Getting Creative

Larry Chin
Canadian Cyber Business Solutions Consultant, BAE Systems Applied Intelligence

Awareness is growing among Canadian insurance companies that cyber risks are on the rise and associated costs can be high. But steps can be taken to creatively improve cyber defences that help guard against fraud and reputational harm.

Today's cyber criminals are perpetrating increasingly organized, creative attacks against Canadian insurance companies. A BAE Systems Applied Intelligence research paper released in early 2014, *The Rise of Digital Criminality*, shows the vast majority — 82% of respondents in the United States and 80% in Canada — believe that the number of cyber attacks will increase.

Part of the reason for this is "starter" toolkits, which have lowered the "technological barrier to entry" for cyber attackers. This, in turn, means that Canadian insurance companies now face an increased need to protect personal and financial information since, if stolen, this information can be used to perpetrate claims fraud.

TOP CYBER CONCERNS

A recent KPMG survey of leaders in the Canadian insurance industry ranked cyber security as third among the Top 10 issues facing the property and casualty insurance industry at this time. In addition, a 2014 case study by Deloitte, *Global Cyber Executive Briefing*, states that concerns around cyber attacks continue to worsen.

One of the reasons for this concern is that insurers are collecting and storing increasing amounts of consumer data for the purposes of running advanced analytics. This information needs to be securely stored.

The requirement for secure storage is well-understood when one considers that while credit card information is readily and cheaply available on the black market, it has a very limited shelf life. However, information such as customer birthdates, addresses, employment information and income can be used to open new credit accounts on an ongoing basis rather than exploiting one account until it is cancelled.

This highlights the reason why fraud is such an area of concern. In fact, these concerns drove the identification of four main areas for life insurers to address, as noted during the Canadian Life and Health Insurance Association's Information Technology & Security Conference in March. These areas were data breach (legal liability), encryption (ransom), data theft (loss intellectual) and reputational risk.

On the positive side, it is worth noting that many of the breaches publicly reported by insurance companies to date have been characterized as short-term attacks, with cyber criminals compromising a system, stealing specific information and then quickly moving on. Deloitte's research did not uncover any documented cases of long-term infiltration and/or cyber crime in the insurance sector, but it is believed the number of long-term attacks may be silently growing as attackers quietly slip in undetected and establish a persistent, ongoing presence in critical IT environments.

CONVERGENCE OF CYBER CRIME AND FRAUD

The real concern for insurance companies is the security of the collected information, and as the global convergence between cyber crime and fraud increases, Canadian insurance companies must increase their defences around claims fraud.

To this end, Canadian auto insurers are already increasing their defences against fraudulent claims. Members of the Canadian National Insurance Crime Services (CANATICS) consortium have begun to pool claims information and use a managed analytics service to detect fraudulent claims activity, perhaps perpetrated by organized crime rings committing claims fraud across multiple insurers.

The use of a managed analytics service is important because for many industries, including insurance, cyber security is not an IT risk, but a business one. Mitigating the risk requires real-world experience, dynamically managing threats and being prepared with appropriate responses.

In addition, since organized crime rings do not necessarily limit their illegal activity to fraud, a side benefit to identifying fraudulent auto insurance claims may be the identification and dissolution of organized crime rings — the very same rings that may be responsible for cyber attacks.

One of the more recently highlighted business risks is with third parties or partners. Insurance companies engage with third parties to assist customers in having their cars repaired. However, this introduces considerable risk for a serious security breach as these third parties — car repair shops, in this instance — may not have the same level of security around customer data as the insurance companies themselves.

The use of a managed analytics service is important because for many industries, including insurance, cyber security is not an IT risk, but a business one. Mitigating the risk requires real-world experience and dynamically managing threats.

One paradigm for addressing this problem is the "zero trust" approach, which enforces specific process and policy to help enterprises prevent unwanted access to their systems. This, in turn, helps block cyber criminals gaining authorized access to a company's network, perhaps through the use of stolen credentials. This is important, because once a criminal has authorized access, there is the potential for launching various types of cyber attacks based on trusted credentials.

