Cybersecurity Bulletin

July 2019

Cybersecurity Guidance for Small and Medium Organizations

Small and medium organizations are increasingly being targeted by cyber criminals, but often have limited financial and human resources available to implement comprehensive cybersecurity measures. In March 2019, the Canadian Centre for Cyber Security issued *Baseline Cyber Security Controls for Small and Medium Organizations* to help Canadian small and medium organizations get the most out of their cybersecurity investments.

Cybersecurity for Small and Medium Organizations

Cybersecurity is important for organizations of all kinds and sizes. The Canadian Centre for Cyber Security's *National Cyber Threat Assessment 2018* warns that "cybercrime is the cyber threat most likely to affect Canadians and Canadian businesses in 2019", and "sophisticated cyber threat actors will likely continue to exploit the trusted relationships between businesses and their suppliers and service providers for espionage and cybercrime purposes".

Cyber criminals are increasingly targeting small and medium organizations, including to obtain data about their customers and business partners and as a means of accessing the information technology systems and data of their business partners. Cyberattacks can cause small and medium organizations to suffer potentially devastating financial losses and liabilities. However, comprehensive cyber risk management programs, such as the *NIST Cybersecurity Framework* and *ISO/IEC 27001:2013*, can be expensive and time consuming to implement and beyond the financial and human resources means of most small and medium organizations.

Government agencies and other organizations have issued basic cybersecurity guidance for small and medium organizations with limited resources. For example, see: *Small Business Information Security: The Fundamentals* (NIST); *Small Biz Cyber Planner 2.0*, *Cyber Security Planning Guide* and *Cybersecurity for Small Business* (FCC); *Cyber Security Small Business Guide* (NCSC); the *Essential Eight* (ACSC); and *Get Cyber Safe Guide for Small and Medium Businesses* (Government of Canada). For more information see BLG bulletin *Cybersecurity Guidance for Small and Medium Size Enterprises*.

The *Baseline Cyber Security Controls* Guide

The Canadian Centre for Cyber Security was established in October 2018 to be the Canadian government's unified source of expert advice, guidance, services and support on cybersecurity for government, critical infrastructure owners and operators, the private sector and the Canadian public. The Centre has recently published helpful cybersecurity guidance for small and medium organizations, including *Protecting High-Value Information: Tips for Small and Medium Organizations* and *Supply chain security for small and medium-sized organizations*.

In March 2019, the Centre issued *Baseline Cyber Security Controls for Small and Medium Organizations* (the "Guide") to provide a condensed set of advice and guidance, including thirteen baseline cybersecurity controls, to help Canadian small and medium organizations (i.e. less than 499 employees) 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 explains that each organization must consider its particular circumstances to determine whether the recommended baseline cybersecurity controls are sufficient and appropriate. The relevant circumstances include: (1) the size of the organization; (2) the information systems and data that are in scope for the implementation of the controls; (3) the value of the organization's information systems and data, and the risk of injury to the confidentiality, integrity and availability of the information systems or data; and (4) the cybersecurity threat level faced by the organization.

The Guide recommends that organizations assign responsibility for cybersecurity to an individual in a leadership role (e.g. a chief information security officer), and assess the adequacy of their financial spending and internal staffing for information technology and cybersecurity. The Guide also recommends that organizations "adopt the thinking that they will suffer a data breach at some point and thus be in a position to detect, respond, and recover".

Following is a summary of the baseline cybersecurity controls recommended by the Guide:

1. **Develop an Incident Response Plan:** Have a basic written incident response plan (in both hard and soft copies) for how to respond to cybersecurity incidents of varying severity, including a plan for engaging external assistance. The plan should identify the individuals responsible for handling incidents, including communicating with external parties, stakeholders and regulators and complying with breach reporting obligations. Consider purchasing cybersecurity insurance that includes coverage for incident response and recovery activities. Consider implementing a security event monitoring system for detecting, monitoring, and responding to cybersecurity incidents.
2. **Automatically Patch Operating Systems and Applications:** Enable automatic patching for all software and hardware, or establish full vulnerability and patch management solutions. Replace software and hardware that are not capable of automatic updates, or have a business process to ensure regular manual updates.
3. **Enable Security Software:** Enable anti-virus and anti-malware solutions, which update and scan automatically, on all connected devices.
4. **Securely Configure Devices:** Implement secure configurations for all devices, change all default passwords on all devices, turn off unnecessary device features/functionalities, and enable all relevant security features on all devices.
5. **Use Strong User Authentication:** Require two-factor authentication for important accounts (e.g. financial accounts, system administrators, cloud administration, privileged users and senior executives), and implement two-factor authentication for other accounts wherever possible. Require password changes only on suspicion or evidence of password compromise. Have clear policies on password length and reuse, the use of password managers and how passwords should be securely stored.
6. **Employee Awareness Training:** Provide cybersecurity awareness and training for all employees, focusing on practical and easily implementable measures such as: (a) use of passwords; (b) identification of malicious emails and links; (c) use of approved software; (d) appropriate Internet use; and (e) use of social media.
7. **Backup and Encrypt Data:** Backup systems that contain essential business information, using an appropriate backup frequency, and ensure that recovery mechanisms can effectively and efficiently restore those systems. Securely store backups in an encrypted state and subject to restricted access. Consider storing backups offsite to provide diversity in the event of a disaster.
8. **Secure Mobility:** Determine an ownership model for mobile devices, and document the rationale and associated risks. Enforce separation between work and personal data on mobile devices with access to corporate IT resources. Ensure that employees only download mobile device apps from trusted sources. Require that all mobile devices store sensitive information in a secure, encrypted state. Implement an appropriate enterprise mobility management solution for all mobile devices, or document the risks assumed by not implementing such a solution. Enforce or educate users to: (a) disable automatic connections to open networks; (b) avoid connecting to unknown Wi-Fi networks; (c) limit the use of Bluetooth and NFC for the exchange of sensitive information; and (d) use corporate Wi-Fi or cellular data network connectivity rather than public Wi-Fi.

