Practice Advisory

(Originally published in Summer 2005 CheckMark)

Digital Data and Security

Introduction

It is a nightmare scenario. The chartered accountant walking towards her car in the parking lot sees the shattered window glass strewn across the pavement. Her heart leaps. She presses the panic button on her key chain which starts the horn and lights flashing. She runs to the car and moments later her fears are confirmed; her laptop is missing.

Similar scenarios are occurring every day across North America. Laptops present an enticing target for would be thieves due to their high value, ease of mobility and difficulty in being traced. Most thieves are only interested in the value of the computer. A small, but growing number, have realized that the data stored on the hard drive can be even more valuable than the laptop.

This article is designed to raise awareness of the issues arising out of the loss or theft of computer equipment or digital data. It will explore the obligations on a chartered accountant to maintain the confidentiality of client data, risk minimization strategies and steps to take if there is a theft or security breach.

Susceptibility of digital data to theft

Computerization has been a boon for accountants. The digitalization of client data has permitted accountants to offer more services, greater, in-depth analysis and faster service, all at lower cost to the client. Specialized software has simplified the preparation of tax returns, financial statements and business analysis.

Technology has also unchained accountants from hard copy documents with a reduction in document loss, storage costs and document retrieval costs. As accountants move towards the paperless office, they are able to access all relevant client information through their computer.

Digital data has also improved mobility and access. An accountant can take the client's data on a laptop or disk, enabling the accountant to have ready access to critical information at client conferences, transactional meetings with other professionals and in responding to government enquiries or audits. It also frees the accountant to work away from the office.

The digitalization of the client's information has brought many advantages. It has also created increased exposures for loss or theft of client data. Client data is susceptible to hacking over the internet, theft of a laptop or inappropriate disposal of storage media.

Chartered Professional Accountants of Ontario
(The Institute of Chartered Accountants of Ontario)
69 Bloor Street East Toronto ON M4W 1B3
T. 416 962.1841 F. 416 962.8900 Toll Free 1 800 387.0735
www.cpaontario.ca

The duties of the accountant

Accountants are under ethical, legal and contractual obligations to maintain client confidentiality. The governing Rules of Professional Conduct require the accountant to maintain any confidential information concerning the affairs of the client in strictest confidence.

There is also an implied, if not express obligation on an accountant to maintain confidentiality of client information received in the course of their engagement.

Accountants are also subject to privacy legislation, principally the Federal Personal Information Protection and Electronic Documents Act (PIPEDA) or its provincial counterpart. Under PIPEDA, the use, disclosure, and retention of information is regulated:

"Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law." (Principle 4)

The financial information of a client is considered to be sensitive information under PIPEDA. Sensitive client information requires the accountant to take an enhanced level of care in protecting the information from disclosure.

It is clear that there are legal, ethical and contractual obligations on accountants to keep client information confidential. Perhaps even more important are the business considerations. Clients expect their accountant to act with integrity and protect their confidential financial information. The success of the business relationship and the quality of advice the accountant is able to provide is dependent upon the client feeling comfortable in fully disclosing his or her information. Any client concerns over the security of the confidential information will compromise this full disclosure. Furthermore, any subsequent loss of client data could damage the accountant/client relationship and ultimately result in loss of the client.

From every perspective, protection and security of client information is of paramount importance to the accountant. Unfortunately, in the press of today's business, appropriate consideration and thought may not always be given to data security issues.

Areas of susceptibility and safeguards

The following are areas that an accountant should consider in safeguarding the digital information of clients:

1. Digital data can be accessed by anyone who has physical access to the storage media. For protection the following should be considered:
   a) Security measures to prevent unauthorized access to the physical office space;
   b) Strong password protection of access to computers containing client information;
   c) Biometric security procedures, such as finger-print scanning;

d) Encryption of data.

2. It is not just outside intruders that pose a danger. Staff and others with access to the office may also potentially make unauthorized access to client data. In addition to the above, consider:
   a) Employment contracts or personnel policies spelling out the employees obligations with respect to confidential client information;
   b) Limiting access of employees to data on files on which they are currently engaged. Remove access when the engagement is concluded;
   c) Monitoring of audit trails on data access to determine if there has been any unauthorized or questionable access.

3. Networks with external access points are susceptible to hacking. Consider:
   a) Firewall protection of networks from outside internet access;
   b) Strong security control over external access to networks including passwords, limits on data accessible and susceptibility of the data link to hacking;
   c) Control over Wi-Fi access to office networks;

4. Laptops and other media taken off site are susceptible to theft, loss and hacking. Consider:
   a) Limits on the data to be stored on laptops which are moved off-site;
   b) Software or hardware safeguards to prevent hacking of laptop data connections or computers when using off site Wi-Fi access;
   c) Encryption of data;
   d) Protocols for use and storage of laptop when off site.

