly risky for Canada’s insurance industry and others over the next decade and beyond.

The growing frequency, severity and complexity of attacks present opportunities for some insurers. Participating insurers are becoming more skilled and experienced at underwriting and pricing coverage for cyber risks. In 2018, Munich Re predicted that global cyber insurance premium revenue would double over the three year period between 2017 and 2020 to reach between C$10.7 billion and C$12 billion, and the Insurance Information Institute reports that

---

3 See Ponemon Institute (2019) The cost of cybercrime. Accenture estimate that the global values at risk are US$5.2 trillion over the next five years.

this coverage has generated consistent profits despite the rising cost of claims. Most large companies purchase cyber coverage. Coverage has been developed for small and mid-sized organizations and is now widely available. Identity theft and fraud coverage is widely available for homeowners and tenants.

Nevertheless, the vast majority of economic losses resulting from cyber attacks are not covered by insurance and are presently uninsured. Indeed, recent global cyber insurance claim payments were less than one percent of the estimated value of overall impact of cyber attacks. Insurance companies have the experience and skills to play a greater role in supporting society’s management of cyber threats, but this requires the collection and sharing of risk information, greater knowledge about the risk of loss and partnership with law enforcement and government agencies. Private / public collaboration has been the foundation for society’s management of the risk of loss from collisions, fire and other perils, but is not yet evident in the Canadian policy discussion about cyber security.

Global cyber insurance claim payments

>1% of the overall impact of global cyber attacks result in cyber insurance claim payments.

Source: Estimate based on several external sources, including Munich Re and Ponemon Institute

Summary

The Insurance Institute’s 2015 Cyber Risks Report

_Cyber Risks: Implications for the insurance industry in Canada_\(^6\) provides a comprehensive assessment of critical questions affecting Canada’s insurance industry. The report also provides recommendations to better protect the industry from malicious cyber attacks and protect Canadians from the consequences of cyber breach and identity theft.
The study began with an assessment of the most common forms of attack. In 2015, attacks using self-replicating viruses and worms were giving way to more sophisticated attacks based on social engineering. This included phishing, trojan horses, watering holes and an emerging threat from ransomware. The tools available to attackers were growing in capability and the cost to make an attack was declining. Minimal skill was needed to hack basic accounts. The report found that it was much easier to perform a cyber attack than to defend against one. Hackers were able to attack repetitively in search of weaknesses and then infiltrate when a single opportunity was discovered. Criminals invested time and effort into finding a successful mode of infiltration, perhaps through glitches or pre-existing software issues that are difficult to defend against. Some successful attacks were a result of poor choices made by employees, such as accidentally installing malware, leaving passwords exposed or not logging out of secure programs. This risk can and should be reduced through training.

The report found that the motivations for most cybercrime was to steal or corrupt personal data, steal corporate secrets, bully victims for financial gain or achieve political goals through state-sponsored attacks. Those initiating cybercrimes included casual hackers, insiders, professional criminals and state-sponsored attackers. A study by IBM found that 75 percent of attacks began outside of the organization, 5 percent involved unwitting employees and 20 percent involved disgruntled insiders. Insiders knew where the most valuable information is stored and had the potential to carry out prolonged attacks without arising suspicion. It was difficult to identify and catch these criminals and attribution was notoriously difficult. Governments had little control over the Internet because criminals were often not in the same country. The vast majority of attacks were not reported and often were not known. Indeed, mechanisms were just emerging to share information about current threats.

The cost of cybercrime was unknown and perhaps impossible to determine. A 2015 report by McAfee estimated that the global impact of cybercrime ranged from US$375 billion to US$575 billion. This is similar in size to the illegal drug industry or the world-wide damage from vehicle collisions. These estimates sought to measure the direct cost and did not include loss of reputation, erosion of consumer confidence and future spending on enhanced cyber security. Cyber impact in Canada was similar in magnitude to those in the United Kingdom when measured as a share of overall economic activity. The risk of loss in Canada was higher than most other countries, but well below that for the United States and China.
The expert consensus in 2015 was that cyberspace will become a less secure place over the next five to ten years. Evidence that organizations are investing in cyber security was welcome news. However, hackers, malicious insiders, organized crime and state-sponsored attackers had an overwhelming advantage. Beyond investments in defense, organizations were beginning to make preparations for recovery in the future. The report also noted an emerging concern about the risk of catastrophic cyber incidents, such as shutting down the power grid.

The report identified actions the insurance industry could take to address cyber security. In particular, the report highlighted the Office of the Superintendent of Financial Institutions’ Cyber Security Self-Assessment Guidance. This voluntary guide set out 89 questions that insurance companies, banks and other financial institutions should consider. The guide is flexible, comprehensive and well designed to address the unique needs of each insurance company.

Four methods identified to improve a company’s defense were: whitelisting programs to block unapproved applications, ensuring applications are kept updated, updating all computer operating systems and reducing the number of users with administrative access. Each of these measures enhance security and make it more difficult for criminals to attack. Most updates for applications and operating systems are centred around security. However, for the best protection, even more is needed. Companies need to be able to describe their current state and target state of security, prioritize improvements and continuously assess their progress. Cyber security requires commitment and resources.

