HOW TO MINIMIZE THE IMPACT OF A CYBERSECURITY ATTACK

PIERRE-MARC GENDRON*
ROBIC, LLP
LAWYERS, PATENT AND TRADE-MARK AGENTS

> […] with great power there must also come -- great responsibility! – Amazing Fantasy #15, August 1962

My last article "Cover Up the Data that I Must Not See!" <http://newsletter.robic.ca/nouvelle.aspx?lg=EN&id=332>presented an overview of the various obligations with which your business must comply in terms of personal information protection. In this article, I will suggest certain means of applying these principles in your business.

Given the frequency of data breaches, every business should be prepared to face such a situation. Although a business should be sufficiently equipped to protect the personal information it holds, the solution on matters of cybersecurity is not necessarily to invest in more software or material. The solution must now be to go beyond prevention towards a more integrated approach comprising risk management and crisis management. Rest assured the applicable laws governing personal information protection do not impose on you an obligation to prevent all attacks. In fact, the total and complete prevention of all leaks is utopic. Hackers' attacks become more and more sophisticated, and all they have to do is to find the weakest link in your infrastructure to infiltrate it. Consequently, your efforts should rather be put on attack detection and the set-up of solutions to minimise the impact of these attacks on your operations and the extent of personal information that could be disclosed.

1- MAKE AN INVENTORY OF THE INFORMATION YOUR BUSINESS HOLDS

The first step is to become aware of the personal information held by your business and to make an inventory thereof. Contrary to the actual trend in terms of personal

* From ROBIC, LLP, a multidisciplinary firm of Lawyers, and Patent and Trade-mark Agents. Published in the Summer 2016 (Vol. 19, no. 4) Newsletter of the firm. Publication 068.206E.

information collection by businesses, “the more, the merrier” is not necessarily the best motto to apply. In reality, the more personal information your business holds, the more susceptible it will be to become the target of an attack.

Such an inventory is essential for a good handling of personal information and cannot be entrusted only to your IT staff. Directors and the management of your business must get personally involved in the process so as to implement a corporate culture that is committed to the protection of personal information. It may also be wise to retain the services of a cybersecurity expert.

To complete this inventory, you should assess:

- The nature of the personal information you collect;
- The manner in which this personal information is collected;
- The purpose for which it is collected;
- The people within your business who have access to this personal information.

Such an inventory will allow you to:

- Identify the quantity and type of personal information you hold;
- Decide whether this personal information is still necessary;
- Determine whether you have obtained each individual’s consent for the purposes for which you are using this personal information.

For example, ask yourself whether you really need the file of an employee who has left your business over 5 years ago, or whether your clients have consented to you sharing the personal information you have gathered when they were ordering products on your website. Destroy or depersonalize all personal information that you hold without consent, or that is no longer necessary. Some information is just as useful after being depersonalised. In fact, marketing data about your clients (age group, gender, geographic area) will be just as serviceable after it is severed from the clients’ name and address.

2- DEVELOP AND PUT IN PLACE A RESPONSE PLAN

As the saying goes, “proper preparation prevents poor performance”. Your conduct and the manner in which you handle an attack on the personal information held by your business cannot be left to improvisation. No matter the size of your business, you must prepare a response plan. Of course, the complexity of that plan will vary according to the size of your business and the nature of the personal information held.

Your plan must provide for the following:

- How and when your clients will be notified of an attack;

- What will be the public relations efforts necessary to minimise the attack's impact on your business reputation;
- How to restore your IT network so as to carry on your operations. Also take a moment to assess whether your backup solution is still appropriate to your business' needs;
- Who are the key resource persons to contact within your firm;
- Who are the external consultants to contact (your data hosting provider, your IT advisors, your legal counsels).

Your plan must evolve with your business. It is not something that can be prepared then forgotten. Having a response plan that falls into oblivion is just as damageable as not having a plan at all. To be fully efficient, a response plan must:

- Be communicated to your employees and be known within your business;
- Be regularly tested to assess its adequacy;
- Be updated to account for internal and external changes in your business.

The pitfall to avoid, following this new awareness and the preparation of an efficient plan, is to have your business become complacent in the face of cybersecurity issues. Indeed, cybersecurity issues are constantly evolving. Hence your awareness and your plan must be updated to account for new realities and to adapt the way in which your business responds to these issues