CANADA'S NEW CYBERSECURITY CERTIFICATION GOES LIVE

Posted on October 13, 2020

Categories: Insights, Publications

The federal government has officially launched the CyberSecure Canada ("**CyberSecure**") online portal.

In mid-August, the voluntary CyberSecure program was introduced to help small and medium-sized organizations implement cybersecurity measures to protect against cyber threats.[1] At the time, the program was in a pilot phase and businesses were only able to sign up as "early adopters" to test the certification process. The program is now open to all eligible businesses.

Participating businesses can improve their cybersecurity with the help of CyberSecure by first adopting the baseline set of security requirements and then completing the certification process.

The baseline security requirements are intended to be simple and affordable steps businesses can take to mitigate or prevent the most common cyber threats. These requirements include, among others, implementing employee awareness training and an incident response plan.[2]

The certification process determines whether businesses have properly adopted the program's requirements. The Standards Council of Canada conducts the evaluation through accredited third party organizations. Once certified, businesses can display a mark on their website or other promotional materials to demonstrate their compliance with the CyberSecure program.

The government hopes the release of this program will promote resilience for Canadian businesses and trust from their consumers and suppliers, ultimately helping those businesses maintain global competitiveness in the digital age. The release of the program is in line with the goals set out in Canada's National Cyber Security Strategy and the Digital Charter, released earlier this year.[3]

Key Takeaways for Businesses

While the CyberSecure certification is voluntary, many organizations are required by applicable privacy legislation – including the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") – to implement appropriate security safeguards to protect personal information against loss, theft or unauthorized access, disclosure, copying, use or modification. Accordingly, organizations with well-developed and mature privacy and cybersecurity programs have likely already met, if not exceeded, the baseline security

requirements needed to demonstrate compliance with the CyberSecure program.

The increased reliance on technology during the ongoing global pandemic has made businesses more vulnerable to cyberattacks. A robust and up-to-date cybersecurity program is therefore more important than ever, particularly for businesses that have migrated sales or other functions online and/or have employees who are working remotely on personal equipment or using less secure personal networks.

Achieving compliance with the CyberSecure program is one way that an organization can turn its mind to protecting against the increased threat of cyberattacks.

by Kristen Pennington and Ouvedi Rama Naiken (Articling Student)

[1] For more information about the initial launch, see McMillan's article on the certification program.[ps2id id='1' target='/]
[2] The full list of cybersecurity controls can be found here.[ps2id id='2' target='/]
[3] See McMillan's summary of the Digital Charter.[ps2id id='3' target='/]

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.