The 2015 study included an assessment of the emerging market for cyber insurance, referencing predictions that the market for cyber breach and identity theft coverage may increase more than five-fold over the next decade. Consumer demand was expected to build due to growing awareness of the threat and the financial consequences for victims without insurance. The report noted, however, that most cyber attacks were uninsurable, including the theft of commercial secrets. Insurance is a powerful mechanism that could support society’s management of a broad range of cyber risks if sufficient information is available to confidently measure the risk. The report noted that modern coverage of other perils — vehicle collisions, fire and theft — evolved over many decades. Nevertheless, the report predicted that industry coverage over the next five to ten years would likely focus on clarifying and expanding the coverage of cyber breach and identity theft.
The report concluded with three recommendations for the insurance industry in Canada to improve its 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 to shield these critical assets.
- Build a corporate culture of cyber security that includes actions to address technological threats and security training for employees.

The report also offered three recommendations for the insurance industry to provide Canadians with solutions for cyber threats:

- 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.
Background

Attacks are increasing and more complex.

The measures of cyber risk presented in the Insurance Institute’s 2015 report on cyber risk have increased and are expected to increase further over the next decade and beyond. For example, the number of Internet users around the world at year end grew from 1 billion in 2005, to almost 2 billion in 2010, 3.4 billion in 2015 and will likely exceed 5 billion in 2020. Moreover, the number of smart devices that communicate wirelessly — the Internet of Things — is expected to increase from 2 billion devices in 2006 to 200 billion in 2020. Furthermore, the 2018 IBM data breach study measured the influence of devices connected to the Internet and the losses have begun to emerge. These measures reflect the importance and value society is placing on our connected world.

7 See Internet World Stats for data on the number of Internet users since 1995 and a current estimate.
Canada’s growing dependence on the digital future also brings risk. The connections that offer great benefits also provide access points for criminals. The number of records exposed by reported data breaches in the United States increased from 16 million in 2010, to 169 million in 2015, and 447 million in 2018. The number of reported breaches in the United States tripled over the five-year period between 2012 and 2017. These figures do not include attacks that are unreported or undetected. Several of the most admired companies in Canada reported breach events in 2018 and 2019 including the Bank of Montreal, Simplii Financial (a subsidiary of the Canadian Imperial Bank of Commerce), and Desjardins Group. An employee with Desjardins shared personal information concerning 2.7 million members and 173,000 businesses. The 2018 Cybersecurity survey report by the Canadian Internet Regulatory Agency found that 70 percent of the breach incidents in Canada involve companies with fewer than 100 employees.

Cyber criminals are targeting organizations that have made little investment in cyber protection and may have no business continuity capacity — organizations with a strong incentive to pay a ransom so they can resume operations.

Ransomware represents a rapidly growing risk for businesses and individuals. Back in 2015, Symantec noted: “Never before in the history of humankind have people across the world been subjected to extortion on a massive scale as they are today.” The Royal Canadian Mounted Police reported, “The incidents of ransomware in Canada are rising at an alarming rate. In 2015, Canadians were affected by 1,600 ransomware attacks a day. By September 2016, the attacks nearly doubled. These are the known cases. Unfortunately, many incidents still go unreported.” The Insurance Information Institute reports that, “Nearly 40 percent of businesses have experienced a ransomware attack in the last year.” Ransomware attacks are now the leading cyber threat for small and medium-sized organizations. Some Canadian victims include

12 See Yakabuski (2019) Data breach has Desjardins doing damage control.
the University of Calgary in 2016 and the communities of Wasaga Beach in 2018, Midland in 2018 and Stratford in 2019. Cyber criminals are targeting organizations that have made little investment in cyber protection and may have no business continuity capacity — organizations with a strong incentive to pay a ransom so they can resume operations. Beazley, a Lloyd's syndicate, estimated that 71 percent of the ransomware attacks in the United States in 2018 targeted small and medium-sized businesses, and ransomware attacks increased by 128 percent in early 2019. They warned, “These attacks do not discriminate in targeting businesses; all industry verticals and organizations of all sizes are falling victim to these crimes.” While most extortion requests were small, they are increasing, and the highest ransom paid by Beazley was C$1.25 million.

The number of denial of service attacks worldwide declined by 13 percent in 2018, but the length of outage increased steadily through the year from 98 minutes to 218 minutes. Cyber experts at Kaspersky Lab find that “the market for unsophisticated, easy-to-organize attacks continues to decrease. Standard DDoS (denial of service) attacks have been rendered almost pointless by improved anti-UDP flood protection, plus the fact that the technical resources are nearly always more profitably deployed for other purposes, like cryptocurrency mining.” The experts warned that “more complex attacks such as HTTP floods, which require time and effort to arrange, remain popular, and their duration is on an upward curve...these trends look set to develop further in 2019.”

