STARTING YOUR OWN FIRM

Invest in security now or pay later

By NICHOLAS CHEUNG

Far too often, media reports tell the world about confidential or personal information being lost — from tax returns found in dumpsters, to laptops stolen from parked cars and faxes sent to a wrong location.

Accounting firms collect a significant volume of confidential and private information and clients expect this information will be protected. Failure to meet statutory and professional requirements can have significant consequences such as:

- Damage to the firm's reputation and credibility
- Legal liability and public regulatory sanctions
- Loss of business

All staff — partners, staff accountants and administrative staff alike — need to understand their responsibilities to protect client information.

Nicholas Cheung, Canadian Institute of Chartered Accountants

Whether a firm is an established practice or a start-up, it is essential to have a robust privacy and data security program. All staff — partners, staff accountants and administrative staff alike — need to understand their responsibilities to protect client information. Showing a strong commitment 'from the top' will help your firm demonstrate that protecting client information is paramount.

A popular mantra of privacy professionals is that you can have security without privacy, but you cannot have privacy without security. Privacy is more than just securing data. It is about implementing policies and procedures so clients understand why their information is needed, how their data is being used, that you will be obtaining consent to collect and use that data and notifying them about their choices.

Firms should develop and implement their privacy policy and procedures, build appropriate security measures into their systems and periodically assess their privacy and security risk.

One tool to use is Generally Accepted Privacy Principles (GAPP), a global privacy framework developed by the Canadian Institute of Chartered Accountants and American Institute of Certified Public Accountants. Internationally recognized, GAPP provides a number of criteria organized around 10 principles for assessing a privacy program and best practices.

Know the law. While privacy laws affecting the private sector have been in force since 2003, there continues to be low to medium awareness of those laws by small and medium sized enterprises, according to a survey commissioned by the Office of the Privacy Commissioner of Canada. Determining which privacy law applies to your firm largely depends on where your firm resides and the nature of transactions being conducted.

Develop a privacy policy. This is done to inform clients about privacy practices within your firm and cover the following:

- The purpose for which personal information is collected, used, retained and disclosed
- The choices regarding collection, use and disclosure
- How personal information is used, retained and/or disclosed to third parties
- How individuals may review and update their personal information and how they may file a complaint
- How personal information is protected.

A privacy officer should be appointed to oversee full implementation and compliance with the firm's privacy policy and procedures.

Most data breaches, contrary to popular belief, are caused by internal factors rather than external hackers. Training employees about privacy and data security is one of the most effective ways to prevent breaches since they handle and process personal information and interact with clients.

The survey commissioned by the Office of the Privacy Commissioner of Canada noted that two-thirds of businesses reported that staff has not received any privacy training. Another report found organizations cite training and awareness programs as the measure most implemented following a breach. Not only is educating employees about privacy required by law, it also helps improve customer service and reinforce corporate culture and values.

CHEUNG

Firms also need to be aware of their obligations to retain client files under their rules of professional conduct and other legal requirements. A policy should be in place to securely retain client information and, once no longer needed, disposed of in a secure manner.

Retaining information has costs. Ensure that shredding machines are placed in convenient locations and used by all staff.

Unwanted photocopies or draft financial statements and income tax returns should be shredded rather than having whole copies going into a recycling or garbage bin.

Maintain up-to-date virus protection on systems and laptops. Use only genuine software to ensure that critical updates are received and installed. Software vendors often will make updates available to correct newly discovered vulnerabilities but only to licensed users. Limit the installation of third-party applications and software to minimize the possibility that malicious software (or 'malware') could be downloaded and compromise security or reduce productivity.

According to Claudiu Popa, author of The Canadian Privacy and Data Security Toolkit for Small and Medium Enterprises, "Companies big and small should take a layered approach to malware and hacker protection, starting with keeping server room doors locked, the use of properly configured firewalls, monitoring for unauthorized network activity, and workstation-level controls including email, password-protection and data encryption."

Lost laptops and other portable devices such as USB memory keys and portable hard drives account for 50 per cent of all data breaches, according to research. For greater security, portable devices must be password protected and hard drives encrypted to prevent unauthorized access.

Never leave laptops in open view in a vehicle or public area. Have employees sign a policy that governs the use and protection of portable devices. A data confidentiality policy can be enforced by enabling only the use of encrypted USB keys and external storage devices.

To reduce the risk of losing portable devices for those employees who frequently work away from the office, use a virtual private network (commonly referred to as VPN) which allows employees to securely connect to the firm's network (and their own desktop) through the Internet without having to store sensitive data on the portable device itself.

Communication through email is not a secure form of transmission. Yes, email is an efficient and often more timely method of obtaining information than trying to play telephone tag. However, it should not be used to transfer information of a confidential or personal nature. From a privacy perspective, this is a major concern during income tax season, when accounting professionals often require additional information to complete a tax return.

To improve security, investigate online services that offer secure email and online file transfer services to ensure that confidential or personal information is not sent in an unsecured manner.

Currently, there is no legal requirement for firms to disclose the loss of any personal information. However, that could soon change with proposals to amend privacy laws to include a requirement for firms to notify clients and possibly other parties (such as the privacy commissioner and police) when a breach occurs.

In anticipation of this and the fact that costs of reacting to breaches almost always exceed those of adopting proactive measures, firms are well advised to invest upfront in robust data security and a privacy program.

Nicholas F. Cheung, CA, CIPP/C, is a principal with the Canadian Institute of Chartered Accountants. He is the contributing author of 'The Canadian Privacy and Data Security Toolkit for Small and Medium Enterprises' which is available at www.cica.ca/privacy.