CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Keeping it Confidential: Securing Your Clients' Information

A recent survey of practitioners in Canada revealed that only a small percentage (between 10% and 15%) of CAs always encrypt the financial statements, tax returns and other financial information that they email to their clients.[1] Sending such information in clear text could pose a security risk to client information. A September 2012 *CAmagazine* article, *Safe & Secure,* explained the technical background on how email passes from the sender to the receiver. As noted in the article, practitioners should "treat email content the same as the content you would write on a postcard." In other words, there is a risk that client information can be breached if it is sent in clear text over the Internet. This document will provide guidance to CAs at firms or in industry on securely sending information to clients or others.

Percentage of CAs who email confidential information to clients

	Send by email	Sometimes uses passwords	Always use passwords	Sometimes encrypt	Always encrypt
Financial Statements	70	29	16	14	11
Other financial information	77	30	13	16	10
Personal tax returns	66	25	22	14	15
Corporate tax returns	61	27	19	15	15

1 The survey was conducted by the International Innovation Network (INN). See **http://bit.ly/SzC9E9** for more details.

This publication was originally published by The Canadian Institute of Chartered Accountants in 2012.
It has been reissued by Chartered Professional Accountants of Canada.

Confidentiality: A Professional Responsibility

Accountants are seen as trusted advisers and competent professionals by their clients and employers and must put in place controls to preserve the trust of those who depend on them. Furthermore, accountants are required by the professional code of conduct to ensure that sufficient controls are in place to protect their clients' information. According to the Rules of Professional Conduct, *"Members have a duty of confidentiality in respect of information acquired as a result of professional, employment and business relationships.... A member, student or firm shall not disclose any confidential information concerning the affairs of any client, former client, employer or former employer."*[2] In summary, accountants have a responsibility to protect the information they are entrusted with.

From a liability perspective, no practitioner has been sued to date for having their emails intercepted by an unauthorized user. However, accountants have been sued in situations where they have taken the responsibility for delivering tax information (e.g. SR&ED tax claims) or payroll remittances to CRA, where the information got lost or was delayed.

Beyond the liability perspective, practitioners should also consider the potential loss of trust from clients. According to Malcolm D'Souza of the Association of Insured Chartered Accountants Services Inc, accountants have advised him of cases where clients were disgruntled when they found out that their information was stored in an unprotected manner (i.e. no password protection or encryption) on computer equipment that was stolen.

Reputational Impact on CAs of a Potential Breach

If confidential information emailed to a client were to be intercepted and exposed, it could have a negative impact on the profession as a whole. Businesses and individuals that rely on CAs for accounting, tax and other advice may feel that their information is not safe with their accountants. CAs enjoy a position of trust and confidence with clients and must do all that they can to protect this trust by attending to such issues. Consequently, accountants cannot risk the wider public losing confidence in CAs, which will undermine the brand reputation of the profession as a whole.

Client Confidentiality: A Risk-Management Perspective

Establishing confidentiality controls begins at the client acceptance stage. Some clients may prefer the convenience of receiving their documents in clear text via email, but they should be made aware of the risks. Practitioners should include as a part of their standard engagement letter wording that makes the client aware that files sent in an unencrypted format may be intercepted.

Within the firm, a comprehensive security and privacy awareness program should be implemented to ensure all personnel who have access to firm systems (administrative staff, junior staff, partners, contractors, etc.) are educated about the cyber risks associated with emailing. For example, such awareness sessions, alerts, etc. should make personnel aware of the prohibition against sending personally identifiable information (e.g. social insurance numbers) or other sensitive information by email. Personnel should also be made aware of best practices when emailing. For example, they should check prior to sending an email that the right recipient is being sent the right document and they do not accidentally divulge confidential information to the wrong individual or entity. Data-loss prevention tools that can plug into email systems do exist to prevent the accidental divulgence of

2 See the Handbook: CI 208 — Confidentiality of Information

specific types of information (e.g. they can block the transmission of emails that contain social insurance or credit card numbers, etc.). However, the costs of such tools are significant and may not be feasible for smaller firms.

Securing Documents Sent: What Are the Options?

Although email has been around for decades, a standard to securely exchange emails has yet to emerge. Consequently, the challenge for the profession is to determine which solution safeguards client confidentiality, but is also practical to use for both the client and the firm itself.

Pretty Good Privacy (PGP) Encryption for Email

PGP encryption can be used to encrypt the entire email sent by firm personnel to the recipient. The system uses public key cryptography infrastructure (PKI) to encrypt and decrypt email, where the client's public key can be used to encrypt the email and its contents—and only that individual can decrypt that email using their private key.[3] PGP can be installed into Thunderbird email client (as explained in this article[4]) or it can be purchased from a company (e.g. Symantec[5]).

