CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Information Security Insights From and For Canadian Small to Medium Sized Enterprises

Paying Attention to Information Security

CPA Canada recently completed an online study conducted by Nielsen called *Information Security for Small and Medium Enterprises*. With a focus on SME practices, it surveyed basic aspects of the IT security of 398 accounting professionals (the margin of error is +/- 4.9%, 19 times out of 20), providing revealing insights into the state of data protection across a diversity of sectors.

The study results are summarized and augmented with suggested questions and resources in CPA Canada's publication *Defence Mechanisms: How Canadian SMEs Are Dealing With Information Security*. In comparing the practices and priorities of Canadian accounting firms with those of non-accounting firms we found that most firms share similar concerns about IT security and the associated risk of data breaches.

How Canadian Businesses See Security

Peering into the IT security practices of Canadian companies has traditionally been challenging due to limited legislative guidance and the natural tendency of small and medium-sized organizations to control their own information.

This year, CPA Canada tackled the challenge by commissioning Nielsen to complete an important study entitled *Information Security for Small and Medium Enterprises*. Based on interviews with CPA Canada members, the results yield rich new insights into the way Canadian businesses *like yours* manage risk, implement security and adopt new technologies.

So what do we know about how you deal with information risk?

You care about information security

CPA Canada members in small and medium enterprises don't just want to protect assets for the sake of security. They are genuinely concerned about safeguarding information owners and their data in the face of evolving cybersecurity threats.

You have adopted good security practices

Many Canadian companies have basic practices such as backing up data and using strong passwords. Although they are by no means sufficient for ensuring cybersecurity, many IT security practices focus on prevention.

You recognize security problems

More than four out of 10 respondents know that they have experienced a security breach, which indicates a high level of awareness of information security risks. Detection of security breaches — either by proactive or reactive means — is a key step towards awareness and the adoption of proper practices.

Information Security
Synonymous with data security, it is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g., electronic, physical).

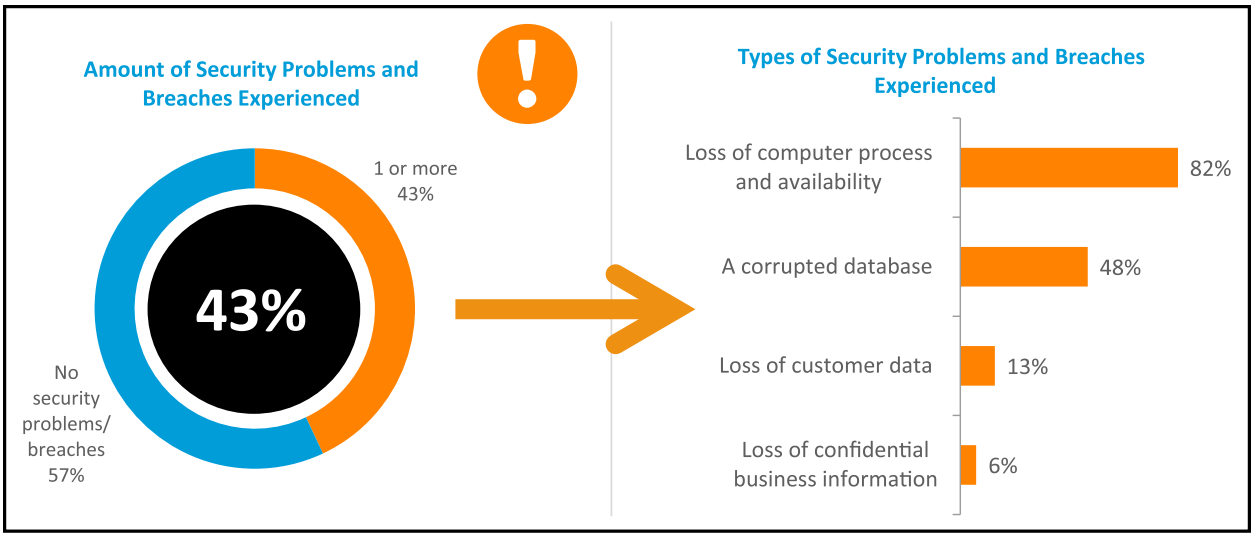
Cybersecurity
Cybersecurity, often used interchangeably with *computer security* and *IT security*, is a broad term that describes protection from and defense against attacks from cyberspace.

