Business Matters

FEBRUARY 2020

VOLUME 34 | ISSUE 1

DIGITAL MANAGEMENT

Cyber Security: Mitigating the Risks to Cyber Attacks

Cyber attacks come in a variety of forms and with a variety of intensions. Whether for money or pure disruption, organizations are at risk of both the intrusion and the potential breach of regulatory obligations.

Identifying cyber risks

While there are many different types of cyber threats, the following are the most common five encountered:

1. **Phishing:** A ploy that utilizes misleading emails in an attempt to get a user to follow a link to a website designed to infect the user's PC or ply away personal information.
2. **Malware:** A generic term that refers to many forms of malicious software. This includes viruses, Trojans, worms, ransomware and spyware. Each of these serves to gain access to a target's system and disrupt normal activity, steal sensitive data, and/or hold access for ransom.
3. **Data breaches and man-in-the-middle:** Data is either stolen directly from unwanted access or intercepted during transmission between two parties.
4. **Denial of service:** Attacks that are targeted at such specific things as hardware, applications or websites in order to disrupt their use.
5. **Internet of things device attack (IoT):** Where corporate devices are connected via the internet, there is opportunity for these connections to be exploited and for data to be stolen.

Nearly 90% of cyber incidents are phishing attacks. While the technological maturity level of an organization can greatly influence the response rate, statistics show that upwards of 30% of the targets of a phishing attack open the malicious emails. Up to 12% were found to take the next step and open the included website or attachment. As a result, your user-base is often one of the weakest points in your environment.

Getting on the right track

Organizations can significantly reduce their cyber risk with the implementation of a consistent IT methodology with security in mind. Start by taking an inventory of your organization's hardware and software. By simply removing unsanctioned hardware and software from access to your network, you immediately improve your defenses. Manage this going forward by restricting the administrative privileges needed to install new applications and to configure hardware options.

As part of your IT methodology, establish a consistent configuration base of all your devices. Add rigour to how these units are configured, and ensure that proper security protocols are used. In many cases, simply making changes from the manufacturer's default settings will help reduce exposure. Once you have established your configuration, employ change-control procedures to assess and monitor their upkeep. Work in a regular patching process to ensure that all your devices are up to date with the latest changes from the manufacturer, which often include security improvements. Many attacks focus specifically on out-of-date software versions.

As discussed earlier, many attacks are buoyed by fooling users into clicking a dangerous link or downloading malicious applications. As such, do not underestimate the importance of educating your user-base. Be sure to highlight what to look for, enforce a critical thinking approach, and reassess as needed. Phishing email drills can be very eye-opening and can help to reinforce preparedness.

Getting the right help

Cyber security is an increasingly complex and important topic. As such, it is often difficult for smaller organizations to stay on top of their security needs. They may not have the proper in-house skills to set the right IT methodology in place or manage it going forward. There is certainly a cost benefit consideration to hiring the needed technical help versus bringing it in externally.

Do not hesitate to look for help. There are numerous consulting companies that can be engaged to conduct an initial cyber security review or assessment of your current environment. These companies can either direct you as to where to make the most important improvements or take over the responsibility as part of an outsource agreement.

Responsibility to protect

Currently in Canada, it is not against the Criminal Code to fail to implement cyber security measures. However, there are a number of civil and liability obligations that are relevant. Most notably, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) is relevant to all personal information involved in commercial activities. PIPEDA calls for the protection against loss or theft, modification, copying, unauthorized access, or even disclosure of personal information. This means that the organization itself has a duty to protect the data in its realm.

PIPEDA is not the only regulatory component to be concerned with. Several provinces have passed similar legislation that require the keepers of data to safeguard this information. Various industry regulators have also implemented regulations around not only the protection of data but also the reporting of intrusive events. For example, the Canadian Securities Administrators (CSA) requires market participants to implement a security framework (relative to their scale).

Cyber attacks are a part of the new reality in our increasingly connected commercial paradigm. Your industry, your scale and the sensitivity of your data will dictate how much you need to do to mitigate the inevitable intrusions. The basic steps above will help to reduce simple or widespread cyber attacks. However, do not underestimate the importance of an effective IT methodology to fully mitigate risks associated with cyber attacks.

FINANCE

Your Credit Score – What Does It Mean?

We've all received email ads for websites that can help us find our credit score, with monthly updates, for free. It's little wonder that many Canadians are now fixated on that three-digit number. Surely a good credit score means that you are on the right path to financial security, right?

Unfortunately, no! A high credit score is no guarantee that you will not face financial difficulty, or even bankruptcy, in the future. There are many misunderstandings about what the credit score is, what factors affect it and who it was developed for (hint: it's not you).

What is a credit score?