The focus of cyber security efforts is shifting from an emphasis on protection against attacks, to improving detection of malicious actors on the network, and responding to and recovering from incidents as quickly as possible.

A Harris Poll commissioned in 2019 by Norton LifeLock found that most (89 percent) Canadians want to do more to protect their privacy, but half (50 percent) say they do not know how. National Bank found that 20,611 Canadians reported that they were victims of identity...
theft in 2014, experiencing a combined loss of C$10.5 million.\textsuperscript{21} The Competition Bureau of Canada received 20,000 complaints from Canadians in 2016 about online fraud, who reported experiencing more than C$40 million in losses.\textsuperscript{22} The RCMP’s Canadian Anti-Fraud Centre warn that less than five percent of mass marketing fraud is ever reported.\textsuperscript{23} The Identity Theft Resource Center found that “victims are not only having money taken from them by a theft, but they are having to spend their own money — and others’ money — to regain their footing and return back to a somewhat normal life, pre-identity theft...for most victims of this crime, it is not a matter that can be resolved quickly. As seen in this report, nearly 62 percent of the respondents had not yet resolved their identity theft case even after more than five years.”\textsuperscript{24} Statistica reports that the rate of identity theft more than tripled in Canada from 2.4 per 100,000 in 2010 to 8.9 in 2017.\textsuperscript{25} Javelin Strategy & Research report that the number of identity fraud victims in the United States increased by 30 percent over the five-year period from 2012 through 2017.\textsuperscript{26}

\begin{itemize}
  \item \textsuperscript{21} See National Bank Insurance (2019) \textit{Statistics on identity theft}.
  \item \textsuperscript{22} See Government of Canada (2017) \textit{Fraud facts 2017 - Recognize, reject and report fraud}.
  \item \textsuperscript{23} See Canadian Anti-Fraud Centre (2019) \textit{Welcome to the CAFC website}.
  \item \textsuperscript{24} See Velasquez (2017) \textit{Identity theft – the aftermath 2017}.
  \item \textsuperscript{25} See Duffin (2019) \textit{Identity theft rate in Canada 2010 through 2017}.
  \item \textsuperscript{26} See Pascual, Marchini and Miller (2018) \textit{Identity fraud enters a new era of complexity}.
\end{itemize}
Consumers want to do more to protect their privacy, but many don’t know how

89% of Canadians want to do more.

yet

50% say they don’t know how.

Source: Norton LifeLock/The Harris Poll (2018)

In response to the continuing increase in the volume and complexity of cyber threats, Scalar’s study of Canadian organizations finds “a new normal” where “the focus of cyber security efforts is shifting from an emphasis on protection against attacks, to improving detection of malicious actors on the network, and responding to and recovering from incidents as quickly as possible.”

A threat

 Protecting insurers and brokers from attacks

Canadians spend more time online, on average, than people in any other country in the world, yet most are failing to take basic steps to protect themselves from cyber attack, identity theft and fraud. Insurers, non-government organizations and several public agencies provide consumer warnings and advice. In 2018, the Government of Canada launched the Get Cyber Safe campaign “to bring together all levels of government, the public and private sectors, and the international community, to help Canadians be safer online.” The campaign provides a toolkit to help Canadians understand and address the risk.

Increasingly, attacks have been directed at small and medium-sized organizations, including an alarming increase in ransomware attacks. Insurance brokers, agents, adjusters and other parties involved in the insurance industry are at risk. Many criminal attacks are broadly based and include targets such as insurers, brokers and agents. The nature of these attacks differs from sustained attacks targeting specific large financial institutions. Most surveys and crime data warn that many organizations are not yet choosing to prioritize efforts to address cyber security. The Get Cyber Safe campaign includes a number of thoughtful tools to help smaller organizations in Canada manage this growing threat, actions that could readily be adopted by those involved in the insurance industry.

A growing number of victims are reporting cyber fraud to the local police, the RCMP’s Canadian Anti-Fraud Centre, the credit protection bureaus and other agencies. Yet the majority of incidents are not reported.

Major banks, insurers and other financial institutions in Canada have been targets of cyber attacks for a long time. Many years ago, these operational threats were managed primarily within IT departments, with a focus on prevention and security. The value and importance of prevention and security continues to grow as the frequency and complexity of attacks increase. Moreover, there is an understanding that insurers must establish a culture of cyber security that extends throughout the organization. Attacks frequently begin with the phishing of unwitting employees responding to an email. Beyond investments in protection and prevention is the need to also develop a recovery strategy that will minimize the consequences of successful attacks.

