Courtesy of
Precept Insurance & Risk Management

CYBERRISKS&LIABILITIES_

Responding to a Data Breach

No company, big or small, is immune to a data breach. Many small employers falsely believe they can elude the attention of a hacker, yet studies have shown the opposite is true. According to the Symantec SMB Threat Awareness Poll Global Results, 40 per cent of the data breaches in 2011 were at small to mid-sized companies.

Data breach response policies are essential for organizations of any size. A response policy should outline how your company will respond in the event of a data breach, and lay out an action plan that will be used to investigate potential breaches to mitigate damage should a breach occur.

Defining a Data Breach
A data breach is an incident where Personal Identifying Information (PII) is accessed and/or stolen by an unauthorized individual. Examples of PII include:

- Social insurance numbers
- Credit card information (credit card numbers – whole or part; credit card expiration dates; cardholder names; cardholder addresses)
- Tax identification information numbers (social insurance numbers; business identification numbers; employer identification numbers)
- Biometric records (fingerprints; DNA; retinal patterns and other measurements of physical characteristics for use in verifying the identity of individuals)
- Payroll information (paycheques; paystubs)
- Medical information for any employee or customer (doctor names and claims; insurance claims; prescriptions; any related personal medical information)
- Other personal information of a customer, employee or contractor (dates of birth; addresses; phone numbers; maiden names; names; customer numbers)

Data breaches can be costly. According to the Ponemon Institute's *Cost of a Data Breach Survey*, the average per record cost of a data breach was $194 in 2011; the average organizational cost of a data breach was $5.5 million.

Breach Containment and Preliminary Assessment
A breach or a suspected breach of PII must be immediately investigated and contained. Since all PII is of a highly confidential nature, only personnel necessary for the data breach investigation should be informed of the breach. The following information must be reported to appropriate management personnel:

- When (date and time) did the breach happen?
- How did the breach happen?
- What types of PII were possibly compromised? (Be as detailed as possible: name; name and social insurance number; name, account and password; etc.)
- How many customers may be affected?

Evaluation of the Risks Associated with the Breach
Once basic information about the breach has been established, management should make a record of events and people involved, as well as any discoveries made over the course of the investigation to determine whether or not a breach has occurred.

After the breach has been verified and contained, perform a risk assessment that rates the:

- Sensitivity of the PII lost (customer contact information by itself may present much less of a threat than financial information)
- Amount of PII lost and number of individuals affected
- Likelihood PII is usable or may cause harm
- Likelihood the PII was intentionally targeted

(increases chance for fraudulent use)
- Strength and effectiveness of security technologies protecting PII (e.g., encrypted PII on a stolen laptop, which is technically stolen PII, will be much more difficult for a criminal to access)
- Ability of your company to mitigate the risk of harm

Notification
Currently, Canada has two federal privacy laws: the Federal Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA). Both laws protect PII by regulating how private sector organizations can collect, use and disclose PII. In 2011, several amendments were proposed to PIPEDA that would require privacy breach notification across the country. Alberta is currently the only province to have mandatory breach notification provisions regarding PII, which were enacted in 2010.

Except in Alberta where notification is mandatory, the decision to notify clients is based both on the number of individuals affected and the nature of the PII that was compromised. If the company does decide to notify clients, notification should occur in a manner that ensures the affected individuals will receive actual notice of the incident, such as a phone call or letter. Notification should be made in a timely manner, but make sure the facts of the breach are well established before proceeding.

In addition to the affected clients, a company that has suffered a data breach is also encouraged to notify the appropriate Privacy Commissioner(s). While this practice is currently not required outside of Alberta, it is recommended.

Prevention of Future Breaches
The final step in the event of a data breach is to protect your company and your clients from the possibility of a future breach. Many times, this practice is as simple as reviewing internal policies and employee training practices. It is advised to perform an audit of all technology to determine the level of security in place. It may also be necessary to contact vendors and partners of the company to ensure that they have effective security policies in place.

We Can Help You Recover from a Data Breach
The four steps outlined in this article are based off of the recommendations made by the Privacy Commissioner in 2007. With the creation of Bill C-12, *An Act to amend the Personal Information Protection and Electronic Documents Act*, we will likely be hearing more soon about requirements for responding in the event of a data breach.

At Precept Insurance & Risk Management, we understand the negative effects a data breach can have at your company. Contact us today so we can show you how to recover from a breach and get your company back on its feet.