Privacy Breach – What Every Organization Needs to Know

By Bev Hooper

We are currently hearing the words "Privacy Breach" in the media on a regular basis. Financial institutions, schools, government bodies, sole-proprietors, and worldwide corporations have all been the focus of media stories concerning the inappropriate access, use, and/or disclosure of personal information.

Individuals are becoming more and more aware of their privacy rights, and have high expectations of those organizations that are entrusted with their personal information. As technology advances at lightning speed, an individual's need to control how their personal information is collected, used, disclosed, and secured becomes more and more essential.

Simply put, privacy refers to an individual's right to remain anonymous or control who, how, when, and where information that is used to identify them is managed. Consumer trust and confidence fosters many business relationships, and an organization's public commitment to privacy now goes a long way to enhance business opportunities. Both British Columbia's *Freedom of Information and Protection of Privacy Act* (public sector) and *Personal Information Protection Act* (private sector) provide the primary legislative requirements for privacy protection within this province.

No matter how committed to privacy protection an organization may be, a privacy breach may occur. A privacy breach refers to any form of collection, use, and/or disclosure of personal information that is made in contravention of applicable privacy legislation. Privacy breaches may occur as a result of system failure (example: an automated letter-stuffing machine jams and causes letters to be inserted into the wrong envelopes), theft (example: a laptop containing personal information is stolen from the office), employee error (example: an email containing a client's information is sent to the wrong email address), or intentional employee action (example: an employee purposefully accesses an individual's data when there is no operational requirement to do so).

How to deal with a breach scenario

Whatever the cause of a privacy breach, there are a number of standard steps that should be taken, as follows:

1. Identify and isolate the cause

Breaches may be reported in many ways, but often we do not become aware of any problem until our clients/customers bring it to our attention.

It is important to act quickly on any known or suspected breaches. First, we must confirm that, in fact, a breach has occurred; once confirmed, we must identify the source and isolate the cause to ensure that it cannot continue to manifest and cause additional breaches. For example, if a systems error has caused the breach, the system must be shut down to ensure that the problem can't replicate itself. Alternatively, in the case of employee error, appropriate training must be provided to ensure that the employee won't continue to make the same error.

2. Assess the impact

The severity of a breach is typically measured by assessing the sensitivity of the personal information involved. For example, a stolen list of contact information consisting of names, addresses, and telephone numbers (information generally found in a phone directory), is typically not as sensitive as stolen information that contains social insurance numbers, financial history, personal health numbers, healthcare information, banking information, etc. While both examples do constitute breaches, the sensitivity differs; and, therefore, risk to the individual(s) also differs.

3. Remediate

Once the cause of a breach has been determined, it is important to ensure that it cannot recur. This process may involve system repair, employee training, increased security measures, and even employee termination.

4. Communicate

An organization should never "hide" and hope that a privacy breach will not be detected by the public. The organization should notify all affected individuals of the breach, and advise these individuals as to how they can further protect themselves from identity theft, if necessary. For breaches that affect a larger number of individuals or involve very sensitive personal information, a company contact name and the use of a telephone hotline to answer the public's questions are very useful.

If the breach was identified as the result of a customer/client's notification, the organization should follow up with that individual to thank them for bringing the issue to its attention and also to assure them that appropriate steps have been taken.

For breaches that affect a large number of individuals or deal with very sensitive personal information, it is advisable to contact the Office of the Information and Privacy Commissioner of British Columbia to ensure that the Office is aware of the issue, should it receive any public complaints.

5. Follow up

Ensure that any problems/causes identified following a breach are completely resolved. For example, the implementation of more stringent security measures (including the use of encryption software, firewalls, building security improvement, etc.) may be required.

It is also strongly recommended that all staff attend annual privacy training to ensure that they understand their privacy obligations.

Mitigate the risk

As we strive to ensure that we're protecting the personal information in our custody or under our control, it is important to remember that mistakes may be made, accidents may occur, technology may eventually break down, and, on occasion, individuals may be motivated to act in ways that are immoral or illegal… If your organization responds quickly, efficiently, and openly to these scenarios, the negative impacts to your business will be greatly reduced!

Bev Hooper, is the president of Hooper Access and Privacy Consulting Ltd., a Victoria-based company that specializes in privacy awareness, employee computer-based and classroom training, breach mitigation, and privacy compliance audits and reviews. For more free resources, visit: www.hooperconsulting.ca.