Managing cyber risks is expected to grow over the next ten years and beyond as a priority for everyone involved in the insurance industry. Proven tools are readily available to those in the industry willing to commit to cyber security.
Protecting individuals

Many Canadians have experienced identity theft or cyber fraud, or know a friend or relative who has been a victim. A growing number of victims are reporting cyber fraud to the local police, the RCMP’s Canadian Anti-Fraud Centre, the credit protection bureaus and other agencies. Yet the majority of incidents are not reported. Nevertheless, most studies show that few Canadians take basic steps to protect themselves. Surprisingly, this even includes some previous victims who resume behaviours that leave them vulnerable to another attack.29

Many organizations are working to increase awareness about this threat and provide information about cyber security. This includes most insurers, banks, the major credit protection bureaus, consumer agencies, the Royal Canadian Mounted Police’s Canadian Anti-Fraud Centre, Public Safety Canada, the Office of the Privacy Commissioner and many other federal and provincial agencies. A number of insurance companies and several other organizations have been working to educate and empower Canadians for many years. Also, several new agencies have emerged recently in Canada to promote online safety and cyber security.

In 2018, the Government of Canada announced its new National Cyber Security Strategy would include funds to establish the Canadian Centre for Cyber Security.30 The Centre provides a unified source for expert advice, guidance, services and support on cyber security. Services are being developed for the public, government agencies, critical infrastructure owners and the private sector.

The Department of Public Safety Canada provides tips to protect devices such as smart phones and laptops, advice about playing safe while gaming, and recommendations to parents about how to protect their children in the digital age. The range and quality of support provided continues to grow.

The federal Government and its partners established October as Cyber Security Awareness Month. Themes that will be discussed in 2019 include: how cyber threats work, how cyber threat affects you, how to protect yourself online, how to protect your small business, and how we can work together.

---

The Government of Canada recommends 5 simple ways to improve online safety:

- Use strong, unique passwords that are different for every site requiring login.
- Keep operating systems up to date.
- Only connect to Wi-Fi networks you know and trust.
- Turn off Bluetooth, camera and location services.
- Don’t download from questionable sources.

Protecting small and medium-sized organizations

Small to medium-sized organizations are experiencing an increase in cyber attacks. These attacks may involve extortion through ransomware attacks, denial of service attacks or malware to steal or corrupt data or personal information about customers and employees. Attacks can be remarkably disruptive, temporarily shutting down operations and eroding the confidence of consumers, business associates and employees. Small incidents can have major and wide ranging consequences.

There is limited information available about the attacks on small insurance companies in Canada, brokers, agents and adjusters. The frequency, severity and nature of the attacks is not fully known. Available national and international data, however, warn that criminal attacks are frequently scattered and confront organizations in a wide range of circumstances. Small insurers, brokers and others involved in the insurance industry would likely be caught up in these attacks. The national and international data show that few companies choose to make cyber protection a priority.

See Government of Canada (2019) 5 simple ways to improve your online safety in 5 minutes or less.
The Government of Canada offers 5 tips to improve security for smaller businesses and provides a comprehensive guide:32

- Keep software and online systems up to date.
- Secure wireless networks.
- Set up firewall and other security.
- Secure access to devices and computers.
- Educate employees on cyber security.

Protecting insurance companies

Aggressive and sophisticated attacks are frequently directed at banks, insurance companies and other major financial institutions. Many attacks are experienced each year. These attacks have been evident for many years and are expected to continue to grow in frequency and complexity over the next decade and beyond. Cyber criminals believe that they can profit from attacks on insurance companies and other large organizations, with little risk that they will be caught.

Attackers may be casual hackers, sophisticated criminals or disgruntled employees. The tools needed to infiltrate the defenses of a company continue to evolve and grow more complex. Attacks are frequently based on social engineering concepts to lure unsuspecting insiders. Sophisticated tools are widely available, inexpensive and easy to use. Attackers have the advantage if they are determined and patient.

Willis assessed the financial disclosures about cyber risk made by Fortune 1000 companies, and found that 41 percent of the companies reported that cyber threats present a critical, serious or significant risk. The proportion of large insurers reporting significant cyber threats...
was even higher (60 percent). Insurers may be subject to a cyber attack resulting in system unavailability, data corruption or disclosure of confidential personal information. Denial of service attacks could compromise operations and disrupt communications with brokers, agents and consumers.

Some insurers are working to implement an enterprise-wide security policy. The focus is on redesigning the insurers’ operations to minimize the risk of cyber disruptions. This moves beyond the importance of the timely application of security patches to also manage employee and partner access to information, and the identification of essential or priority systems requiring the highest level of protection. A commitment to cyber security goes beyond the IT department and includes training for all employees regarding cyber security. Employees must learn to recognize, reject and report cyber threats. Moreover, best practices cyber security policy now includes an assumption that good systems may not be able to mitigate all risks given the increased sophistication and volume in the threat landscape. Barriers can be erected to limit the ability of hackers to move across a compromised network. Teams can work to ensure early detection and quickly initiate a comprehensive and rigorous response.

Best practices cyber security policy now includes an assumption that good systems may not be able to mitigate all risks given the increased sophistication and volume in the threat landscape.

In 2014, the National Institute of Standards and Technology released a framework for improving critical infrastructure cyber security. An updated framework was released in 2018. The Framework provides a comprehensive approach for major insurance companies and other large organizations to manage cyber risks, and is one of several cybersecurity frameworks addressing security control, program and risk factors.

