Bulletin | Cybersecurity, Privacy and Data Protection

June 2020

Cybersecurity certification for small and medium enterprises

Cybersecurity is vital for organizations of all kinds and sizes, including small and medium enterprises (SMEs). Both Canada and the United Kingdom have government-authorized cybersecurity certification programs suitable for SMEs. Cybersecurity certification can enable an SME to provide its customers, investors and business partners with independent confirmation that it has achieved a baseline of cybersecurity.

Cybersecurity for SMEs

Cybersecurity is vital for SMEs. Cybercriminals are increasingly targeting SMEs, including to extort ransom payments, to obtain information about their customers and to access the systems and data of their business partners. Cyberattacks can cause SMEs to suffer potentially devastating financial losses and liabilities. However, sophisticated cybersecurity programs can be expensive and time-consuming to implement and beyond the financial and human resources means of many SMEs.

The Canadian Centre for Cyber Security's guide, *Baseline Cyber Security Controls for Small and Medium Organizations*, provides a condensed set of advice and guidance to help 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) back-up 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.

Similar guidance has been issued by the U.K. National Cyber Security Centre (*Small Business Guide: Cyber Security* and *10 steps to cyber security*), the U.S. Federal Trade Commission (*Cybersecurity for Small Business*), the U.S. Cybersecurity & Infrastructure Security Agency (*Cyber Essentials*) and the Australian Cyber Security Centre (*Small Business Cyber Security Guide* and *Essential Eight Maturity Model*). The *CIS Controls Implementation Guide for SMEs* is also a useful resource.

Cybersecurity certification

Cybersecurity certification, based on an audit by an accredited certification body, can validate the effectiveness of an SME's cybersecurity program and provide the SME's customers, investors and business partners with an independent confirmation that the SME has achieved a baseline of cybersecurity. Both Canada and the United Kingdom have government-authorized cybersecurity certification programs suitable for SMEs.

CyberSecure Canada

CyberSecure Canada, established by the Canadian federal government, is a voluntary cybersecurity certification program designed for SMEs. A CyberSecure Canada certification requires an implementation of the *Baseline Cyber Security Controls for Small and Medium Organizations* (discussed above). An SME that demonstrates compliance with those controls, based on an audit conducted by an accredited certification body, will be deemed certified and entitled to use the CyberSecure Canada certification mark. Certifications are valid for two years. When an SME's certification expires, the SME must apply for recertification. See BLG bulletin *Ready, Set, Certify – Canada's New CyberSecure Canada Certification Program*.

Cyber Essentials

Cyber Essentials, established by the U.K. National Cyber Security Centre, is a voluntary cybersecurity certification program designed for organizations of all kinds and sizes, including SMEs. A certification requires an implementation of the following five technical controls to protect against the most common cyber attacks: (1) use of firewalls to secure internet connections; (2) secure configuration of devices and software; (3) controls on access to data and services; (4) protection against viruses and other malware; and (5) keeping devices and software up to date. There are two levels of certification – Cyber Essentials (based on an independently evaluated self-assessment) and Cyber Essentials Plus (based on an independent technical assessment). Certifications are valid for one year. When an organization's certification expires, the organization must apply for recertification.

Comments

Following are some considerations for selecting a cybersecurity certification program and applying for certification:

- The significance of a cybersecurity certification depends primarily on the underlying mandatory cybersecurity controls. A CyberSecure Canada certification requires the implementation of a broad set of controls based on people, processes and technologies. In contrast, a Cyber Essentials certification requires the implementation of a smaller set of technological controls, and omits certain controls (e.g. employee awareness training, data back-ups and an incident response plan) that are necessary for a CyberSecure Canada certification and might provide significant benefits.
- It is important to note that the cybersecurity controls required for certification might not be sufficient for compliance 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 SME should consider its particular circumstances to determine whether additional cybersecurity controls are necessary.
- Many cybersecurity controls have legal implications, including compliance with privacy/personal information protection, labour/employment and human rights laws. Timely legal advice can assist an SME to lawfully implement cybersecurity controls.
- SMEs should consider implementing a legal privilege strategy to help establish and maintain legal privilege, where appropriate, for sensitive communications and documents created in connection with the cybersecurity certification process. 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*.

- SMEs that obtain a cybersecurity certification and use the certification logo should take measures to help ensure that they properly maintain the required cybersecurity controls. Failure to do so could expose an SME that suffers a cybersecurity incident to claims by affected customers, investors and business partners, and resulting liabilities, for false or misleading advertising, misrepresentations or (in extreme circumstances) fraud. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity, Privacy & Data Protection Group has extensive expertise and experience in cyber risk management and crisis management legal services. Find out more at **blg.com/cybersecurity**.