Small Business, Big Threat

Cyber crime has become increasingly frequent, expensive and complex. Yet, many small businesses do not believe they are targets and may not be prepared to prevent or withstand a data breach. What can the insurance industry do to help?

Derrick Hughes
Vice President,
The Boiler Inspection and Insurance Company of Canada, part of Munich Re

Virtually all businesses collect and store sensitive business and personal information about customers and employees. The increasing frequency and severity of data breaches across the globe signals that such information is becoming even more valuable and easier to access.

Most members of the Canadian property and casualty insurance industry understand the imminent cyber risk facing the business community. Many of the business executives and owners they insure, however, may find it difficult to assess their own company's exposure and may not understand how to manage the risk.

With the recent passage of *The Digital Privacy Act* (Bill S-4), it is more important than ever to educate business customers.

A recent PwC Canada study, *Balancing Digital Opportunity with Cyber Security Risk*, shows that 88% of private companies agree or strongly agree that cyber security is an important issue for their organizations, but are uncertain about their vulnerabilities and what they need to do to prevent or manage an attack. This lack of awareness creates a compounding issue — failure to detect a data breach — which, notes Ponemon Institute research, takes an average of 170 days to discover.

Small and medium-sized businesses, which typically have fewer data security resources than big businesses, are particular targets for cyber criminals. In a survey of small business owners and professionals in the United States, published in 2014, the Ponemon Institute found that 55% of respondents report having had a data breach in the past year and 53% had multiple breaches.

Yet, only a third of those surveyed businesses notified the people affected — even though most states have had reporting laws in place for several years. Experts point to many factors for the lack of compliance, including confusion about reporting laws, how to respond and the costs involved in doing so.

Now, Canadian business owners face the same pressures. *The 2015 Cost of Data Breach Study: Global Analysis* by the Ponemon Institute on behalf of IBM suggests that the direct cost of notification in Canada is about $85 per record. (The average per capital cost of data breach over three years in Canada was $207. When divided by direct per capital costs, 41%, the result is $85 per record).

A Statistics Canada report released in 2014 found that 6% of the 17,000 Canadian enterprises surveyed had experienced an Internet security

breach. IT and security professionals say the actual number may be higher.

While it is too early to gauge the impact of Canada's breach notification law on businesses and insurers, in the U.S., where the first state notification law was enacted more than a decade ago, the number of data breaches has increased and the market for cyber insurance has steadily expanded. If experience in the U.S. is a guide, the Canadian cyber insurance market is poised to grow significantly.

Like their counterparts in the U.S., it appears that Canadian small business owners continue to underestimate their risk of data breach. In a recent study in Canada conducted by Shred-it, which provides information destruction services, half of polled small business owners believe that they would not be affected by a data breach and almost one-third do not have a protocol in place to store or dispose confidential information.

How can the insurance industry help small businesses better understand the risk and protect them from cyber intrusions and their associated losses?

The first step is to alert them of potential vulnerabilities and quantify the risk. Then, it is about implementing a plan to reduce hacking activity. To do so, those in small business must think like hackers.

COMPUTER SECURITY PROTECTIONS

It should come as no surprise that most cyber criminals enter a company through emails and browsers. Two of the most common methods of attack include phishing and watering holes.

In a typical phishing attack, employees receive socially engineered emails with a toxic attachment or link, as well as a convincing reason to click. It is difficult to guarantee that all employees will detect phishing emails all of the time, which is why phishing is a common and effective tactic.

More sophisticated hackers now also use watering holes — malicious code installed on trusted websites. For example, if a hacker wanted to attack an online retail store, he or she would put malicious code on a low-security web forum discussing new clothing trends. In going to this forum, every visitor (business owner or employee) could come under the attacker's control.

By understanding the primary methods that hackers use to attack, small businesses can improve security by focusing on the following areas:

- **Browser security:** It is difficult to decipher which websites to trust, so keeping up to date with the latest browser versions and regularly testing the browser's configuration for weakness is critical.
- ***Computer and operating system security:*** Implementing password protections and "time out" functions (requires re-login after period of inactivity) for all business computers helps. Firms should also make sure strong passwords are

being used and all operating systems, which have major security improvements baked in, are regularly updated.