Pros: Allows for full encryption of email sent; PGP is a well-established protocol.

Cons: Requires a significant amount of set-up/configuration effort to implement PKI (for both firm and the client); may be difficult for the client to decrypt such an email.

Other considerations: Vendor selection, reputation of the firm, cost of implementation, and other software acquisition issues.

File Encryption

Office productivity software, such as Microsoft Word, Excel and Adobe Acrobat, often has the ability to encrypt individual files. To decrypt the file the client must enter the password. Practitioners can alternatively use file compression software, such as the open-sourced 7-zip, which has AES 256 bit encryption to send any file format to their clients.[6]

Pros: Free and easy to use for both the firm and client.

Cons: Managing client passwords is significantly challenging. Clients must receive their passwords in a secure format (i.e. via a channel other than email, such as a text message or verbally over the phone). It may also be necessary to resend the file or password if the client forgets the password.

Other considerations: Using the client's SIN as the password can overcome some of the password management issues described above. However, the SIN is a sensitive piece of information that is not suited to be a password since it only contains numeric values. Best practice is to use a passphrase, which includes a combination of upper case and lower case letters as well as numerical values and special characters.

3 http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy

4 http://lifehacker.com/180878/how-to-encrypt-your-email

5 http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-pgp_desktop_email_DS_21158806.en-us.pdf

6 http://www.7-zip.org/7z.html

File-sharing Services

Some Software-as-a-Service (SaaS) providers are in the market for sending files that are too large to be sent by email. Such SaaS providers may also offer encryption services. For example, yousendit.com and sharefile.com (which is owned by Citrix) offer these services. However, since these are SaaS providers, practitioners should be aware that this is actually an outsourcing arrangement. Consequently, they need to obtain from these providers a report that provides assurance that the controls relevant to the firm are operating effectively. For example, yousendit.com claims to have a SOC 2 Type II security audit performed,[7] while sharefile.com has an SSAE 16 audit performed on its data centres.[8]

Pros: Easy for both practitioners and clients to use.

Cons: Reliant on a third party to keep confidential client information safe; client information can be accessed by law enforcement (potentially in a different country) without warrant; audit reports may not be granular enough to give the assurance that the practitioner requires.

Other considerations: Maintaining local backups, outsourcing best practices (e.g. assessing vendor reliability, establishing service level agreements, service monitoring, assessing relative merits of software against other software, etc.).

Portals

Accountants can also use client portals. Examples of client portals include: CCH,[9] Thomson Reuters[10] and others.[11,12] The portals provide a client-dedicated site for practitioners to upload files that are only accessible to the client. The client can download the files securely from the site. These services, like the file-sharing services noted above, are SaaS-based services. Consequently, practitioners need to deal with reputable companies who can provide an audit report over their controls. Firms can maintain their own portals, such as the one provided by DOC. IT,[13] but this requires the firm to have access to IT staff who can adequately maintain and secure the server (e.g. patch it, protect it from viruses, unauthorized access, hardening, etc).

Pros: Ease of use; portals are designed to be used by accountants and their clients.

Cons: Can be difficult to maintain (e.g. may be missing maintenance features, such as the ability to mass-delete data related to clients who are no longer with the firm).

7 http://www.yousendit.com/security-overview

8 http://www.sharefile.com/industries/Business/security.aspx?src=unknown&v=e&cat=1

9 http://www.cch.ca/AccountantsSuite/CCHPortal/Index.aspx?tid=133

10 cs.thomsonreuters.com/portals

11 This article http://www.journalofaccountancy.com/Issues/2010/Feb/20092359.htm provides some other vendors that offer this service.

12 Disclaimer: These examples are provided for illustrative purposes only. CICA and the authors of this document have not performed any due diligence on these vendors and do not implicitly or explicitly endorse any vendor or service listed here or throughout the publication.

13 http://www.doc-it.com/phocadownload/productinformation/docitportal.pdf

Other considerations: Outsourcing best practices (listed above), resources required to maintain/secure on-premise hardware/software, trade-off between cost and ease-of-use (e.g. more expensive solutions may require less ongoing effort/resources).

About the Authors

Malik Datardina, CA, CISA, is an independent consultant in the field of information systems risk and assurance, specializing in information security governance and data analytics. He is a technical consultant for CICA's Information Management and Technology Advisory Committee.

Claudiu Popa, CISSP, CIPP, PMP, CISA, CRISC is the principal Risk Advisor and CEO of Informatica Corporation, a Toronto-based management consulting firm recognized for innovative data protection solutions. He is one of the leading security and privacy consultants in Canada, a published author and frequent media resource on all things related to cybercrime, compliance and emerging threats to the personal information of Canadians.