---

33 Willis (2013) *Fortune 1000 cyber disclosure by financial institutions.*
In 2013, the Office of the Superintendent of Financial Institutions issued a cyber security self-assessment guide. It was designed to address the emerging cyber threats to banks, insurers and other financial institutions in Canada. The Guide sets out a flexible and comprehensive approach for insurers to manage cyber security. Insurance regulators in other countries are also actively working with financial institutions to support the effective management of cyber risks.

Some industry continuity and security best practices include:

- Regular threat and vulnerability assessments.
- Constant monitoring of systems.
- Rapid intervention if an incident occurs.
- Continuous upgrading of applications.
- Monitoring of external cyber security trends.
- Benchmarking to learn from industry leading practices.
- Employee information security awareness and training.
- Cyber security exercises.

An opportunity

A growing market for cyber insurance

While identity theft and fraud protection is widely available in Canada, awareness of the coverage is very low for policyholders, cyber experts, consumer advocates and government agencies. Coverage is available as an endorsement for homeowners and tenants insurance, or included in basic coverage. Insurance premiums have been low for consumers, and claims costs have been readily managed by the industry, with insurers supporting restoration and recovery.
Commercial cyber insurance coverage is high risk and has experienced strong growth and consistent profits. Few insurance companies offer this coverage due to the complexity of the risk, an absence of loss experience data, uncertain policyholder needs and the risk of a catastrophic event. Global cyber insurance premiums have been doubling every three years and are expected to reach C$10.7 billion to C$12 billion in 2020. Claims paid have also increased significantly. Importantly, coverage provided has changed significantly over the past 10 years, and continues to evolve, with large differences from company to company.

**Global cyber insurance premiums — expected growth**

Source: Munich Re (2018)

**Identify theft and fraud cover**

Several insurance companies have been offering identity theft and fraud coverage in Canada for more than a decade. The product has changed very little over time and there are differences

37 See Munich Re (2018) *Demand for cyber insurance growing rapidly.*

in coverage from company to company. Identity theft coverage is an optional endorsement with many companies but is included in basic coverage for some insurers. Indeed, one insurer has automatically extended identity theft cover to all residential policyholders since 2007.  

Insurers focus on prevention, restoration and recovery services, while direct losses are not covered. As a result, this coverage differs significantly from personal auto, homeowners and tenants cover where the focus is on covering the losses incurred. The cost of coverage for consumers is very low or included in the basic premium. Deductibles are low or absent. Some insurers exclude identify theft claims when they offer a claims free discount.

Coverage typically includes a cap. Limits of $10,000 several years ago have increased over time to $25,000 for many insurers. The cap for some companies applies to the policy term while others now extend the cap to each occurrence. Insurers provide prevention and protection advice. The nature and extent of the advice available has been growing over time in response to the increased interest from policyholders and growing loss experience.

The provision of credit and identity restoration services has always been central to coverage. This includes personal information monitoring services, alerts, legal advice and provision for lost wages. Some companies have introduced coverage of legal defense costs for the resolution of disputes and repair or replacement of hardware and software if due to an attack or extortion. Enriched protection typically has not increased the low cost of coverage.

Identity theft and fraud coverage is seldom acknowledged by cyber security and consumer protection agencies. Advice concerning a wide range of other established perils focuses on actions to avoid, reduce, transfer and accept risk. Yet discussion in Canada about identity fraud seldom, if ever, recognizes that consumers can transfer part of this risk by securing insurance coverage. The purchase of identity fraud insurance is not recommended or even identified as an option for Canadians in the advice provided by government agencies, cyber security experts, or consumer advocates. Consumer and policymaker awareness of identity and fraud coverage appears to be very low.

40 See Intact (2019) my Identity – Advice and coverage for today’s world.
Commercial cyber insurance and breach coverage

Cyber insurance for businesses is evolving. There is no standard cyber insurance policy form, so terms and conditions vary considerably. Insurers offering coverage continue to respond to changing policyholder needs. Policy and coverage terms in Canada largely follow those in the United States, the primary international market for commercial cyber insurance coverage.

Concerns in the 1990s about Y2K and in the early 2000s with the 9/11 attacks led to an active campaign to clarify that insurance companies did not intend to cover the loss of digital information and other cyber risks through traditional liability and property coverage. A few insurance companies provided specialized coverage to major banks and some other large corporations, but modern cyber insurance coverage only began to emerge over the past decade. The industry continues to clarify its wordings to exclude cyber risks from traditional liability and property policies in response to challenges in the courts and feedback from policyholders and other stakeholders about ambiguity in coverage terms.\(^{41}\)

Since the late 2000s, several insurers began to offer stand-alone cyber coverage or package policies for large commercial policyholders. Recently, coverage for small and medium-sized organizations has become widely available, offered, for example, as an optional endorsement to Business Owners Policies.\(^{42}\)

Data released by insurance regulators show that 10 insurance companies accounted for 80 percent of cyber insurance premiums in the United States in 2015.\(^{43}\) This is one of the fastest growing

---

41 See Moren, Cohen and Swaminathan (2016) *Does insurance cover phishing attacks and business email compromise? The uncertainty continues.*
43 Ibid.
lines of business, and according to Aon Benfield, coverage has been profitable for insurance companies despite rising claims costs.\textsuperscript{44} Swiss Re reports that “The U.S. has been at the forefront of the cyber insurance market, driven by a high interest in data protection and the development of related laws and regulations, particularly data breach laws. In Europe, market participants expect similar developments as in the U.S.”\textsuperscript{45}

A factor limiting the insurability of cyber risks is the difficulty of projecting claims costs, which is essential for determining pricing that is acceptable to both insurers and insureds. Uncertainty is due to a lack of historic claims information and incomplete knowledge about the impact of cyber events on a broad scale.