Credit scores are a product developed by credit bureaus to sell to banks and other lenders as well as insurance companies. They are portrayed as a "measure of trust" – that is, a higher credit score provides lenders with more confidence that you will pay them back. Lenders are primarily interested in maximizing their profitability, which depends on you carrying balances and paying interest as well as paying them back. What's in their best interest is not necessarily what's in yours.

The credit bureaus access data from your financial institutions and phone and utility companies. They then apply their algorithms to come up with a three-digit score. Credit scores from different credit bureaus can be different, as they weigh the importance of certain factors differently or use different time frames for your credit history.

What factors affect your credit score?

The most important factor that affects your credit score is your repayment history, accounting for 35% of your score. To have a high score, it is important that you make all required payments on time. However, you get no benefit for paying the balance in full or for making extra payments against a debt. Nor are all payments tracked; for example, faithfully paying your rent on time will not improve your credit score.

Your credit utilization (i.e., the ratio of your credit card balance to your credit limit) accounts for 30% of your score. It is meant to track whether you are getting close to "maxing out" your available credit, which will make you a riskier customer for a new lender. It is suggested that you maintain a balance of no more than 30% of your borrowing limit. Credit utilization only applies to "revolving credit," such as credit cards and lines of credit. It doesn't apply to instalment loans, such as mortgages or car loans. Perhaps surprisingly, your credit score does not take into account your salary or other sources of income, though this may be considered by lenders when they determine your credit limit.

The credit score rewards those with a longer credit history, which accounts for 15% of your overall score. It considers the age of your oldest account as well as the average age of all your accounts. It also rewards you for having multiple sources of credit, such as credit cards, car loans and mortgages. This credit mix accounts for 10% of your score.

The number of credit enquiries can impact your credit score. These are distinguished between soft enquiries for non-lending purposes (e.g., by you or a potential landlord) versus hard enquiries (e.g., when you are applying for a mortgage or loan). Isolated hard enquiries will not likely raise any red flags. However, if you apply for a lot of credit in a short period of time, lenders may get concerned that you are shopping for loans and potentially getting in over your head. Other factors that may affect your credit score include your personal stability (e.g., if you move frequently) and your professional stability (e.g., if you change jobs frequently).

It may seem counterintuitive, but paying off your car loan or mortgage or closing an old credit card that you no longer need could have a negative impact on your credit history and credit mix, which may actually reduce your credit score.

These algorithms may result in a scenario where a person who is unemployed, behind on their rent, and has a seven-year car loan that is "underwater" (i.e., the remaining balance on the loan exceeds the current value of the car), but who makes the minimum payments on their credit card every month, could have a *higher* credit score than someone who has paid off their mortgage years ago and has just one credit card that they pay off in full every month.

How can you improve your credit score?

Once you understand the factors that do and don't affect your credit score, you can assess whether some of the common suggestions for improving it are in your best interests or in the best interests of the lenders. Obviously, making sure that you make all minimum required payments on all your debts is important to maximize the payment history.

There are several ways that you can keep your utilization rate under the 30% target. You might consider making multiple payments during each month if you have a significant purchase, or if you are approaching the target because of regular charges throughout the month.

Two methods that are often suggested, but should be approached with caution, are to ask for an increase in your credit limit or to take out an instalment loan to pay down the balance on a credit card (which could also have a positive effect on the credit mix factor). Both methods come with the risk of additional borrowing if you are not disciplined about managing your finances. It's also worth noting that carrying credit card balances of up to 30% of your credit limit means that you will be paying a significant amount of interest each month.

You could improve your credit history by taking out longer loans, but, like many of the other suggestions, this will result in you paying more interest to the banks.

It is important to know your credit score and to check your credit report from each of the credit bureaus annually to ensure that there are no mistakes. Just remember that the credit score was developed by and for lenders, and that it was not designed as a measure of your personal financial health. And those free services with monthly updates? They make money by recommending financial products to consumers, for which they receive a referral fee. Some even have "coaches" to provide personalized tips to improve your credit score and offer product recommendations. So, if you receive a recommendation to get a consolidation loan to pay down your credit card balances, remember that that's how these services make money. Don't focus on improving your credit score by making decisions that are in the lenders' best interest and not your own!

MANAGEMENT

Protecting Your Business From Identity Theft

When we think about fraud committed against individuals, many of us immediately think of identity theft. Identity theft is the taking of a victim's private information (such as their social insurance number or birthdate) to use for financial gain. Examples of identity theft include applying for and using a credit card with the stolen information. Our awareness of identity theft as a crime has increased significantly over the past few years, because the issue has been regularly featured on the news and in popular culture, and the risks have been frequently highlighted by financial literacy organizations (such as CPA Canada).

What is business identity theft?

Though many people are well aware of the risks of individual identity theft, what is not as commonly known is that identity theft can just as easily happen to a business. Identity theft for a business has the same definition as for an individual: acquiring a business's private information to use for financial gain.

