May 25 2015

THOMPSON'S WORLD INSURANCE NEWS

• CANADA'S INDEPENDENT NEWS SOURCE FOR INSURANCE PROFESSIONALS • SINCE 1988 •

Institute aiming to establish cyber risk framework

THE INSURANCE Institute of Canada has released a new report to help the p&c industry tackle cyber risk issues.

"Cyber incidents are constantly in news headlines and insurance organizations now rank cyber security among the top three issues facing Canada's p&c insurance industry," institute ceo Peter Hohman said.

"The institute has an important role to play in conducting research for the benefit of the industry, and this seminal research report on cyber risk will provide a valuable foundation for the industry's ongoing discussions about this critical issue."

The report, 'Cyber Risks: Implications for the Insurance Industry in Canada,' examines the most common forms of cyber attacks, who the criminals are and what they are after. It also explores the types and scope of cyber losses and why these losses are expected to get worse — including catastrophic scenarios.

It is the first in a series of emerging issues reports by the institute that will explore risks facing the p&c industry.

Paul Kovacs, president and ceo of the Institute for Catastrophic Loss Reduction, prepared the report and will be part of a panel discussing the findings at the institute's inaugural Emerging Issues Forum May 28 in Toronto.

Other panel members include Serge Solski, vp, business development at Watsec Cyber Risk Management and Jacqueline Detablan, vp professional liability at AIG Canada.

The report offers 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, and
- Build a corporate culture of cyber security that includes actions to address technological threats and security training for employees.

Continued on page 5 ➤

Brokers address quake risk confusion

THE B.C. brokers' annual meeting with government MLAs is usually an easygoing, uncontroversial affair.

This year, not so much.

Chafing at the government's seeming inertia in the face of what the industry regards as alarming public ignorance about earthquake risk, the Insurance Brokers Association of B.C. was blunt with the politicians.

The meeting took place about six weeks after government of Premier Christy Clark released its 'Earthquake Consultation Report' to much fanfare and the promise of action.

IBABC executive director Chuck Byrne said the in-your-face approach was quite deliberate.

"It really was just to make them uncomfortable.

"That is really what this is about — a very uncomfortable situation," he said.

"We're basically taking the conversation (about) preparedness, which is something Premier Clark's government has recently been aggressive about, and turning it on its ear a bit, saying: 'OK, well preparing is one thing. Now you prepare and tell us where you stand on the issues of disaster relief and other things.'"

How did that go over?

"Like a lead balloon — and we expected as much," Mr. Byrne said.

He said the brokers wanted the legislators to "come clean with their perception of their role after the earthquake hits, after the big one comes," especially the extent to which they believed government would or would not reimburse citizens for damaged homes.

"This was a political question: What are you going to do? And it was meant to be leading, because they don't have a clue what they'll do and no one's expecting them to really know," Mr. Byrne said.

"But understanding the confusion that surrounds the public's perception of post-loss recovery is the point."

Continued on page 4 ➤

EGR aiming to double in size in three years

THE PRESIDENT of Quebec brokerage EGR Insurance said his firm, formed last fall, is looking to double its premiums written within the next three years.

Louis Belanger said EGR recently acquired Montreal-based Labrecque, Brouillette & Castelli because it has a solid book of business with specific expertise in transport.

That office will continue to operate as Labrecque, Brouillette & Castelli in the short term and will eventually be brought under the EGR brand. Mr. Belanger said EGR intends to keep all of its employees, who have already moved to EGR's Montreal office.

He said EGR was started with a book of business worth around $150m in commercial premiums and is aiming to hit $300m.

The firm is currently looking at other acquisitions in Quebec first, but also has sights set on Ontario.

"Is it possible that we extend to Ontario? The answer is probably," Mr. Belanger said when asked about inter-provincial plans.

"Let's start something (in Quebec) and make sure that everything goes well. And then we will look for something probably in Ontario."

He noted EGR has already had meetings and phone calls with prospects in Ontario.

"It's part of the scenario," he said.

EGR intends to grow intemally but also through strategic acquisitions of brokerages that have specific expertise or are involved in niche markets, he said.