- ***Internet router security:*** Hiding the wireless network's service set identifier (SSID) — the name the wireless network broadcasts to identify itself — can help prevent the interception of data.
- ***Data encryption:*** Mandating the encryption of all data is vital. Additionally, firms should consider encrypting company emails, if personal information is regularly transmitted, and avoid using Wi-Fi networks.

BUSINESS POLICIES AND PROCEDURES

A small business, such as a restaurant or retail store, has a lot to lose if its assets are stolen and data is breached. Consider the negative implications, including the loss of customer loyalty, information and revenue, business disruption and damage to equipment.

To improve its level of preparedness, small businesses must review (and re-review) company policies regarding the following:

- ***Passwords protections:*** Reusing passwords and trusting websites that store passwords will dramatically reduce a company's level of security. These activities should not be done. To add an extra layer of security for online business accounts, small businesses should set up two-factor authentication systems. These rely on something only the business should know (a user's password) and authenticates something only the user should have (typically a user's phone).
- ***Payment processing:*** Outsourcing payment processing is critical. Reputable vendors, whether for point-of-sale or web payments, have dedicated security staff trained to protect data.
- ***Social media and financial activity:*** Using two separate devices — one for online banking/other financial activities and one for email and social media — will help limit a company's cyber risk. Otherwise, just visiting one infected social site could compromise both a banking machine as well as sensitive business accounts.
- ***Employee training and education:*** Establishing a written policy about data security, educating employees about sensitive or confidential information and outlining their responsibilities will create accountability throughout the organization. It is also important to restrict staff use of work computers to business purposes only, prohibit file-sharing on peer-to-peer websites and block access to inappropriate websites.
- ***Old procedures:*** Developing another employee and client ID system, beyond social insurance numbers, is critically important. In addition, small businesses should question the security posture of business lines, vendors, suppliers and partners, and ensure that their procedures comply with applicable provincial and federal laws.

Often, criminals capitalize on employee and contractor mistakes and the loss or improper disposal of laptop computers, physical records, smartphones, tablets and storage media — the leading causes of small business data breaches.

INFORMATION STORAGE AND DISPOSAL

Criminals of all kinds, not just cyber criminals, view a small business both as a target and as a conduit to sensitive business and client information. Often, criminals capitalize on employee and contractor mistakes and the loss or improper disposal of laptop computers, physical records, smartphones, tablets and storage media — the leading causes of small business data breaches.

These elements should be considered to prevent the aforementioned activity:

- ***Clean-up:*** Reducing the "clutter" can help protect valuable data. Businesses should inventory the type and quantity of information in their files, reduce the volume of collected information and retain only what is necessary.
- ***Proper disposal:*** Cross-cutting all paper files before disposal is vital. Deleting files or reformatting hard drives does not erase data. Instead, it is important to use software designed to permanently wipe the hard drive or physically destroy the drive itself.
- ***Data safeguards and back-ups:*** Locking physical records that contain private information in a secure location and creating back-ups can significantly reduce a small business' risks. Back-ups should be encrypted and off site in case there is a fire or burglary.
- ***Portable media:*** Properly disposing of portable media such as DVDs, CDs and USB flash drives can reduce a business' susceptibility to loss or theft. Other portable devices can include smartphones, MP3 players and personal electronic devices with hard drives that "sync" with a computer. Businesses should only allow encrypted data to be downloaded to portable storage devices.

TIME FOR ACTION

Despite the considerable risks, small businesses have been slow to adopt other forms of protection, such as cyber insurance, in the Canadian marketplace. Advisen's 2015 cyber risk report, *The Real Cyber Claims Trends*, shows less than 5% of surveyed U.S. businesses with revenues of US$10 million or less have purchased cyber insurance. That number is likely even smaller in Canada, where the market is less developed and notification laws have not yet taken effect.

The fact is that many business owners still mistakenly believe their assets are "too small" for hackers and, therefore, do not think they are vulnerable.

The insurance industry can better communicate not only the risks, but also share these actionable steps to help the small business community thwart, mitigate and manage a cyber attack — and, it is hoped, get ahead of potential breach activity.