Why does business identity theft happen?

Any person(s) committing fraud, including identity theft, will typically need to have all three of the following factors: incentive, rationalization and opportunity. These factors are, in fact, more commonly present when committing business identity theft for the following reasons:

1. **Incentive:** A business will typically have access to a greater amount of money than an individual. This includes corporate bank accounts, credit cards and access to large loans from banks. Therefore, the financial incentive for committing business identity theft is higher.
2. **Rationalization:** A person that will commit any fraud, including identity theft, will typically need to convince themselves it is ok to commit this crime. This is much easier to believe when the crime is committed against a business, which can be viewed as an entity and not an individual and, therefore, cannot be personally hurt by the act.
3. **Opportunity:** Finally, a person that intends to commit identity theft needs the opportunity to acquire key information. For a business, this key information is more likely to be publicly available on a company website and/or social media accounts and, therefore, easier to acquire.

What information is needed to commit business identity theft?

For individual identity theft, a person's social insurance number (SIN) and birthdate are key pieces of information to acquire. For a business, the key information to protect against identity theft is your company's business number (BN) and/or provincial tax identification number. In Ontario, that would be your Business Identification Number (BIN). Other key information that may be used for business identity theft include:

- legal corporate / business name
- mailing address
- supplier names
- customer names
- employee information (e.g., email addresses and phone numbers)

What are examples of business identity theft schemes?

There are several ways in which a business identity thief can use the acquired information for financial gain. Examples include:

- transferring funds out of the business bank accounts
- opening and using a corporate credit card
- applying for and receiving a loan from the bank
- making large business purchase orders
- filing false tax returns to receive refund amounts from the government

What are the consequences of business identity theft?

The consequences of identity theft for a business, much like for an individual, is lost time and money. Examples include:

- loss of revenue and cash from the business if fraudulent purchases are made
- reputational damage if the fraudulent use of the business's identity is carried out in ways that are antithetical to the business
- tax liabilities to the government if fraudulent corporate tax returns are filed

How can businesses mitigate the risk of identity theft?

To mitigate business identity fraud, there are both preventative and detective actions that can be taken. Preventative actions help to protect against the theft occurring in the first place. Detective actions help to discover the business identity theft before significant losses have occurred.

Preventative measures

1. Protect your BN as you would protect your individual SIN. Only provide this number to approved and authorized employees, customers, suppliers or third parties (such as the CRA).
2. Restrict access to key websites. For example, only authorized individuals should be allowed administrative access to the company website, online accounting software or CRA business account.
3. Use strong passwords / passphrases for access to key websites, and change these on a regular basis (at least annually).
4. Protect your business banking information when making or receiving electronic payments. For example, do not make an online supplier payment on a public computer / browser, such as at the business center of a hotel.
5. Review all public information for your company, specifically on the company website and social media accounts. Make a list of key identifiers (such as mailing address and legal corporate name), and evaluate the purpose of having this as publicly known information. Remove this information from any websites and/or social media accounts if it serves no benefit to the company to have it public.

Detective measures

1. Review and reconcile all corporate bank and credit card accounts on a regular basis (at least monthly).
2. Review your business credit reports on a regular basis (at least monthly). The four nationwide credit reporting bureaus in Canada are Equifax, Experian, TransUnion and Dun & Bradstreet.
3. Review your business tax account (made available by the CRA) on a regular basis (at least monthly).

TAXATION

Tax and Ethics

Tax practitioners help their employers and clients to understand and meet their tax compliance obligations, and to know what tax planning opportunities may be available to them. These opportunities can range from illegal tax evasion schemes to those that are merely taking advantage of tax incentives in the manner that the government intended. In between those two extremes is a grey area. The General Anti-Avoidance Rule (GAAR) was introduced in 1988 to address this grey area by distinguishing between legitimate tax planning and abusive tax avoidance.

Understanding where the line is between legitimate tax planning and abusive tax avoidance is critical, as the latter can be costly due to third-party civil penalties for preparers, gross negligence penalties for clients and potential reputational damage for both. Tax planning and tax compliance activities can also raise unique ethical issues for CPAs.

All CPAs are required to adhere to the CPA Code of Conduct ("Code"), called the Rules of Professional Conduct in some provinces. To understand how the Code applies to specific situations encountered by tax practitioners, it is helpful to consider each of its fundamental principles:

- professional behaviour
- integrity and due care
- objectivity
- professional competence
- confidentiality

Professional behaviour

CPAs must conduct themselves, at all times, in a manner that will maintain the good reputation of the profession and protect the public interest. In particular, CPAs must consider whether any tax planning opportunities with which they may be associated might bring them, and the profession, into disrepute.