9. **Establish Basic Perimeter Defences:** Implement a dedicated firewall at boundaries between corporate networks and the Internet. Implement a DNS firewall for outbound DNS requests to the Internet. Activate software firewalls on devices within networks, or document the alternative measures in place. Require secure connectivity to all corporate IT resources, and require VPN connectivity with two-factor authentication for all remote access to corporate networks. Secure internal Wi-Fi, preferably with WPA2-Enterprise. Never connect public Wi-Fi networks to corporate networks. Follow the Payment Card Industry Data Security Standard (PCI DSS) for all point-of-sale terminals and financial systems, segment those systems from other parts of the corporate network, and isolate those systems from the Internet. Implement domain-based message authentication, reporting and conformance (DMARC) on all email services.
10. **Secure Cloud and Outsourced IT Services:** Require all cloud service providers to share an SSAE 16 SOC 3 report that confirms they achieved Trust Service Principles compliance. Evaluate comfort with how outsourced IT providers handle and access sensitive information (e.g. their privacy policies, data security incident notification processes, data deletion processes, physical location and security of data centres, and physical location of personnel), and with the laws in the jurisdictions where outsourced IT providers store or use sensitive information. Encrypt sensitive information stored outside local IT systems, and ensure secure access to data stored in the cloud. Ensure that IT infrastructure and users communicate securely with all cloud services and applications. Ensure that administrative accounts for cloud services use two-factor authentication and differ from internal administrator accounts.
11. **Secure Websites:** Ensure that corporate websites meet the Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) guidelines.
12. **Implement Access Control and Authorization:** Apply the principle of least privilege – provision accounts with the minimum functionality and data access necessary for assigned tasks, restrict administrator privileges to an as-required basis, and remove accounts and functionalities when no longer required for assigned tasks. Permit administrator accounts to perform only administrative activities, and not user-level activities. Ensure all users have unique individual accounts, and minimize or eliminate the use of shared or shared-use accounts. Have a process to revoke accounts when they are no longer required (e.g. when employees leave). Consider implementing a centralized authorization control system.
13. **Secure Portable Media/Storage Devices:** Ensure the exclusive use of organization-owned secure portable media (e.g. USB drives) and storage devices that have strong asset controls and use encryption. Have processes for the sanitization or destruction of portable media and storage devices before disposal.

Comment

The baseline controls recommended by the Guide are important, but might not be sufficient to comply with applicable laws or industry-specific requirements. For example:

- **Personal Information:** Small and medium organizations that handle personal information must comply with obligations under Canadian privacy/personal information protection laws to safeguard personal information under their control using security safeguards (including physical, organizational and technological measures) appropriate to the sensitivity of the information. The required safeguards might include items (e.g. a privacy and security governance framework) that are not part of the baseline controls recommended by the Guide. For more information, see BLG bulletins *Regulatory Guidance for Safeguarding Personal Information* and *Regulatory Enforcement Action Emphasizes Need for an Information Security Governance Framework*.
- **Regulated Industries:** Small and medium organizations in regulated industries (e.g. the financial services industry) must also be mindful of cybersecurity guidance and best practices recommended by relevant regulators. For more information, see BLG bulletins: *Financial Industry Regulator Issues Cybersecurity Guidance*; *Investment Funds Institute of Canada Issues Cybersecurity Guide*; *U.S. Financial Institution Regulators Issue Guidance About Cyber Insurance*; *Cybersecurity Guidance from Canadian Securities Administrators*; and *Cybersecurity Guidance from Investment Industry Organization*.

- **Reporting Issuers:** Small and medium corporations that have issued securities to the public must establish cyber risk identification and assessment processes and internal incident reporting procedures required to comply with continuous disclosure obligations under Canadian securities laws. For more information, see BLG bulletin *Cyber Risk Management – Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*.

Many of the baseline controls recommended by the Guide have legal implications, including compliance with privacy/personal information protection, labour/employment and human rights laws. Timely legal advice can assist organizations to implement the baseline controls in a manner that complies with applicable laws.

In addition, the involvement of lawyers in cybersecurity activities (e.g. assessing an organization's cybersecurity maturity, conducting testing/training activities and responding to cybersecurity incidents and data breaches) is necessary to establish legal privilege over communications and reports relating to those activities. Organizations should consider implementing a legal privilege strategy to help avoid inadvertent and unnecessary disclosures of privileged legal advice given during cybersecurity activities. 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*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG's Cybersecurity Law Group is available at **blg.com/cybersecurity**.

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349