CYBERSECURITY

Posted on July 2, 2015

Categories: Insights, Publications

Privacy laws in Canada require that organizations implement physical, organizational and technological security measures to protect personal information under their control. The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") provides that: "The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection."[1] Similar explicit or implicit requirements exist under substantially similar provincial legislation.

Most organizations have basic technological measures in place to protect their systems, including firewalls as well as anti-spyware and anti-virus software. Organizations are also increasingly cognizant of the need for additional controls such as intrusion detection systems, auditing software, and data encryption (especially during data transmission and/or when personal information is stored in the cloud). However, organizations should consider the sensitivity of personal information under their control, in order to determine whether additional cybersecurity measures may be required to satisfy their legal obligations.

Failure to evaluate the organization's cybersecurity status and implement appropriate controls can expose the organization to complaints under PIPEDA and substantially similar provincial legislation. Furthermore, there have been a number of class action lawsuits filed in recent years following data breaches, where the plaintiffs have alleged that the defendants did not adequately protect their personal information. For example (in brief):

- Numerous class action lawsuits (which were eventually consolidated) against Target Corporation by shoppers, credit card companies and shareholders after Target was the victim of a cyber attack in 2013, which involved theft of credit and debit card data as well as other personal information. The plaintiffs alleged that Target did not adequately protect the personal information that it collected.
- Class action against Sony after a 2011 cyber attack on its PlayStation Network, Qriocity and Sony Online Entertainment accounts. The plaintiffs alleged that cyber criminals were able to access and steal their personal information due to inadequate security measures.
- Class action against LinkedIn after an SQL injection attack in 2012 breached LinkedIn's servers and led to the posting of certain information online. The plaintiffs alleged that LinkedIn used outdated security measures which did not meet the standards of the industry.

- Class action against Schnuck Markets, Inc. after its payment card system was infected with malware that allowed cyber criminals to steal credit and debit card information for a period spanning several months in 2012/2013. The plaintiffs alleged that the company did not take appropriate care to protect its systems.
- Class action against Vendini, Inc. after a 2013 breach involving the company's servers, which led to disclosure of customers' personal information including credit card information.
- Class action filed against The Home Depot Inc. after cyber criminals used malware to breach the company's cash register system in 2014, allowing them to steal customers' credit and debit card information. The plaintiffs alleged that the company did not use appropriate security measures to protect customers' personal information.

Given the rise in class action lawsuits related to cyber attacks, organizations would be well advised to conduct an audit of their existing cybersecurity status, including an evaluation of: (i) who and what is connected to their systems and networks; (ii) what is running on their systems and networks; and (iii) whether they have technology in place to prevent most breaches, rapidly detect breaches that do occur, and minimize the damage of such breaches (e.g., automatic shutdown when data leaks are detected).

Organizations should also take into account the advice of cybersecurity experts. For example, the Australian Government's Department of Defence has suggested the following four mitigation strategies, which it has found can significantly reduce the risk of a cyber intrusion:[2]

1. Application whitelisting
2. Timely patching of applications
3. Timely patching of operating system
4. Minimize administrative privileges

See more information on these mitigation strategies.

The four mitigation strategies noted above have also been emphasized by the Council on Cyber Security, in its paper "The Critical Security Controls for Effective Cyber Defense", as being amongst the "First Five Quick Wins" that will have the most immediate impact on preventing cyber attacks. The fifth "quick win" emphasized by the Council on Cyber Security is "use of standard, secure system configurations."

Although the controls listed above have been recommended by some cybersecurity experts, they are just a few measures that organizations could consider in the context of their overall security plan. Once the organization understands the current state of its cybersecurity, it would be well advised to seek input from cybersecurity experts who can advise on whether additional controls are required.

by Lyndsay A. Wasser

[1] PIPEDA Article 4.7.2.

[2] See more information.

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.