Integrity and due care

CPAs must act honestly in all dealings with their clients, tax authorities and other parties, and do nothing knowingly or carelessly that might mislead either by commission or omission. They must also ensure that their staff have appropriate training and supervision.

The Institute of Chartered Accountants of England and Wales issued guidance in the Professional Conduct in Relation to Taxation report (**www.icaew.com/en/technical/tax/pcrt**) that "[a] member who has reason to believe that the proposed arrangements are, or may be, tax evasion must strongly advise clients not to enter in to them. If a client chooses to ignore that advice, it is difficult to envisage situations where it would be appropriate for a member to continue to act other than to rectify the client's affairs."

In addition, practitioners who believe that they are being asked to use a statement that is clearly false or highly suspicious when preparing tax returns or other filings should consider withdrawing from the engagement, particularly if they want to ensure that they won't be subject to third-party civil penalties. These penalties were introduced into income and excise tax legislation to apply to those who counsel others to file their returns based on false or misleading information, or to those who turn a blind eye to false information provided by their clients for tax purposes. Two penalties are possible: one for tax promoters and one for tax preparers. These penalties are not intended to apply when there are honest mistakes or when there are differences of opinion where there is bona fide uncertainty.

Objectivity

Relationships which unduly influence or bias the professional judgment of the member must be avoided. If practitioners receive a commission or other financial incentive from a third party relating to a matter upon which they are advising the client, they must ensure that the remuneration does not compromise their objectivity, and they must disclose the compensation arrangement to the client.

Professional competence

CPAs have a duty to carry out their work with requisite skill and care. At the 2019 The One Conference, there was a joint presentation by CPA Canada and the administrator of the professions professional liability insurance programs, where they identified that almost 60% of the number of liability insurance claims from 1999 to 2019 were a result of taxation services, accounting for almost 40% of the claims paid. The most common reason for those claims was a lack of expertise – that is, errors due to practitioners advising on technical tax matters when they did not have adequate experience or knowledge. Other common reasons included a lack of attention to detail, such as missing filing deadlines and lacking relevant documentation. CPAs should consider obtaining second opinions on significant matters and seeking assistance from suitably qualified specialists when appropriate. For more information on how practitioners can help reduce risk in their tax-related practice, please refer to CPA Canada's comprehensive *Tax Risk Management Guide*: **www.cpacanada.ca/en/business-and-accounting-resources/taxation/corporate-tax/publications/evaluate-tax-risk-in-your-practice/tax-risk-management-guide**

Confidentiality

CPAs can only disclose confidential client information without the client's consent when there is an express legal or professional right or duty to disclose, such as complying with anti-money laundering legislation or practice inspection by their CPA body. When CPAs withdraw from engagements, they have a duty to respond promptly to communication from a successor member or firm as to whether there are any circumstances that might influence their decision to accept the engagement. In these cases, practitioners

should state that there are such circumstances but that they cannot disclose them without the client's permission. Further, CPAs cannot inform the Canada Revenue Agency due to the confidentiality requirement, but there may be a legal duty to report schemes that involve suspicious transactions or large cash transactions under anti-money lending legislation (visit **www.fintrac-canafe.gc.ca/re-ed/accts-eng%20** for further details). When confidentiality is in doubt, the CPA should consider obtaining legal advice.

CPAs who accept payment to prepare more than 10 tax returns in a calendar year are required to file personal and corporate tax returns electronically, with some limited exceptions. They must file these returns as an agent for the taxpayer, and the client must review and approve the tax filings before they are submitted. It is critical that the practitioner ensure that authorization forms are completed and that there are appropriate controls over the filer's access credentials. While there is no requirement to verify the information provided by the client, CPAs should not be associated with the presentation of facts that they know (or should have known) to be false or misleading, or to assert tax positions in the filing that they consider to have no sustainable basis.

As with any ethical matter, CPAs can consult with the Member Advisory Services at their provincial body for guidance on application of the Code.

Learn how to apply key concepts in ethics to issues you face every day in your tax practice and hear from a wide range of tax practitioners about their experiences with accounting ethics through CPA Canada's online Ethics and Tax course: **www.cpacanada.ca/en/career-and-professional-development/courses/leadership-management/business-ethics/ethics-and-tax?_ga=2.210863441.512533157.1579018234-1870218406.1548793286**

BUSINESS MATTERS is prepared bimonthly by the Chartered Professional Accountants of Canada for the clients of its members.

Authors:

Cyber Security: Mitigating the Risks to Cyber Attacks	Cory Bayly, MBA
Your Credit Score – What Does It Mean?	Susan Cox, CPA, CA
Protecting Your Business From Identity Theft	Garth Sheriff, CPA, CA, CPA (Illinois), CIA, CGMA, MAcc
Tax and Ethics	Susan Cox, CPA, CA