FIELD LAW

Business Group

The Advisor

November 24, 2014

Heartbleed Virus Causes Heartburn: Information Security Implications

By Anne Côté

News reports regarding the so-called Heartbleed computer virus sparked concerns regarding cyber security and digitally-stored personal information. The Canada Revenue Agency announced that the virus caused a security breach involving the compromise of the social insurance numbers of hundreds of individuals. Other high profile payment system breaches have also been reported.

Although it makes for interesting news, it is not always the effect of a computer virus or the actions of a computer hacker that can lead to a breach of personal information. Human error or systems errors also lead to reported privacy breaches (see our previous article "Alberta Privacy Commissioner Issues Report on Privacy Breaches").

Nevertheless, the security of digitally-stored personal information is a key part of securing all of the personal information held by your organization. What can your organization do?

1. **Keep up-to-date on information security practices**. Your IT personnel and your organization's Privacy Officer should be involved in this crucial ongoing obligation.
2. **Limit your collection of personal information**. Consider your organization's collection practices. Collect only what you need. For instance, a social insurance number is valuable information for identity thieves. Your organization may only need this information for limited groups of individuals (such as your employees).
3. **Take steps to secure personal information**. Put in place adequate safeguards which are appropriate to the types of personal information you collect. Adopt appropriate policies and procedures, including those related to responding to a privacy breach.
4. **Be vigilant and provide training**. Monitor for privacy breaches, and train your employees to report potential privacy breaches to your Privacy Officer.
5. **Consider your reporting duties**. If your activities fall under Alberta's *Personal Information Protection Act*, or certain other privacy statutes in other jurisdictions, report to the appropriate

parties any breach that leads to a real risk of significant harm (including the risk of identity theft). Proposed amendments to the federal private-sector *Personal Information Protection and Electronic Documents Act* will also necessitate the reporting of privacy breaches.

6. **Consider the potential for liability**. Depending on the application of privacy laws and the availability of tort actions in a particular jurisdiction, a lawsuit, including a class action, could be filed in relation to privacy breaches. Consult legal counsel about liability issues.

Questions about how to deal with a potential privacy breach? Not sure if your organization is compliant with privacy legislation? Contact Anne Côté, Chair of Field Law's Privacy Group. We offer comprehensive advisory and litigation services, including a Privacy Audit of your organization's practices. Our Privacy Audit will help your organization identify and minimize privacy risks.

SHARE THIS ARTICLE

CALGARY
400 - 604 1 ST SW
Calgary AB T2P 1M7
403-260-8500

EDMONTON
2000 - 10235 101 ST NW
Edmonton AB T5J 3G1
780-423-3003

YELLOWKNIFE
601 - 4920 52 ST
Yellowknife NT X1A 3T1
867-920-4542