SEEING BEYOND RISK

Canadian Institute of Actuaries / Institut canadien des actuaires

Welcome to the new issue of *Seeing Beyond Risk*, the quarterly electronic publication from the Canadian Institute of Actuaries (CIA). Each issue presents the latest actuarial thinking from experts; below, **Patrick Vice**, MPA, looks at the online dangers facing Canadians and how actuaries and other professionals can help protect your finances from digital thieves. We are sure you will find this article informative and thought-provoking, and we encourage you to distribute it among your friends and colleagues.

RISK IN CYBERSPACE – INSURING AGAINST THE DIGITAL DANGER

INTRODUCTION

In the 1990s, before the internet became a ubiquitous business tool, Sun Microsystems[1] used the tagline "The Network is the Computer" to promote its servers. One ad campaign featured a very large dog named Network, with an explanation along the following lines: "Like a good retriever, Network will fetch what you need."

By **Patrick Vice**, MPA

Today, with the prevalence of cloud computing, arguably Sun's vision is being actualized, albeit a few decades later. However, to carry the canine analogy further, there are as many rabid pit bulls wandering around as there are friendly Labradors: when Spot retrieves the information, there is some chance he will chew up, and swallow, a good portion of your cash.

The threat posed by online criminals/fraudsters is worsening all the time. Companies have to protect themselves against a variety of risks, including data loss, fraud, website hacking, and theft of intellectual property or identities.

They are increasingly turning to cyber insurance policies as a part of their enterprise risk management security strategy.

The market for such policies is gaining traction and, given the ever-changing nature of the risk and potential exposures, actuaries are playing an indispensable role on behalf of insurers, brokers, and risk managers.

HOW BAD IS THE PROBLEM?

Consumers, businesses, and government rely on technology for day-to-day activities. Over the last two decades, there has been an exponential growth of the commercial internet to increase availability of resources for information and commerce. In 2000, 394 million people used the internet. This year, an estimated 2.9 billion are online[2].

Canada continues to be a leader in internet usage: Canadian users spend an average of 45.6 hours per month online versus 40.3 hours for U.S. users and 24.4 hours worldwide[3]. Consequently, individuals and businesses nationwide are exposed to cyber threats via various avenues. Canada's **Cyber Security Strategy** notes:

- 59% of personal tax filings were electronic in 2008 (75% in 2013[4]);
- 67% of Canadians banked online in 2009 (77% in 2014[5]); and

CONTINUED ON PAGE 2

1. Now a part of Oracle.
2. **Statista**.
3. Canadian Internet Registration Authority (CIRA) **2013 Factbook**.
4. **Canada Revenue Agency**.
5. **Canadian Bankers Association**.

Document 214116

Insurers' top 5 cyber threats[6]

- **Ever-more sophisticated attacks**. The frequency and sophistication of cyber-attacks are increasing.
- **Weak perimeter defences.** The increasing availability of systems and data through mobile devices, customer self-service portals, and shared services increases the number of "attack surfaces" insurers have to protect.
- **Poor use of security resources.** Most businesses use essentially the same tools to protect networks, systems, and data, but tools are not solutions if they are not used effectively.
- **Careless end users.** Even well-intentioned end users are careless.
- **A gap in IT/business alignment.** Communicating with business partners in terms of risk management and mitigation is a must.

- Canadian online sales in 2007 were estimated at $62.7 billion ($136 billion in 2013[7]).

In issuing the strategy, the Honourable Vic Toews, then Minister of Public Safety, wrote:

> Canadians—individuals, industry, and governments—are embracing the many advantages that cyberspace offers, and our economy and quality of life are the better for it. But our increasing reliance on cyber technologies makes us more vulnerable to those who attack our digital infrastructure to undermine our national security, economic prosperity, and way of life.

The **2013 Norton Report** estimated the total cost of cyber crime in Canada at US$3 billion. In January 2012, RCMP Commissioner Bob Paulson wrote to Public Safety and Emergency Preparedness Minister Steven Blaney asking that the government provide more information to help Canadians protect themselves online, and expand the powers of law enforcement agencies in this area. Commissioner Paulson wrote: "This growing threat significantly impacts the economic prosperity of our country, as well as individual Canadians."

Cyber hacking (and cyber policing) has progressed in pace with the evolution of the commercial internet.

In 1994, Vladimir Levin and a group of Russian hackers illegally transferred US$10 million from Citibank to accounts around the world. Levin was captured, tried, and convicted by the U.S. The majority of funds were ultimately recovered[8].

Fast forward to 2014. Mt. Gox, a "Bitcoin Exchange" (a cyber currency system) was hacked, with a loss of approximately US$500 million. By June, the founder of Mt. Gox reported that only 23% of the bitcoins were rediscovered, adding that he did not believe more would be found. Mt. Gox is presently in liquidation proceedings[9].

Cybercrime does not simply affect commercial operations or people. Earlier this year, it was **revealed** that Canada's National Research Council had been hacked by what was described as a "highly sophisticated Chinese state-sponsored actor". The intrusion meant that the council's IT system had to be isolated in order to protect other government departments. In previous years, key Canadian organizations like Defence Research and Development Canada have also been **attacked** in cyberspace.