Specific stand-alone coverage varies from company to company, but typically includes: defense costs, settlements, punitive damages and crisis management costs incurred as a result of a breach of privacy due to theft of data, settlement of an extortion threat, damage to or destruction of company data resulting from cyber attacks, and loss of business income resulting from an attack.\textsuperscript{46} Cyber insurance policies have typically excluded losses incurred as a result of third parties, but insurers are now broadening policy wordings to account for emerging risks and the dependence on information technology vendors and cloud providers. Some insurers have begun to offer coverage that addresses risk of equipment failure, property damage and injury from a cyber attack. Coverage extensions can now also include loss of income directly resulting from adverse media attention and loss of reputation following an actual or alleged event.

A factor limiting the insurability of cyber risks is the difficulty of projecting claims costs, which is essential for determining pricing that is acceptable to both insurers and insureds. Uncertainty is due to a lack of historic claims information and incomplete knowledge about the impact of cyber events on a broad scale. Changing economic, technical and social conditions, combined with evolving legislation and regulations add to the difficulty of anticipating future claims. The increasing frequency, severity and complexity of cyber threats serves to limit the

\textsuperscript{44} See Laux and Kerman (2017) Cyber update 2016 cyber insurance profits and performance.
\textsuperscript{46} See Hartwig (2019) Cyberrisk threat and opportunity.
Emerging Issues Research Series Update

appetite of most insurance companies to provide coverage. Considerable effort is required for insurers to understand current and emerging cyber risks so they can appropriately respond to changing policyholder needs, design and price coverage and effectively manage claims. Limits may emerge in the capacity of insurance companies to respond to increased demand for coverage and cost of claims.

The absence of historic data has limited the industry’s ability to confidently respond to current risks. A number of initiatives are underway seeking to collect and share information about attacks and vulnerability, however, there does not appear to be any consideration that this information could or should be used to improve and extend insurance coverage.

An emerging concern is the threat of massive wide-ranging attacks as a systemic risk for the insurance industry. Most traditional coverages assume independent losses, but a single cyber attack has the potential to affect many organizations simultaneously. Critical infrastructure, like the power grid, have been subject to repeated attacks with the potential for extensive consequences for policyholders across the country. A study commissioned by Lloyd’s estimates that a 1/200 year cyber attack on the power grid could result in significant losses in the United States and Canada. Lloyd’s estimates economic losses of C$325 billion and insurance payments of C$28.5 billion.\(^{47}\) Another emerging concern has been the shift of critical commercial data to cloud service providers. Lloyd’s predicts that a successful attack on a major cloud service provider would result in economic losses of C$6.1 billion and result in insurance claims of C$0.8 billion.\(^{48}\) These values are expected to increase over time as more data moves to cloud service providers. Some countries are exploring the idea of a government backstop for the insurance industry to address catastrophic cyber attacks as a systemic risk.\(^{49}\)

Lloyd’s predicts that a successful attack on a major cloud service provider would result in economic losses of C$6.1 billion and result in insurance claims of C$0.8 billion.

---


\(^{48}\) See Cyence (2017) *Counting the cost – Cyber exposure decoded.*

\(^{49}\) Ibid.
An issue

The uncertain role of insurance in public policy

Insurance is central to policy discussions about issues that include road safety, flooding and earthquakes, yet is surprisingly absent from the cyber security policy conversation in Canada. Policymakers are yet to demonstrate a serious interest in the nature, availability and affordability of insurance coverage for the breach of confidential consumer information, identity theft and other risks. Moreover, there is an active policy discussion about information sharing to minimize the extent of disruption from attacks and enhance the prospect of bringing charges against cyber criminals. However, this policy conversation, at least in Canada, does not appear to consider the provision of better information for insurance companies. Society would greatly benefit if insurers are provided with information so they can extend coverage to cyber risks that are presently uninsurable and to better inform management of current coverage. The absence of any discussion about insurance in cyber security policy is a marked contrast to the Canadian and international policy debate about auto insurance, flood and climate change, where the societal benefits of better data for insurance underwriting are recognized.
Report of the Senate Committee

_Cyber assault — It should be keeping you up at night_ is the 2018 report by the Canadian Standing Senate Committee on Banking, Trade and Commerce. The Committee's plan to study cyber attacks that result in the compromise of financial data grew into a wide-ranging assessment of evolving cyber risks with advice for all sectors of society and recommendations for the Government of Canada and its agencies.

