Bulletin | Cybersecurity, Privacy and Data Protection

July 2023

Cybersecurity guidance for small organizations

Cybersecurity is a significant challenge for organizations of all kinds and sizes, including small organizations with limited resources for a cybersecurity program. Each of the Canadian Centre for Cyber Security ("CCCS"), the United States Cybersecurity & Infrastructure Security Agency ("CISA"), and the Australian Cyber Security Centre ("ACSC") have issued recent guidance to help small organizations implement foundational cybersecurity measures to begin building cybersecurity resilience.

The cybersecurity challenge

Cybersecurity is important for all Canadian organizations. The CCCS'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.

Cybercriminals are increasingly targeting small and medium organizations, including to obtain data about their customers and as a means of accessing the information technology systems and data of their business partners. In December 2022, the Canadian Federation of Independent Business reported survey results that nearly half of small businesses (45%) experienced a random cyberattack in the previous year, and 27% experienced a targeted attack.

Cyberattacks can cause small organizations to suffer potentially devastating financial losses and liabilities. However, sophisticated cyber risk management programs are beyond the financial and human resources means of most small organizations. For those reasons, government agencies and other organizations have issued cybersecurity guidance designed for small organizations. For example, in 2019 CCCS issued guidance titled *Baseline cyber security controls for small and medium organizations* to help Canadian organizations maximize the effectiveness of their cybersecurity investments. The recommended baseline 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 Organizations*, *Cybersecurity Certification for Small and Medium Enterprises*, *Ready, Set, Certify – Canada's New CyberSecure Canada Certification Program*, and *Cybersecurity Certification for Small and Medium Enterprises*.

Recent guidance

CCCS, CISA, and ACSC have each recently issued cybersecurity guidance designed for small organizations.

CCCS

CCCS's *Foundational cyber security actions for small organizations* recommends basic security measures (with checklists and links to additional resources) that small organizations can take to begin building their cybersecurity resilience. Following is a summary:

- **Credentials:** Use different complex passwords and multi-factor authentication ("MFA") for each device and account.
- **Updates/patching:** Update and patch operating systems and applications automatically.
- **Backups:** Create and securely store data backups.
- **Security tools:** Install preventative security tools (e.g., anti-virus software and a virtual private network) on networks and devices, and use a protective domain name system.
- **Training:** Train employees on basic cyber security practices.
- **Incident response readiness:** Establish and test an incident response plan.

The guidance recommends small organizations take regular inventories of their information technology assets to identify and prioritize protection for high-value assets. The guidance also recommends small organizations consider outsourcing cybersecurity activities to a service provider, based on CCCS's guidance *Choosing the best cyber security solution for your organization*.

CISA

CISA's *Cyber Guidance for Small Businesses* provides guidance (with links to additional information and resources) for building an effective cybersecurity program organized by roles and responsibilities suitable for small businesses. The guidance includes tasks to address the "most common attacks". Following is a summary:

- **CEO:** The organization's CEO should: (1) establish a culture of security; (2) select and support a "Security Program Manager" and receive regular reports from the manager; (3) review and approve an incident response plan; (4) participate in regular attack simulation exercises (i.e., tabletop exercises); and (5) support the IT leaders.
- **Security program manager:** The organization's security program manager should: (1) ensure all staff are formally trained about key cybersecurity issues and tasks; (2) write and maintain an incident response plan; (3) host quarterly tabletop exercises; and (4) ensure all staff use MFA to access key systems.
- **IT lead:** The organization's information technology lead should: (1) ensure MFA is mandated using technical controls; (2) enable MFA for all system administrator accounts; (3) patch and update software with priority to known exploited vulnerabilities; (4) perform and test backups and restoration plans; (5) remove administrator privileges from user laptops; and (6) enable disk encryption for laptops.

The guidance emphasizes the importance of using MFA for account access. The guidance also explains the potential security benefits of using secure cloud-based services rather than on-premises services.

ACSC

ACSC's *Small Business Cyber Security Guide* provides a checklist of basic cybersecurity measures and a detailed guide to help small businesses protect against common cyber security threats. Following is a summary:

- **Secure accounts:** Use MFA and a password manager, limit the use of shared accounts, and limit access based on need-to-know.
- **Protect devices/information:** Automatically update devices and software, regularly backup information, use security software to regularly scan devices, get professional advice about securing networks, secure websites, factory reset devices before selling/disposing of them, configure devices to automatically lock after a brief time of inactivity, understand the business data and responsibilities to protect it.
- **Prepare staff:** Educate employees about cybersecurity, create a cybersecurity incident response plan, and register with the ACSC Partnership Program.

The guide also encourages small organizations to implement the first maturity level of *The Essential Eight* cyber risk mitigation strategies for protecting Microsoft Windows-based internet-connected networks.

Comments

The basic cybersecurity measures recommended by CCCS, CISA, and ACSC are important but might not be sufficient to comply with applicable laws or industry-specific requirements. For example:

- **Personal information:** 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 appropriate to the sensitivity of the information, including items (e.g., a privacy and security governance framework) that go beyond basic cybersecurity measures. See BLG bulletins *Regulatory Guidance for Safeguarding Personal Information* and *Regulatory Enforcement Action Emphasizes Need for an Information Security Governance Framework*.
- **Regulated industries:** Organizations in regulated industries (e.g., the financial services industry) must be mindful of regulatory requirements and cybersecurity guidance issued by relevant regulators. See BLG bulletins *OSFI's new Guideline B-13 – Managing technology and cyber risks*, *OSFI updates Technology and Cyber Security Incident Reporting Advisory*, *Investment industry organization provides additional cybersecurity guidance*, *Investment Funds Institute of Canada Issues Cybersecurity Guide*, *Cybersecurity Guidance from Canadian Securities Administrators*.
- **Reporting issuers:** Organizations 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. See BLG bulletins *Cyber Risk Management – Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents* and *Cyber risk management guidance for Canadian corporate directors – 2023 Update*.

When considering whether and how to implement recommended basic cybersecurity measures, organizations should consider the following:

- **Compliance with applicable laws:** Many cybersecurity measures 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.
- **M&A transactions:** Start-ups and other small organizations planning for a sale or other exit should be mindful of the increasing importance of privacy and cyber risks in M&A transactions. See BLG bulletin *Managing privacy and cyber risks in M&A transactions*.
- **Outsourcing cybersecurity activities:** Outsourcing cybersecurity activities (e.g., to a managed security services provider) can present legal risks, including compliance with laws of general application (e.g., privacy/personal information protection laws) and industry-specific requirements. Consequently, organizations should consider outsourcing best practices recommended by government agencies, regulators, privacy commissioners, and other authoritative sources. See BLG bulletins *Improving cybersecurity with internal resources and outsourced services* and *Cyber risk guidance for customers and providers of managed IT services*.
- **Incident response preparedness:** An effective response to a cybersecurity incident requires more than an incident response plan. See BLG bulletins *Cybersecurity incident response – Tips from the trenches* and *Ransomware attacks – Tips from the trenches*.
- **Data minimization:** Data minimization is a fundamental principle of Canadian personal information protection laws and can help reduce privacy and cyber risks. See BLG bulletin *Less is more – Data minimization and privacy/cyber risk management*.

- **Legal privilege:** Where appropriate, organizations should take steps to establish and maintain legal privilege over communications and documents relating to their cybersecurity activities, including the preparation and testing of their incident response plans and the training of their incident response team. 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, 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**.