Bulletin | Cybersecurity, Privacy and Data Protection

January 2023

Improving cybersecurity with internal resources and outsourced services

Cybersecurity is a fundamental issue for organizations of all kinds and sizes, but many organizations have limited financial and human resources available to implement comprehensive cybersecurity measures. In October 2022, the Canadian Centre for Cyber Security issued guidance to help Canadian organizations assess and improve their cybersecurity posture and effectively outsource cybersecurity to a managed security service provider.

The cybersecurity challenge

Cybersecurity is important for all Canadian organizations. The Canadian Centre for Cyber Security's *National Cyber Threat Assessment 2023-2024* warns that cybercrime continues to be the cyber threat activity most likely to affect Canadians, and ransomware is a persistent threat to Canadian organizations.

Government agencies and other organizations have issued cybersecurity guidance for organizations of all sizes and kinds, including small and medium organizations with limited resources. For example, the Canadian Centre for Cyber Security's guide titled *Baseline Cyber Security Controls for Small and Medium Organizations* provides guidance to help Canadian organizations maximize the effectiveness of their cybersecurity investments. The recommended controls reflect the view that organizations can mitigate most cyber threats through awareness and best practices and successfully apply the 80/20 rule – achieve 80% of the benefit from 20% of the effort – in the cybersecurity domain. See BLG bulletins *Cybersecurity Guidance for Small and Medium Size Enterprises* and *Cybersecurity Certification for Small and Medium Enterprises*.

Nevertheless, comprehensive cybersecurity programs can be expensive and time-consuming to implement and require technical knowledge and resources that are beyond the means of many organizations. For those reasons, many organizations outsource part or all of their cybersecurity requirements to a managed security service provider (MSSP).

The Guide

In October 2022, the Canadian Centre for Cyber Security published guidance titled *Choosing the best cyber security solution for your organization* (the "Guide") to help organizations improve their cybersecurity posture using internal resources and outsourced services. Following is a summary of key aspects of the Guide.

Cybersecurity assessment and best practices

The Guide encourages organizations to assess their cybersecurity posture by conducting a risk assessment and identifying the organization's specific cybersecurity requirements. The Guide provides a list of preliminary questions that organizations of all sizes should ask when conducting a cybersecurity risk assessment.

The Guide recommends organizations implement the cybersecurity controls described in *Baseline Cyber Security Controls for Small and Medium Organizations* for all information technology systems and assets (whether owned, contracted or otherwise used). The Guide explains that organizations with limited technological or financial resources should start with the following foundational controls: (1) implement strong user authentication; (2) patch operating systems and applications; (3) backup and encrypt data; (4) train employees; and (5) develop an incident response plan. The Guide explains that implementing the following advanced controls might require the assistance of a service provider: (1) enable security software; (2) secure websites; (3) secure mobile devices; (4) access control and authorization; (5) establish basic perimeter defences; (6) configure devices securely; (7) secure portable media; and (8) secure cloud and outsourced services (including outsourced cybersecurity services).

The Guide notes that cybersecurity service providers can provide organizations with tailored cybersecurity advice and guidance, including assistance in developing and implementing an effective cybersecurity plan.

Outsourcing cybersecurity

The Guide notes that outsourcing some or all cybersecurity requirements has become a common practice for organizations of all sizes. The Guide reminds that organizations that outsource cybersecurity to a service provider remain legally responsible for protecting their IT systems and data (including personal information). The Guide explains that a decision to outsource cybersecurity services should be based on a thorough understanding of the organization's cybersecurity objectives/requirements and the ability of a proposed service provider to address those requirements. The Guide also reminds that the organization should ensure the outsourced cybersecurity services are periodically reviewed and updated to meet the organization's evolving business priorities and systems.

The Guide summarizes the different kinds of cybersecurity services provided by different kinds of service providers – Internet service providers, IT/cybersecurity consultants, cloud service providers (CSP), managed service providers (MSP), and managed security service providers (MSSP). The guide also details the differences between an MSP (which focuses primarily on information technology administration/management) and an MSSP (which focuses on cybersecurity).

The Guide describes some of the benefits and risks of outsourcing to an MSSP. It details the services typically provided by an MSSP: (1) consultancy/advisory services; (2) managed security service technologies; (3) data protection and security monitoring; (4) risk and vulnerability assessment and management; and (5) compliance monitoring and management. The Guide explains that selecting an MSSP "is a complex decision for any organization and requires thorough research and analysis". The Guide includes a list of criteria to help evaluate an MSSP and its services.

Comments and recommendations

- The baseline cybersecurity controls recommended by the Guide are important but might not be sufficient to comply with generally applicable laws or industry-specific requirements. See BLG bulletin *Cybersecurity Guidance for Small and Medium Organizations*.
- Many cybersecurity controls have legal implications, including compliance with privacy/personal information protection, labour/employment and human rights laws. Timely legal advice can help an organization lawfully implement cybersecurity controls.
- An organization's engagement of a cybersecurity service provider should be subject to appropriate oversight and monitoring by the organization's directors, who have a legal responsibility to ensure their organization has appropriate cyber risk management policies and practices and is prepared to respond effectively to cybersecurity incidents. See BLG bulletins *Cyber risk management guidance for Canadian corporate directors* and *Cyber Risk Management – Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*.

- Outsourcing cybersecurity presents business and legal risks, including compliance with laws of general application (e.g., privacy/personal information protection) and industry-specific requirements. Consequently, organizations should consider outsourcing best practices recommended by government agencies, regulators, privacy commissioners, industry associations and other organizations. For example, see BLG bulletins *BCFSA finalizes information security and outsourcing guidelines*, *Privacy Commissioner reports provide guidance for outsourcing agreements* and *Cloud services – Guidance for managing cybersecurity risks*.
- Where appropriate, organizations should take steps to establish and maintain legal privilege over communications and documents relating to outsourced cybersecurity services. 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*.
- Outsourced cybersecurity services often require the customer to use locally installed software and cloud-based services, both of which present business and legal compliance risks that should be addressed in applicable agreements. See BLG publications *Software License Agreements: A Practical Guide* and *SaaS Agreements: A Practical Guide*.
- An organization's cybersecurity service provider should be part of the organization's incident response team and should participate in periodic evaluations and testing of the organization's incident response plan. See BLG bulletins *Cybersecurity incident response – Tips from the trenches* and *Data Security Incident Response Plans – Some Practical Suggestions*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

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