The report is critical of current cyber security efforts in Canada and offers a number of bold recommendations — including an increased prioritization of cyber security education, a requirement that government agencies must report privacy breaches to the Office of the Privacy Commissioner, and enhanced information sharing to support law enforcement agencies in the prosecution of cyber criminals. The influential Senate Banking Committee also recommends that the federal government should create a minister of cyber security who reports to the Prime Minister, table an annual report on the state of cyber security in Canada, and establish an expert task force to advise the government on cyber security.

Society would greatly benefit if insurers are provided with information so they can extend coverage to cyber risks that are presently uninsurable and to better inform management of current coverage.

The Committee sent an overall message that cyber security is an issue in need of much greater attention from all Canadians, businesses and policy makers. The Committee said, “Canadians need to know that cybersecurity is a serious problem — people are failing to protect themselves from current and emerging cyber threats. All Canadians must take action to protect the country before cyber criminals are able to infiltrate critical systems and orchestrate a technological catastrophe in Canada.”

The insurance industry did not appear before the Committee, and therefore the role of the insurance industry covering the breach of consumer information or identity theft was not

---

50 See Government of Canada (2018) _Cyber assault – It should be keeping you up at night_.
acknowledged in the report. The potential for insurance to cover uninsurable cyber risks was absent in this wide-ranging discussion about cyber security policy. The Committee said, “We were particularly disheartened to learn that, other than suing the company that was hacked, Canadian consumers generally have few option of recourse when their personal information is stolen...when notified of a data breach, it is up to individual Canadians to take steps to determine if their information is being used, as there is no mechanism to help them.”

**Average monthly time spent online**

- **Canada Average**: 43.5 hrs
- **Global Average**: 23.1 hrs

Source: Comscore

**Canada’s National Cyber Security Strategy**

*National cyber security strategy — Canada’s vision for security and prosperity in a digital age* is the 2018 report renewing the cyber security strategy of the Government of Canada. The Strategy sets out C$500 million over five years to fund a new centre to enhance collaboration with other countries, the creation of a cybercrime unit to enhance the capacity of the RCMP to investigate cybercrime, and actions to address the severe shortage in skilled workers capable of confronting cyber risks. Previously, the 2010 strategy provided C$430 million over ten years.

---

to address three priorities — securing the systems of the Government of Canada, partnering to protect Canada’s critical infrastructure, and helping Canadians to be secure online.

The Honourable Ralph Goodale opens the 2018 report with the observation, “Virtually everything Canadians do is touched by technology in some way — on a per capita basis, we spend the most time online of any country in the world, at 43.5 hours per Canadian per month. We are heavily inter-connected and networked, a fact that enhances our quality of life, but also creates vulnerabilities. From commercial supply chains to the critical infrastructure that underpins our economy and society, the risks in the cyber world have multiplied, accelerated and grown increasingly malicious.”

The Strategy suggests that the government is largely unaware of the current role of insurance, let alone the potential role of insurance. For example, the Strategy states, “From a financial perspective, victims of cyber compromise face immediate costs to recover and restore their systems. They also face long-term costs to replace or upgrade cyber systems, as well as untold reputational costs. While start-ups are particularly vulnerable, the loss of intellectual property has contributed to financial ruin for businesses of all sizes.”

The Strategy does include plans for financial institutions, although the details are not yet determined. “Some cyber systems — such as electricity grids, communications networks, or financial institutions — are so important that any disruption could have serious consequences for public safety and national security. The federal government will work with provinces, territories, and the private sector to help define requirements to protect this digital infrastructure.”

Privacy legislation

Demand for cyber insurance around the world, and the nature of the coverage offered, has changed significantly over the past decade due in part to evolving privacy breach notification

52 See Kovacs (2015) Cyber Risks: Implications for the insurance industry in Canada for a discussion about an initiative lead by Homeland Security seeking to bring coverage to uninsurable risks and CRO Forum (2016) Concept paper on a proposed categorization methodology for cyber risk is an initiative to improve the information supporting cyber insurance coverage in Europe.

53 Ibid.
requirements and the alarming increase in the number of records exposed by breach incidents. In 1995, data protection was established as a right for citizens of the European Union. In 2003, privacy breach notification laws were enacted in California and spread across the United States. In 2018, the number of records exposed by reported breach incidents in the United States increased by 250 percent.

The Government of Canada passed the Privacy Act in 1983 to regulate how federal government institutions collect, use and disclose personal information. In 2000, the Personal Information Protection and Electronic Documents Act (PIPEDA) came into effect. Initially PIPEDA applied to federally regulated industries, including federally supervised insurance companies. Since 2004, PIPEDA applies to any organization that collects personal information, except in seven provinces where provincial agencies have substantially similar privacy laws and organizations must comply with provincial regulations. Since November 2018, organizations subject to PIPEDA are required to notify affected individuals if there is a breach.

