Bulletin | Cybersecurity, Privacy and Data Protection

January 2023

Cyber risk guidance for customers and providers of managed IT services

Cybersecurity is a fundamental issue for Canadian organizations of all kinds and sizes, including organizations that use information technology services managed by independent service providers. The Canadian Centre for Cyber Security has issued guidance to help organizations manage cyber risks when procuring and using managed information technology services.

Managed IT services and cyber risks

Many organizations engage specialist service providers – known as managed service providers (MSPs) – to manage some or all of the organization's information technology (IT) infrastructure and services (including infrastructure and services provided by cloud service providers and other third parties). The outsourcing of IT management services can provide significant benefits, but it can also present potentially significant business and legal compliance risks.

An organization that uses managed IT services is often dependent on the MSP (because the services are often mission-critical for the organization's daily operations) and vulnerable to misconduct by the MSP or its personnel (because the MSP's personnel usually have privileged, remote access to the organization's IT systems and data). In addition, an MSP's services present inherent cybersecurity risks because cyber criminals target MSPs to obtain access to their customers' IT systems and data. The Canadian Centre for Cyber Security's *National Cyber Threat Assessment 2023-2024* warns that cybercriminals will "almost certainly" continue to target MSPs to maximize the reach of their ransomware attacks. (See also *Alert - Malicious Cyber Activity Targeting Managed Service Providers* and *Alert - 2021 Trends Show Increased Globalized Threat of Ransomware*.)

For those reasons, organizations should identify and manage cyber risks (as well as other business and legal compliance risks) when procuring and using managed IT services. Helpful cyber risk management guidance regarding managed IT services is available from various authoritative sources, including The Canadian Centre for Cyber Security and The U.S. Cybersecurity & Infrastructure Security Agency.

Procurement guide

In October 2020, the Canadian Centre for Cyber Security issued guidance titled *Cyber Security Considerations for Consumers of Managed Services* (the Guide) to help organizations determine whether an MSP is able to perform IT management services effectively and securely and to negotiate an appropriate services agreement with an MSP. The Guide addresses key cybersecurity topics that organizations should consider when procuring managed services from an MSP. Following is a summary:

- Data security: The organization should identify the kinds of data that will be accessible to the MSP and determine the security controls required to protect the data.
- Legal compliance: The organization should understand its obligations, under laws of general application and industry-specific laws, regarding the data that will be accessible to the MSP.
- MSP assessment: The organization should assess the adequacy of the MSP's internal security controls against recognized security standards/frameworks and using third-party audit reports.
- Access control: The organization should establish policies and procedures governing access to the organization's data and IT systems (including data access rules based on the principle of least privilege, authentication and authorization mechanisms, system administrator roles, physical access to servers, password policies and federated authentication) and specify the related roles/responsibilities of the organization and the MSP.
- Encryption: The organization should determine the required level of encryption for data in transit and at rest and assess whether the MSP can support the required encryption with appropriate practices and procedures (including key management).
- Incident reporting/response: The organization should establish clear requirements for incident reporting and response and ensure that the MSP can support the requirements. The services agreement with the MSP should specify expected turnaround times, communication media, escalation processes, metrics for assessing performance, and financial remedies for deficient performance.
- Business continuity/disaster recovery: The organization should determine its service level (i.e., quality) requirements and understand the measures implemented by the MSP to prevent service disruption and support service recovery in the event of a disaster.
- Supply chain integrity: The organization should understand the third-party services (including information and communication technologies) used by the MSP and the assurances the MSP will give for those services.
- Exit strategies: The organization should understand its rights to terminate the engagement of the MSP and transfer data to an alternative MSP.
- Data destruction: The organization should establish a data retention/deletion policy and ensure that the MSP can support the policy.

The Guide emphasizes that an organization's agreement with an MSP should clearly specify the respective roles and responsibilities of the organization and the MSP regarding each of the issues detailed in the Guide.