5. An area of growing concern is the disposal of old technology that contains client data. Consider:
   a) Protocols for the disposal of media which may contain client data (don't forget your backup media);
   b) Physical destruction of CD's, disks and hard drives;
   c) Scrubbing software for hard drives which are being repurposed, reassigned or discarded.

This list is by no means exhaustive. The steps required to provide protection in each of these areas are beyond the scope of this article. There is a wealth of information available on the Internet that will get you started on addressing these issues. The best method is to engage a security consultant to review your processes, systems and procedures in order to maximize the security of the client data.

WHAT TO DO IF THERE IS A BREACH

If client information is lost or inappropriately accessed by third parties, the accountant is under an obligation to do all that he or she can to avoid or minimize any damage to the client.

If there has been a theft of equipment or media containing confidential client information, the police should be immediately informed and appropriate reports completed. The accountant will have to

determine what information was on the computer or the media and which clients are potentially affected.

The privacy officer of the accounting firm should be notified and should follow the procedures previously formulated by the firm. Such procedures should include informing the client whose data has been potentially compromised. This should be done as soon as possible to minimize the risk of loss to the client arising out of identity theft or other misuse of the information. This is particularly of concern where the client data includes social insurance numbers, bank account information, information identifying specific assets, security registrations or the signature of the client in digital form.

The client should be informed of the specific information which has been lost or stolen so the client can take steps to protect himself or herself to the extent possible.

It will be appreciated that communicating with clients in these circumstances will be embarrassing to the accountant. Such communication, however, cannot be avoided to minimize the client's exposure. The thought of potentially having to make such a communication should create a greater incentive to keep the client data safe and secure in the first place. This is particularly motivating considering the number of different clients whose data may be on a particular laptop.

Firms should consider an incident response plan such as the template prepared by CICA.

LIABILITY EXPOSURES FOR CLIENT DATA

If client information is lost or stolen, the accountant is exposed to more than the embarrassment of advising the client of the loss. There is potential liability on the accountant for any and all damages that flow from that loss.

To establish liability, the courts will consider whether there was a breach of duty or breach of contract on the part of the accountant. The duty on an accountant will be described by the ethical rules, PIPEDA or similar provincial legislation and common law obligations with respect to confidential information. If the accountant did not take reasonable steps to maintain the security and confidentiality of the information, then the accountant would be liable for the damages that flow from the disclosure of the information. Such damages can include losses arising out of identity theft, the costs of the client in minimizing his or her exposure to identity theft or misuse of the information as well as any emotional upset or embarrassment caused to the client as a result of the disclosure.

The Federal Privacy Commissioner has found that a business which had a computer stolen from the automobile of an em ployee was in breach of PIPEDA. In that case, the commissioner felt that the company's failure to follow its own internal guidelines on protection and security of client information was an important factor. In that case, the business had guidelines with respect to the use and security of laptops, but these had not been followed in this particular instance. This decision

highlights the importance of not only developing a security plan, but also following it and monitoring employees to ensure that they are adhering to the systems which have been put in place.
There have been a number of high profile disclosures of confidential financial information by businesses, credit card facilities and financial institutions. These businesses are facing claims arising out of the disclosure of the information. The businesses are exposed to claims regardless of whether there has been a misuse of clients' information. The mere fact that client information may have been potentially disclosed to unauthorized third parties, creates a potential for loss and embarrassment.

CONCLUSION

Accountants handle sensitive client information every day. They are ethically, legally, and contractually bound to exercise care in maintaining the confidentiality of this information. Accountants must take steps to ensure that client information, particularly in digitized form, is kept in a secure environment. This requires appropriate systems, security measures and office procedures to be put in place. It also requires that the system be monitored for compliance and updated as technology changes.

The security of your client and your professional relationship with your client require care and vigilance in maintaining confidentiality of the client's information.

About the author

Michael E. Girard is a principal of Girard Law Office. He graduated from University of Windsor (1983) and was admitted to the Ontario Bar (1985). He completed his Master of Laws (Osgoode 1998), with his major paper on CyberConflicts: Jurisdiction and Choice of Law for Internet Transactions. His practice is focused on professional liability of accountants, discipline, computer and technology issues. Mr. Girard has written and lectured on technology issues, professional liability, advocacy and insurance law. He is a past member of the Faculty of Computer Education of the Law Society of Upper Canada. Mr. Girard is lead counsel on the first privacy law class action in Canada.