Organizations are also required by law to report breaches to the Office of the Privacy Commissioner of Canada. The Office provides extensive guidance about reporting obligations.

The Insurance Bureau of Canada and others in the industry have been actively working for many years to influence how federal and provincial privacy legislation applies to the insurance industry in Canada.

Breach coverage offered by insurers provides policyholders coverage for the cost of notifying consumers, loss of income and legal fees. Coverage may be extended to include legally required compensation of others and the legal expenses of consumers. Evolving provincial, national and international legislation and regulations mandating the protection of private consumer information and requiring notification of consumers if a breach occurs has been an important driver shaping cyber insurance coverage sought by organizations.

55 Ibid.
56 See Clement (2019) *Annual number of data breaches and exposed records in the United States from 2005 to 2018.*
57 See Privacy Commissioner of Canada (2019) *What you need to know about mandatory reporting of breaches and security safeguards.*
Recommendations for the insurance industry in Canada

Insurance companies, brokers, agents, adjusters and other parties involved in the insurance industry are increasingly at risk of cyber attacks. The insurance industry in Canada should improve its resilience to cyber threats. Therefore the industry should:

- 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 to shield these critical assets.
- Build a corporate culture of cyber security that includes actions to address technological threats and training for employees to be safer online.

The insurance industry provides Canadians and businesses with solutions to support the management of a number of cyber threats. Presently, this includes the risk of identity theft and fraud, the breach of personal information, cyber extortion and denial of service attacks. The industry should:

- Build the cyber insurance market over the next ten years until most businesses large and small, homeowners and tenants purchase coverage.
- Inform cyber security policy makers, consumer advocates and law enforcement about the industry’s current contribution to cyber risk management.

Public awareness of cyber threats is growing. Canadians, their friends and their families are increasingly becoming victims. However, the majority are not implementing basic cyber safety practices online and with their devices. Businesses are experiencing losses and disruptions due to cyber criminals, but many organizations are failing to take action to protect themselves and their consumers. Moreover, most cyber risks are not covered by insurance.

- Insurance companies and brokers should partner with governments, law enforcement agencies and other stakeholders in the national Get Cyber Safe campaign to educate and empower Canadians to understand and address cyber security.
- Work with governments and law enforcement agencies to establish the conditions over the longer term to expand coverage to other cyber risks.
Bibliography


Canadian Anti-Fraud Centre. Canadian Fraud Website, 11 July 2019.
http://www.antifraudcentre-centreantifraude.ca/index-eng.htm


Clement, J. “Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions).” Statista, 26 February 2019.

http://newsreleases.cooperators.ca/index.php?s=5651&item=3494


https://sencanada.ca/content/sen/committee/421/BANC/Reports/BANC_Report_FINAL_e.pdf
https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04201.html


Government of Canada. “Ransomware: Recognize, reject and report it!” Royal Canadian
Mounted Police, 12 July 2019.


Intact. “ING Insurance launches improved ID Theft product and consumer education
campaign in Ontario.” Intact Insurance, 08 April 2008.
INGInsurancelaunchesimprovedIDTheftproductandconsumereducationcampaigninOntario/
default.aspx


http://ontario.intactinsurance.com/commerciallines/privacybreach/assets/privacybreach_ 
brokerfaq_06-18.pdf
https://www.internetworldstats.com/emarketing.htm


Munich Re. “Demand for cyber insurance growing rapidly: Munich Re offers more than just insurance.” Munich Re, 22 October 2018.  
https://www.nbc-insurance.ca/on/advises-benefits/identify-theft-statistics.html


https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf


Willis North America, 2013.

https://www.theglobeandmail.com/business/commentary/article-data-breach-has-desjardins-doing-damage-control/
PROFESSIONAL DESIGNATIONS
Chartered Insurance Professional (CIP)
Fellow Chartered Insurance Professional (FCIP)

CERTIFICATE PROGRAMS
Advanced CIP (ACIP)
ACORD Certified Expert
Adjusters’ Training & Education Series
Associate Customer Service
Canadian Managing General Agent (CMGA)
Commercial Insurance
General Insurance Essentials (GIE)
Instructor Certification
Rehabilitation Benefits Administration
Risk Management

INSURANCE LICENSING & CE CREDITS
Brokers & Agents
Independent Adjusters
CE OnDemand

PROFESSIONAL DEVELOPMENT
Business/Management
Insurance/Technical
Interpersonal/Communications

NETWORKING & CAREER DEVELOPMENT
Seminars, Symposium, Special Events connect the industry
Career Connections provides introduction to careers in insurance
mycareer maps career pathways in the industry

INDUSTRY INSIGHT & RESEARCH
Demographics of the P&C Insurance Industry in Canada, 2017 - 2027
Emerging Issues Research Series:
  Cyber Risks: Implications for the Insurance Industry in Canada
  Automated Vehicles: Implications for the Insurance Industry in Canada
  Sharing Economy: Implications for the Insurance Industry in Canada
  A Changing Workforce: Implications of Technological Disruption
  for the Insurance Industry in Canada