What Security Concerns Do SMEs Have?

Cybercrime tops the list of concerns that respondents have: 72% are concerned about having their business data hacked and stolen, which is not surprising given the malicious data breaches in recent news headlines. Roughly two-thirds (66%) are concerned about having intentional errors or corruptions of their business data and systems, while 61% are concerned about having their website or other systems crash and 50% are concerned about having their website or other systems attacked.

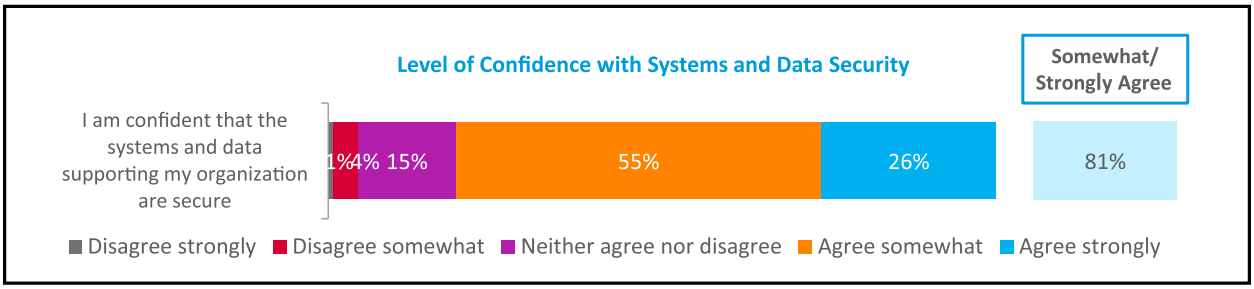
Are their concerns justified? Almost half (43%) of businesses reported security incidents, and more than 80% of these firms reported that at least moderate resources (cost and effort) were required to recover from the damage, which included:

1. loss of computer usability or availability
2. corrupted database information



How Are Canadian Firms Managing Security Risks?

Surprisingly, confidence is one of the key metrics determining the preparedness of Canadian companies to address security concerns. The vast majority of Canadian respondents (81%) indicate they have confidence in the IT security of their organization, even when these practices are very basic and provide inadequate protection.