The brokerage was formed last fall by EssOR Assurances, Pratte Morrissette and Assuraction and is now one of the largest surety specialists in Quebec.

Most cyber risks are not currently insured, report says

➤ *Continued from front page*

A report by Intel's McAfee and the Centre for Strategic and International Studies estimates that the global cost of cyber crime in 2013 was between US$375bn and US$575bn. The global impact of cyber crime is similar to estimates by the United Nations of the international production, trafficking, and sales of illicit drugs and the worldwide damage resulting from vehicle collisions.

"There is uncertainty over the precise extent of cyber crime, yet it is agreed that the impact is significant and growing," the institute report said.

The most recent KPMG survey of leaders in the Canadian insurance industry ranked cyber security as third among the 10 most important issues facing p&c insurers.

The institute notes that 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."

It says 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."

Cyber security is also a business opportunity for insurers.

Presently, the majority of companies in Canada, including most insurers, do not purchase cyber insurance. But this is expected to change over the next five to 10 years.

Breach coverage has become one of the fastest growing insurance markets in the U.S., Europe, and Canada and insurers also provide identity theft coverage for individuals.

"However, most cyber risks are not insured," the report notes.

"Global cyber insurance premiums, for example, are presently less than one-half of one per cent 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, the institute says.

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.

"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."

The institute says evolving federal and provincial privacy legislation will also have a significant influence over insurance practices.

"Insurers providing cyber insurance may become more actively engaged in contributing to the federal government's cyber security strategy."

Is says 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.

Cyber cover expected to be the norm by 2025

CYBER INSURANCE should become as common a purchase for businesses as property insurance within the next 10 years, the Association of British Insurers predicts.

"Only around 10% of large businesses have any form of cyber insurance, despite more than 80% suffering a cyber breach in a 12-month period," an ABI spokesperson told *Thompson's* last week.

Any company which uses the Internet is vulnerable to dangers including deliberate attacks by thieves and data losses caused by human error.

The association says that cyber cover will likely be the norm by 2025.

Speaking at the ABI's recent conference on cyber insurance, director general Huw Evans said the stakes are high because online breaches can cost millions and threaten the viability of many businesses.

Cyber insurance is an increasingly important way for businesses of all sizes to manage this threat."

The five key factors for cyber policies becoming a business essential include:

- Cyber crime is one of the fastest growing forms of crime in the world. It operates across international borders and attracts organized criminal gangs.
- Cyber threats are at the cutting edge of technology. The nature of threats changes so rapidly that it's almost impossible for individual companies to keep their defences ahead of the game.
- Businesses are increasingly dependent on IT for their everyday activities. It is not just information being stored online. Companies are increasingly operating telephone and payment systems through computer-based technologies.
- Cyber attacks and failures can result in businesses closing or having to dramatically change what they do. The latest government survey on information breaches found 10% of affected organizations had to change the nature of their business as a result.
- The British insurance market is already able to offer businesses the innovative protection they need. The market in London is responsible for more than 10% of global cyber insurance business, the majority of that from the U.S.

The *THOMPSON'S* TSX TICKER

■ Closing prices for shares of p&c-related companies traded on the Toronto stock exchange

COMPANY	SYM.	MARKET VALUE	APR 21	APR 28	MAY 5	MAY 12	MAY 19	YR. HIGH	YR. LOW
Co-operators General	CCS.PR.C	100m	24.62	24.90	24.90	24.70	25.00	25.24	23.43
EGI Financial	EFH	176m	15.59	15.83	15.85	14.80	15.01	17.00	11.80
Fairfax Financial	FFH	13,782m	652.00	643.50	637.23	626.29	623.00	739.00	488.31
Intact Financial	IFC	11,822m	93.62	92.90	92.50	88.83	89.90	95.90	70.30
Kingsway Financial	KFS	158m	6.79	6.75	7.04	7.20	7.28	7.59	5.97
Westaim Corp.	WED	234m	3.45	3.38	3.47	3.25	3.31	3.63	2.54

Market value is approximate, in millions of dollars, as of May 19, 2015. Figures reported in Canadian dollars.