CANADIAN UNDERWRITER.ca

Canada's Insurance and Risk Magazine

TABLE OF CONTENTS Dec 2014 - 0 comments

Breach teach

There is a need for more information about privacy insurance in Canada. Any organization that collects, transmits or stores customer, employee sensitive personal or corporate information should consider buying the insurance, but a number of important factors must be reviewed prior to purchase.

By: Bobbie Goldie, Vice President, Professional Risk, ACE Group
2014-12-01

Inundated daily by reports of the latest cyber attacks, one cannot help but assume an insurmountable number of incidents go unreported. However, the Armageddon-like articles about high-profile clients and worst-case breaches do not represent the day-to-day realities of underwriting privacy risks.

Although much can be learned from these breaches, often they do not correlate with the experiences or needs of a typical buyer of privacy insurance coverage.

A broker will be hard-pressed to convince a first-time buyer of the need for privacy insurance when these high-profile breaches do not represent the exposures and claims faced by small, middle market customers. Instead, companies contemplating privacy insurance coverage need to consider a number of important factors before purchasing a policy.

NOT ALL BREACHES CREATED EQUAL

Like other insurance companies, ACE has insured some highly publicized, prolific hacker and malware-related breaches. However, the company's historical loss data clearly shows that the majority of the incidents for which notice was received are much smaller in size and not the result of hacking. As of March 2014, just 24% of all notices received were due to a hack.

Interestingly, 36% of all incident notices were not IT-related. A strong firewall is critical to protect data, but many breaches are the result of human error, vendor-related mistakes and lost paper files and laptops.

The International Cyber Security Protection Alliance (ICSPA) provides another perspective for Canadian organizations in its 2013 study relating to Canadian cyber crime exposure. The study included survey results of 520 Canadian businesses, with 341 participants having annual revenue of $10 million or less.

ICSPA reported 69% of respondents had some type of cyber-crime attack in the past 12 months. Even more staggering, a total of 5,866 attacks were reported or 16.5 attacks per affected business.

When purchasing privacy insurance, it is important to recognize that every breach response is different and, consequently, costs associated with each breach response are unique. Consideration must be given to the type and format of the compromised information in question.

For example, if a manufacturing company's human resources department misplaces a box containing the private information of pension plan participants, computer forensics services will not be needed. However, while breaches may not always trigger the need for forensics, the majority of breaches will require legal expertise.

MYTH VERSUS REALITY

The privacy myth suggests that there is minimal exposure in Canada with few claims or class actions. In reality, there has been an unprecedented uptick in legal actions - ranging from class actions that are easily being certified to individual plaintiff cases - related to privacy in the past 12 months.

There have been at least 13 class actions, five of which are already certified. One of these classes had just slightly more than 200 individuals, which demonstrates that class actions are a reality for any business.

In addition, courts are allowing actions to proceed based on the assertion that private information was compromised, not that the affected individuals suffered an actual loss.

Taking this a step further, those organizations that did not maintain the appropriate privacy policies and system infrastructure - or poorly handled the breach response - are not only threatening their corporate brand and reputation, but are also creating liability. The regulators and courts have clearly dictated stricter judgments for these organizations.

Within the underwriting arena in the Canadian marketplace, one often hears the close rate on first-time buyers purchasing privacy insurance will increase significantly once more established mandatory notification requirements are introduced.

Based on current legislation, only Alberta and certain health laws require notification.

However, anecdotal reports from Canadian privacy experts who manage breaches on a daily basis indicate that organizations are notifying affected individuals even though there may be no requirement to do so. Organizations recognize notification as a way to manage reputational and legal risk.

From a legal perspective, notifying people allows entities to take steps to mitigate potential damage, while failure to notify has led to liability in recent actions in Canada.

ONE SIZE DOES NOT FIT ALL

It can be difficult to determine the extent of privacy insurance in Canada since almost every commercial insurance company provides some sort of privacy coverage. These offerings range from robust standalone policies to built-in enhancements within another coverage, or an endorsement added to an existing policy.

This can be daunting to the first-time purchaser of privacy coverage and also makes it difficult for insurance brokers to compare offerings available in the marketplace.

Coverage has expanded considerably in recent years. Offerings can range from third-party liability to costs associated with responding to a potential breach, and coverage for business interruption and extortion.

Historical data demonstrates the costs associated with the potential breach are the most triggered part of coverage under privacy insurance. These costs include, but are not limited to, notification, credit monitoring, forensics, public relations and legal costs, although how each carrier provides these expenses may vary widely.

1. a carrier may provide a dollar amount to respond to these costs, and the insured is responsible for handling the breach and contracting with the appropriate third-party service providers;

2. a carrier could provide a dollar amount and specifically state that an insured must use the carrier's contracted one or two vendors for all losses - or the breach may be excluded; or

3. a carrier may provide an insured a dollar amount and a greater variety of vendors with breach-related experience.

It is vital that this portion of coverage is reviewed prior to purchasing insurance.

As expected, many organizations purchasing privacy insurance are in the retail, healthcare, education and financial institution sectors. As of March 2014, however, company data shows that these sectors only accounted for 48% of all incidents reported to ACE.

It is important to consider purchasing privacy insurance for any organization that collects, transmits or stores any type of customer, employee sensitive personal or corporate information.

Additionally, if an organization uses a third-party vendor to manage data, there may be an assumption that the exposure is minimized. That may not be the case since it is the organization's employees and customers who are impacted, not those of the vendor.

Some carriers provide coverage for these kinds of breaches where a third-party service provider is at fault.

In today's connected environment, cyber security is now a widespread concern.

When dealing with evolving privacy exposure, informed companies are looking for more than just a liability insurance policy. They want risk management tools to mitigate risk and, in the event of a privacy breach, access to experts to assist in responding to the breach.