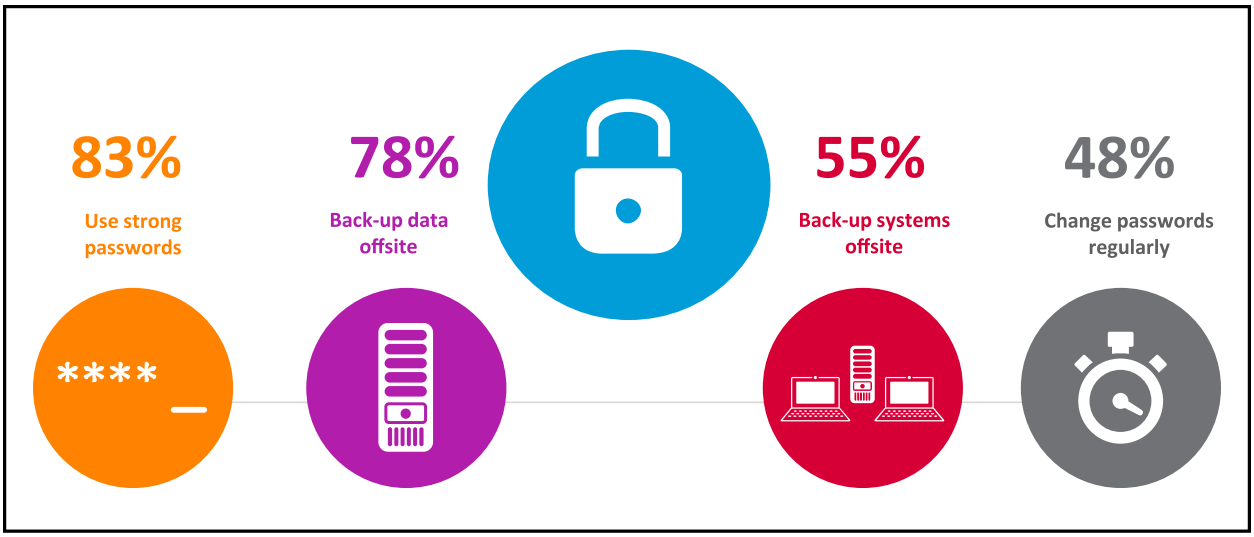


What does the confidence of Canadian SMEs have to do with the effectiveness of their cybersecurity? Results indicate that those confident in their approaches are also more likely to:

1. have more IT security safeguards in place
2. check their IT security safeguards more often
3. have a dedicated person responsible for information security

But confidence alone will not protect you and your business. The top IT security measures followed by Canadian organizations reveal some basic best practices. CPA Canada recommends that all members adopt these security practices:

1. the use of strong passwords
2. off-site data backups
3. off-site system backups
4. regular password changes

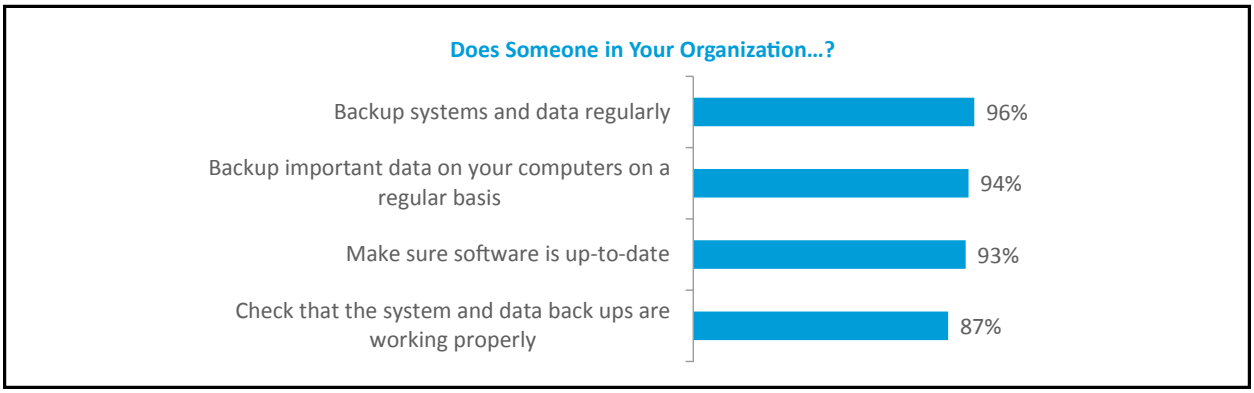


Asking the Right Questions About Security Makes Good Business Sense

Our research indicates that just over six-in-ten (61%) of small and medium enterprises use external IT resources. Knowing what to ask of your IT and security providers will not only save you time and money, but it can also save your business. Here are the top five questions that are deemed most relevant to the majority of Canadian firms:

1. We run a very lean operation with limited resources. Can we protect our data in-house without breaking the bank?

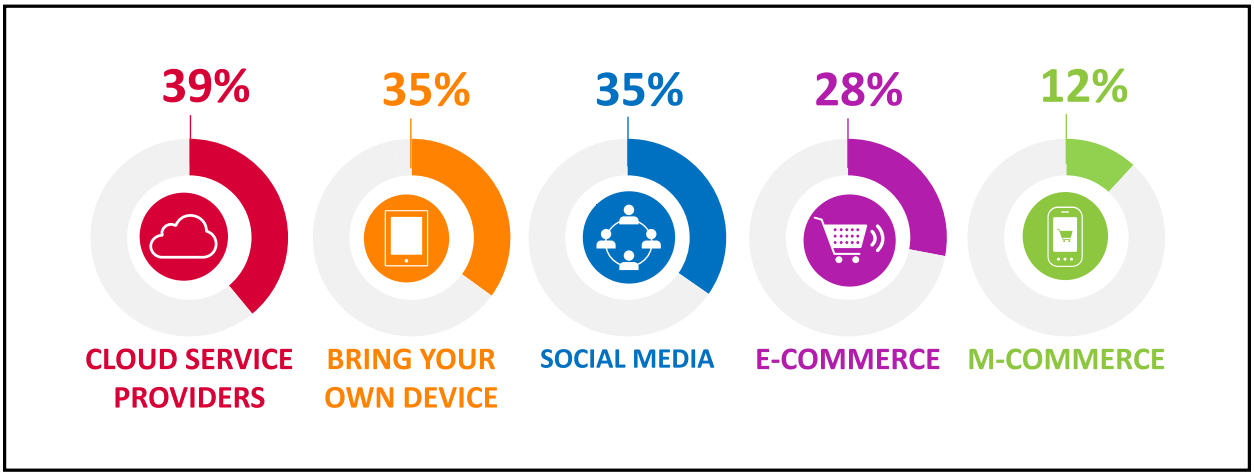
There are relatively easy and inexpensive measures that you can take in-house to protect your data that are a good start. Below are measures that over four-out-of-five SME respondents reported that their organizations are taking to help protect their data.



In addition, over six-in-ten respondents reported that their organizations review user account privileges periodically (62%) and review user accounts periodically (61%).

2. We are small, nimble and innovative. What should we know about technologies such as the cloud, social media and mobile commerce?

You are not alone. Between 12% and 39% of Canadian businesses currently use such innovative solutions. Exploit new technologies for your business but be sure to ask your trusted IT and security pros about ways to secure these emerging technologies.



3. We only found out about our last security incident because something stopped working. How can we detect a hacking attack or data theft?

Your network should be properly designed and environment segmented to support data storage according to sensitivity. That is, your network should have one gateway (connection) to the internet and this should be a firewall. Most SME level firewalls today can also filter out 'bad' internet traffic and provide Virtual Private Network (VPN) service to allow your employees to access the LAN and internal systems securely. If you have very sensitive data inside your LAN, you can also 'cordon off' a part of the LAN, much like a restricted office space using another firewall. Don't panic! Understand the concept, and ask IT or information security professionals for help with all of this. Depending on your business practices, industry sector and cybersecurity measures, your adviser may describe potential hacking scenarios and suggest ways to recognize when a security incident has occurred.

An authoritative resource to consult is the *Canadian Privacy and Data Security Toolkit*, a CPA Canada publication designed specifically to address the needs of small and medium-sized businesses. It discusses intrusion detection and prevention and suggests that to maximize your chances of discovering a breach, you must rely on people, processes and technology:

- your people should be trained to recognize and report security problems
- your processes must be able to detect suspicious activity
- your technology should monitor systems for evidence of incidents

4. If we discover a breach, what should we do?

Much depends on the type and circumstances of your security or privacy incident. The type of access control (passwords or multifactor authentication) will also play a part. If it's possible that personal information has been compromised, you may be advised to leave the crime area untouched to facilitate a forensic investigation. You can contact the Office of the Information and Privacy Commissioner of Ontario or the Office of the Federal Privacy Commissioner to make a report and ask for more guidance. You can also contact the Canadian Anti-Fraud Centre to report Internet-borne cybercriminal activity and other types of computer-based mischief.

5. What are some other sources of information about security and privacy for SMEs?

Your adviser may suggest information sources specific to your sector, business focus and preferred degree of technical detail. You should also consider the following resources:

- *The Canadian Privacy and Data Security Toolkit* (**CAStore.ca**)
- *Securing Personal Information: Self-Assessment Tool* (**Priv.GC.CA**)
- *Information Systems Security Compliance (search on* **CPACanada.ca**)
- *IT Security Practices* (search on **CPACanada.ca**)
- *Cyber-security Opportunities for Smaller Accounting Firms* (contains a glossary of security terms used in this publication and additional references; search on **CPACanada.ca**)

Author: Claudiu Popa