COST TO CANADIAN INSURANCE COMPANIES

Successful cyber attacks and loss of consumer information can result in significant cost associated with incident response, including forensics, notification, fraud monitoring, crisis communications and legal fees.

For an insurance company, reputational risks may be the most significant concern because insurance is built on a foundation of trust — trust that is hard won and easily lost. Therefore, in addition to considering potential monetary losses related to a cyber breach or claims fraud, insurance companies must also factor in reputational cost when considering data security.

Unfortunately, in this instance, compared to other parts of the world, North American insurers are more trusting and someone suspected of criminal activity is considered innocent until proven guilty. This has cost implications for Canadian insurance companies, since evidence of fraud must be collected to prove guilt, which, in turn, has the potential to allow cyber criminals to remain active for longer periods, or alternatively, delay the sharing of threat intelligence related to fraudulent claims.

A recent study issued by the Ponemon Institute, *2015 Cost of Data Breach Study: Canada*, found that the average cost incurred for each lost or stolen record in the country was $250, compared to the global average of only $154. The study examined the costs incurred by 21 Canadian companies from 11 different industry sectors "following the loss or theft of protected personal data and the notification of breach victims as required by various laws."

It also found that 52% of data breaches involved malicious or criminal attacks.

The first Canadian study of its kind, the results indicate that the average total consolidated cost of a data breach in Canada was $5.32 million and, of this amount, the largest cost component was lost business at $1.99 million on average, followed by detection and escalation at $1.68 million, and ex-post response at $1.53 million.

Moreover, since trust is integral to an insurance company, the costs of lost business could be even higher. In the case of one known cyber attack on an insurance company noted in a Deloitte briefing, there was an impact on cus-

tomers and individuals who had input information into a free credit-scoring app. After the breach, the organization was obliged to provide affected customers with free credit monitoring for a year, and to reimburse all damages resulting from the breach. In addition to those tangible costs, which were substantial, the organization suffered significant brand damage and loss of trust.

While this data is interesting, it is hard to determine the exact cost of data breaches in Canada because of the lack of reporting. Canada's so-called *Digital Privacy Act*, passed this past June, will eventually require companies to report breaches once associated regulations take effect.

The act will introduce fines of as much as $100,000 for deliberately not reporting a breach. However, this is pennies compared to the millions of dollars in reputational costs that a company would incur by adhering to the act and reporting the breach.

Unfortunately, the net effect could be that since the financial penalties attached are so insignificant, there will be no deterrent effect on companies' breach reporting practices.

Based on BAE Systems Applied Intelligence research from 2013, 48% of Canadian respondents agree with the perspective that organized groups of fraudsters are the most likely group to mount targeted cyber attacks against a company's IT systems. In the insurance sector, where awareness is greater, 66% agree fraudsters are the most likely to attempt an attack.

In the event of a successful cyber attack, 58% of Canadian respondents say the loss of customer data would be the biggest concern. For insurance industry respondents, 74% express concern over a successful cyber attack.

Additionally, BAE Systems research from 2014 shows that 77% of Canadian respondents note that their companies have increased the amount they spend on protecting themselves from cyber attacks over the previous year, and 65% also report they would be increasing that amount even more in the future.

These numbers are not surprising when taking into account that 15% of Canadian respondents say a cyber attack is the number one risk facing their companies. This is double the average of other countries surveyed and is significant since it demonstrates Canadians are aware of the devastating effects that a cyber attack can have on an organization and the importance of mitigating the risks.

Canadian insurance companies need to accept that the cost of cyber attacks is growing and has rippling impacts across the organization, from reputational risk to increased likelihood of fraud. Understanding today's changing cyber landscape means insurance companies can take steps to improve their cyber defences and fraud prevention efforts across the business.