Similar guidance has been issued by the U.S. Cybersecurity & Infrastructure Security Agency (*Risk Considerations for Managed Service Provider Customers*) and the Australian Cyber Security Centre (*Managed Service Providers: How to Manage Risk to Customer Networks*).

Cybersecurity advisory

In May 2022, the Canadian Centre for Cyber Security announced a cybersecurity advisory titled *Protecting Against Cyber Threats to Managed Service Providers and their Customers* (the Advisory) issued jointly with the cybersecurity authorities of the United Kingdom, Australia, New Zealand and the United States. The Advisory notes an increase in cyber crime targeting MSPs and provides guidance for MSPs and their customers to protect against cyber threats. The Advisory explains that it is intended to "enable transparent, well-informed discussions between MSPs and their customers" regarding cybersecurity that should "result in a re-evaluation of security processes and contractual commitments to accommodate customer risk tolerance".

The Advisory recommends that MSPs and their customers implement specified and detailed baseline security measures and operational controls to prevent and mitigate cybersecurity risks. Following is a summary:

- Prevent initial compromise by implementing recommended countermeasures and controls.
- Enable/improve monitoring and logging processes to detect threats, and retain logs for at least six months.

- Enforce multifactor authentication for access to networks and systems.
- Manage internal architecture risks and segregate internal networks to reduce the scope and impact of a compromise.
- Apply the principle of least privilege access throughout all network environments.
- Deprecate obsolete accounts and infrastructure (including systems and services) to limit the attack surface.
- Apply software updates and prioritize security updates for known software vulnerabilities.
- Backup systems and data on a regular basis consistent with recovery point objectives, and securely store the backups.
- Develop and regularly exercise incident response and recovery plans.
- Proactively manage IT supply chain risk, including risks associated with third-party vendors and subcontractors.
- Promote transparency with contractual arrangements that clearly define responsibilities, including clear explanations of the MSP's services.
- Manage account authentication and authorization using best practices for password and permission management.

The Advisory recommends specific actions by the MSP and the customer for each cybersecurity control, and emphasizes that agreements with MSPs should address the recommended cybersecurity controls.

Comments and recommendations

- The cybersecurity controls recommended by the Guide and the Advisory are important but might not be sufficient to satisfy legal requirements. In addition, many cybersecurity controls have legal implications, including restrictions and requirements under privacy/personal information protection, labour/employment and human rights laws. Timely legal advice can help an organization lawfully implement cybersecurity controls that satisfy legal requirements.
- The services provided by an MSP (which focuses primarily on information technology administration/management) are different from the cybersecurity services provided by a managed security service provider (which focuses on cybersecurity). See BLG bulletin *Improving cybersecurity with internal resources and outsourced services.*
- An organization's engagement of an MSP should be based on a documented risk assessment, informed by appropriate due diligence and expert advice, as to whether the relative benefits of the specific MSP and its services justify the relative risks in light of all of the circumstances, including the organization's overall enterprise risk tolerance. In this context, risks and benefits are both absolute and relative concepts. Accordingly, the risks and benefits of engaging a specific MSP should be assessed realistically and in comparison with practicable alternatives (e.g., engaging other MSPs or using internal services).
- An organization should have a documented program, supported by contractual rights, to monitor the MSP's performance and verify the MSP's compliance with contractual obligations.
- Managed IT services are a form of outsourcing that presents business and legal risks and might be subject to industry-specific legal requirements. Consequently, organizations should consider outsourcing best practices, issued by privacy commissioners, regulators and other authoritative sources, when procuring and using managed IT services. 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*.
- An organization's engagement of an MSP 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*.
- Where appropriate, organizations should take steps to establish and maintain legal privilege over communications and documents relating to the procurement and use of managed IT 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*.

- Managed IT services often require the customer/organization 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 MSP 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**.

blg.com | Canada's Law Firm
Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances.

Borden Ladner Gervais