August 15, 2019

ARTICLE

Ready, Set, Certify – Canada's New CyberSecure Canada Certification Program

On August 12, 2019, the Canadian federal government announced CyberSecure Canada, a voluntary certification program to help small and medium enterprises ("SMEs") achieve a baseline of cybersecurity. SMEs that demonstrate compliance with specified baseline cybersecurity controls, based on an audit by an accredited certification body, will be granted a two-year certification and be entitled to use the CyberSecure Canada logo.

Cybersecurity for SMEs

Cybersecurity is important for organizations of all kinds and sizes, including SMEs. Cyber criminals are increasingly targeting SMEs, including to obtain information about their customers and business partners and to access the systems and data of their business partners. Cyberattacks can cause SMEs to suffer potentially devastating financial losses and liabilities. However, comprehensive cybersecurity programs can be expensive and time consuming to implement and beyond the financial and human resources means of many SMEs.

In March 2019, the Canadian Centre for Cyber Security issued a guide titled *Baseline Cyber Security Controls for Small and Medium Organizations* to provide a condensed set of advice and guidance to help Canadian SMEs maximize the effectiveness of their cybersecurity investments. The guide reflects the view that organizations can mitigate most cyber threats through awareness and best practices, and can successfully apply the 80/20 rule – achieve 80% of the benefit from 20% of the effort – in the cybersecurity domain. The guide recommends SMEs implement thirteen baseline security controls: (1) develop an incident response plan; (2) automatically patch operating systems and applications; (3) enable security software; (4) securely configure devices; (5) use strong user authentication; (6) provide employee awareness training; (7) backup and encrypt data; (8) secure mobility; (9) establish basic perimeter defences; (10) secure cloud and outsourced IT services; (11) secure websites; (12) implement access control and authorization; and (13) secure portable media.

For more information, see BLG bulletin *Cybersecurity Guidance for Small and Medium Organizations*.

CyberSecure Canada Certification Program

On August 12, 2019, the Canadian federal government announced CyberSecure Canada, a voluntary cybersecurity certification program to help SMEs achieve a baseline of cybersecurity. The program is an initiative under the *National Cyber Security Strategy*, and supports the "Safety and Security" principle of Canada's *Digital Charter*.

The CyberSecure Canada certification will be based on an implementation of cybersecurity controls that reflect the thirteen baseline controls described in *Baseline Cyber Security Controls for Small and Medium Organizations*. A SME that demonstrates compliance with all of those controls, based on an audit conducted by an accredited certification body, will be deemed certified and entitled to use the CyberSecure Canada logo. Certifications will be valid for two years. When an organization's certification expires, the organization will have to apply for recertification.

Compliance with the baseline controls is important, but does not guarantee that an organization will not suffer a cybersecurity incident. The CyberSecure Canada *Frequently asked questions* explain:

"Certification does not guarantee complete protection from cyber threats. However, the processes and best practices learned as you make your way through the certification process, will provide businesses owners, managers and employees with the tools and abilities to improve your level of cyber risk and to better deal with breaches, if they occur."

The CyberSecure Canada program is targeted at Canadian SMEs (maximum of 499 employees), but all organizations in Canada (including not-for-profit and for-profit organizations) are eligible to apply for certification.

There are six initial accredited certification bodies listed on the CyberSecure Canada website. The CyberSecure Canada *Frequently asked questions* explain that the fee for the certification process will be set by each certification body, that some certification bodies may choose not to charge for the certification (if a SME uses their products and services that already meet the security controls) and others may charge anywhere from a few hundred dollars to several thousand dollars depending on the complexity of the SME's business and the audit required.

According to the CyberSecure Canada website, the CyberSecure Canada program will start with a pilot phase that will continue until the establishment of a national standard based on the controls described in *Baseline Cyber Security Controls for Small and Medium Organizations*. The national standard will be "developed by consensus of a balanced committee of stakeholders", undergo public scrutiny, be consistent with or incorporate existing international and pertinent foreign standards, and not act as a barrier for trade.

Innovation, Science and Economic Development Canada is responsible for implementing, overseeing and evaluating the CyberSecure Canada program, including designing the documentation and framework for certification and operating a public database of certifications. The Standards Council of Canada is responsible for accrediting public and private businesses as certification bodies.

Comment

The baseline controls that are the foundation of a CyberSecure Canada certification are important, but might not be sufficient or appropriate for all organizations. For example, the baseline controls might not be sufficient to comply with applicable laws (e.g. privacy/personal information protection laws), industry-specific requirements (e.g. cybersecurity guidance and best practices recommended by regulators and self-regulatory organizations), or cybersecurity requirements for reporting issuers (i.e. public companies). Each organization should consider its particular circumstances to determine whether additional cybersecurity controls are necessary. For more information, see BLG bulletins *Regulatory Guidance for Safeguarding Personal Information*; *Financial Industry Regulator Issues Cybersecurity Guidance*; *Investment Funds Institute of Canada Issues Cybersecurity Guide*; *Cybersecurity Guidance from Canadian Securities Administrators*; *Cybersecurity Guidance from Investment Industry Organization*; and *Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*.

Many of the baseline controls that are the foundation of a CyberSecure Canada certification have legal implications, including compliance with privacy/personal information protection, labour/employment and human rights laws. Timely legal advice can assist SMEs to implement the baseline controls in a manner that complies with applicable laws.

An organization's participation in a cybersecurity certification process can result in sensitive communications and documents that might be subject to mandatory disclosure in regulatory investigations and litigation relating to a cybersecurity incident, unless the communications and documents are protected by legal privilege. Organizations that apply for CyberSecure Canada certification should consider implementing a legal privilege strategy to help establish legal privilege over certain communications and documents created in connection with the certification process. For more information, see BLG bulletins *Cyber Risk Management – Legal Privilege Strategy (Part 1)*; *Cyber Risk Management – Legal Privilege Strategy (Part 2)*; *Legal Privilege for Data Security Incident Investigation Reports*; and *Loss of Legal Privilege over Cyberattack Investigation Report*.

Organizations that obtain a CyberSecure Canada certification and use the CyberSecure Canada logo should take appropriate measures to help ensure that they remain compliant with the baseline controls. Failure to do so could expose an organization that suffers a cybersecurity incident to claims by affected customers and business partners, and resulting liabilities, for false or misleading advertising, misrepresentations or fraud.

Services: Cybersecurity, Privacy & Data Protection

Related Content

Information Technology

Technology