In its **2014 Cost of Breach Study**, the respected Ponemon Institute reported that, in the U.S., the

CONTINUED ON PAGE 3

6. Insurance Networking (registration required).
7. CBC.
8. Wikipedia and the FBI.
9. Reuters.

average cost of a data breach to an organization was US$3.5 million, up 15% from the prior year, inclusive of direct and indirect costs. Reputation and loyalty repair have the greatest impact on cost. The well-publicized theft of credit card information from Target earlier in 2014 was originally estimated to cost the company over US$1 billion[10]. Current estimates are US$148 million[11].

As internet technology expands its reach, there will be increased exposure. Business Insider **describes** the next evolution of connectivity functionally: "The Internet of Things (IoT) will make many of the familiar devices and objects in our lives—from door locks to toll booths to refrigerators—suddenly Internet-connected, smartphone-accessible, and responsive." This will lead to significantly greater control by legitimate users. It will also become an increasingly attractive target for cyber criminals.

WHAT ARE INSURERS AND OTHERS DOING?

As the commercial internet rolled out in the mid-1990s, interest rose in selling products and services over the medium. This was quickly followed by concerns about risk, which led to opportunities to offer insurance against the risk. The initial response was weak. However, with the expansion of e-commerce and the emergence of risks specific to it, plus pressures from third parties—including governments—a market has developed for more sophisticated insurance products.

In 1999, *Canadian Underwriter* magazine **reported** on a panel hosted by the U.S. Society of Chartered Property Casualty Underwriters addressing insurance and e-commerce. Citing the rise in e-commerce, Jeff Behm from Atlantic Mutual noted that this would create demand for new insurance products. According to Mr. Behm, central concerns for insureds were business disruption caused by security breaches and data loss.

However, over the next decade the uptake did not meet the initial expectations. According to ComputerWorld staff writer Sarb Sembhi, this was due to **two factors**: "lack of data for underwriting and the lack of knowledge by consumers to understand the risk transference benefits."

High-profile events, such as the credit card data breach at Target and, more recently, Home Depot, or the **online theft** of 900 social insurance numbers from the Canada Revenue Agency, are raising the profile of cyber risk.

Mr. Sembhi notes that the current cyber liability coverage product has features that more directly meet the needs of commercial customers, including:

- Data breach/privacy crisis management cover;
- Multimedia/media liability cover;
- Extortion liability cover; and
- Network security liability.

Governments are adding pressure for commercial entities to enhance data security. In the U.S., 46 states have enacted **legislation** requiring disclosure of data breaches, and the Obama administration is contemplating federal legislation. The European Union voted in favour of a European data protection regulation in March. Proposed penalties include fines of EUR100 million or 5% of worldwide turnover, whichever is greater.

At the executive level of insurance organizations, cyber risk is a new revenue opportunity. According to a **white paper** from Crawford and Company, 2013 cyber insurance premiums in the U.S. totalled US$1.3 billion. Broker Marsh has **estimated** this could be US$2 billion in 2014.

CONTINUED ON PAGE 4

10. TwinCities.com.
11. Forbes.

Insurers are bringing new products to market, albeit cautiously. According to Crawford and Company's paper,

> "Insurers currently lack the data and claims history to build an accurate picture of the exposure and in lieu of this are reluctant to offer broad coverage wording and capacity to fully indemnify against first- and third-party cyber risks . . . Very few carriers are able to offer indemnity in excess of $50m with the majority writing a maximum limit of $10m or under."

Regardless, the market pressures are expected to push both limits and coverage over time.

HOW ARE ACTUARIES HELPING TO PROTECT YOU AND COMPANIES?

Given the complexity of the risk profiles, the emerging nature of the threats, the dynamic environment of the foundational technologies, and the large exposures, the role of the actuary is both challenging and critical. Fortunately there is a growing body of knowledge on which they can draw. Actuarial models to calculate the risk of cyber attack and the size of premiums to insure against it are constantly maturing, and this year actuaries—members of the CIA among them—formed a **task force** to research activities and provide educational opportunities in the analysis of cyber risk. Others have held workshops and presentations on the topic.

Some **experts** believe that as more data breaches are widely reported the availability of extra statistics will further enhance the value of actuaries' models, making their role increasingly important.

CONCLUSION

As our adoption of internet technology continues to grow, so do the economic risks to individuals, businesses, and governments and, indeed, the security risks to society. Understanding and managing these risks is very challenging but rest assured that the actuarial community is running in parallel with leaders on the insurance-selling side, ensuring that there will be alignment as the market and risk profiles become better defined.

Patrick Vice has more than 25 years of experience enabling technology and electronic commerce in the insurance and risk management communities. A founding partner of Insurance-Canada.ca, a leading source for technology and insurance news, he has held senior management positions with insurance companies, distributors, consulting firms, and technology solution providers. He serves on boards and committees of various industry associations and writes for leading trade publications.