Craig Burley, LL.B., Barrister and Solicitor

20 Hughson Street South, Suite 203, Hamilton ON, L8N 2A1
(905) 870-0196
craig.burley@gmail.com

CRA DATA SECURITY ISSUES
11 July 2014

I wrote a brief article in 2009 on data security within CRA at a time when the issue received much less attention generally than it does now. (I am not happy with the article in hindsight, but I have included it.) The following brief tries to give a high-level overview of what has happened since and to flesh out some of the more interesting data security issues.

Basic Premise

The basic premise to take as a starting point for CRA data security issues is that CRA has a positive obligation to preserve the confidentiality of all the data it collects. It has a basic overview of its data security measures at http://www.cra-arc.gc.ca/ntcs/scrty-eng.html and of its internet security measures at http://www.cra-arc.gc.ca/ntcs/ntrnt_scrty-eng.html.

We have all run into some of the basic security countermeasures before. Whether this means CRA refusing to speak to unauthorized persons (or indeed shredding communications from persons they consider unauthorized), CRA demanding client information before engaging in a discussion, the limited access to information that frontline service personnel have, or CRA's refusal to employ email and voicemail. The concern over data security has grown, though, and now encompasses much more than worries over this type of social engineering or "phishing" attacks against CRA, or middleman attacks that target e-mails.

CRA also routinely fails to follow routine government procedures on privacy. In one recent incident, it failed to consult with the Privacy Commissioner before removing true dual authentication from NETFILE (not that the existing dual authentication worked well; both tokens could be accessed from documents sent in the same envelope).

Heartbleed

"Heartbleed" was a vulnerability in the most popular "SSL" ("secure socket layer") cryptography software that encrypts internet communications. It was a "buffer overrun" exploit (I will circulate a very neat little cartoon that explains it quite clearly) and was an extremely crude fishnet, but in a classic story a teenage hacker used it to fish nearly 900 SINs off CRA's secure servers used for tax filings. We don't know (it wasn't reported) what other information that hacker may have accessed, or what other information others may have used. SINs are the "story" and therefore they are what get reported, even though SINs are a comically unsecurable piece of data (despite CRA's fairly pathetic redaction efforts).

This points to the most common problem in CRA security: you most likely will never be informed of a breach. This is not only because a breach is likely never to be found; even in Heartbleed which was a major news story, the RCMP ordered CRA to delay informing the taxpayers in order to help them catch the culprit (for obvious reasons, this basically never works, and culprits are caught in other ways, but police do it anyway.)

Rogue Employees

A more serious concern, because it's a much more precise instrument, is the use of CRA employees to spy on taxpayer files. Like many (most?) other large organizations, the CRA is replete with such behaviour. In 2010 there was a large dump of reports about dozens of rogue CRA employees accessing unauthorized information about third parties, most likely because there were simultaneous reports about criminal and even violent behaviour by CRA employees working on behalf of criminal organizations for criminal purposes.

CRA has internal data controls and monitoring, but there have been so many successful scams and frauds occurring from inside CRA itself in the past ten years that it seems that, as one would expect, they are not generally effective. However, while that's not a hopeful message, it is worth remembering that if a taxpayer *does* have a problem with confidential data on the lose or being sold, it is worth checking out the CRA as a possible source.

The good news is, that if someone is targeting a taxpayer directly, unless they are a CRA employee it will *usually* be easier to gain unauthorized access to the taxpayer's own systems, rather than CRA's systems. Cold comfort, perhaps.

What can you do?

As a tax practitioner, there is simply very little that can be done to ensure the security of client information with CRA. As my earlier article on the topic shows, most of the provisions under which CRA can legally release information are no-notice to the taxpayer.

The most important aspect that you can control is to encourage clients to maintain up-to-date authorizations, and where possible to offer to manage their authorization for them with CRA. Client reminders, explaining how to remove old authorizations and how to "wipe the slate" and explicitly re-authorize, are probably the most useful tool in this regard.

If a client learns of a possible problem or leak within CRA data security, acting fast but know it will usually be too late; all their accessible data is probably gone. However, it will be important in these situations to reset passwords and limit use of CRA e-services. You can call CRA's e-services helpdesk at **1-800-714-7257** for individuals and **1-877-322-7849** for businesses.