Foundational cyber security actions for small organizations

CANADIAN CENTRE FOR CYBER SECURITY

May 2023 | ITSAP.10.300

Small and medium organizations (SMO) face growing cyber security concerns, including phishing and ransomware attacks, that can compromise sensitive information and lead to financial or data loss. In this publication, we summarize the foundational security actions you can take to begin building your cyber security resilience. These actions are a minimum set of practices that you can implement over time. You will find some additional recommendations on security actions that you can implement as your organizational resources and capacity increase.

Use complex passwords and multi-factor authentication

Use different complex passwords for each device and account. Threat actors know people reuse the same passwords across different accounts. If threat actors can access your devices and accounts, they can take them over, lock you out, and steal sensitive information. Instead of relying solely on your password for protection, you should use multi-factor authentication (MFA) as well. With MFA enabled, you must prove your identity in multiple ways to log in, which provides additional protection and time to respond even if a threat actor knows your password. To learn more, see Best practices for passphrases and passwords (ITSAP.30.032) and Secure your accounts and devices with multi-factor authentication (ITSAP.30.030).

- ☐ Do you use different complex passwords that are at least 12 characters in length for each account?
- ☐ Do you use a password manager or do you have a process for physically writing down and securely storing passwords?
- ☐ Have you set up MFA on devices and accounts?
- ☐ Do you change passwords if there has been a suspected or actual compromise to devices or accounts?
- ☐ Do you change all default vendor supplied passwords?
- ☐ Do you have a password policy to guide all your users?

Update operating systems and applications automatically

Updates and patches address known security vulnerabilities, fix bugs, and improve the usability and the performance of applications and operating systems (OS). Postponing or ignoring updates and patches leaves your OS and applications vulnerable to cyber threats. Threat actors look for known vulnerabilities, backdoors and other ways to access your networks, systems, and information. To learn more, see How updates secure your device (ITSAP.10.096).

- ☐ Do you apply security patches for software and hardware when vendors release them?
- ☐ Do you keep track of what applications and operating systems you use?
- ☐ Have you turned on automatic updates?
- ☐ Do you use unsupported or legacy systems that can no longer be updated? If so, do you have a plan to replace these systems?

Aside from the list of recommended actions, we suggest that you take regular inventory of your assets to identify those of high-value that you want to protect. This will help you adjust and enhance your security practices over time. The following are possible assets that your organization may have:

- desktop and mobile devices (computers, laptops, tablets, and phones)
- storage devices (hard drives and USB keys)
- peripherals (printers, scanners, monitors, keyboards, mouses, and docking stations)
- Internet-connected devices (point-of-sale devices, smart security systems, and smart speakers, other Internet of Things devices)
- digital assets and services (social media accounts, websites, cloud and online bookkeeping services)

Backup data

If your networks, systems, or information are compromised by a threat, such as ransomware, or damaged from a natural disaster, a backup enables your organization to reduce the risk of data loss, minimize downtime, and restore its essential services. To learn more, see Tips for backing up your information (ITSAP.40.002).

- ☐ Have you identified which business information and software is essential to your organization and your business continuity?
- ☐ Have you determined how often you will backup your information and systems?
- ☐ Have you backed up systems containing essential business information?
- ☐ Have you tested your backups and your recovery process?
- ☐ Are your backups stored securely (e.g. an offsite location, offline and unconnected to your systems) and only accessible to authorized individuals?

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Foundational cyber security actions for small organizations

CANADIAN CENTRE FOR CYBER SECURITY

April 2023 | ITSAP.10.300

Install preventative security tools

Install security software on your networks and devices to add a layer of protection. Security software like anti-virus software scans systems and files for malware, blocks it from downloading, and detects anomalies or malicious behaviour. A virtual private network (VPN) acts as a tunnel that allows your encrypted data to go through the Internet securely, and away from malicious actors. Ensure that your organization has security software installed on its networks and devices. Consider a protective domain name system (PDNS) service to protect your employees from inadvertently visiting potentially malicious domains on the Internet. To learn more, see Preventative security tools (ITSAP.00.058) and Protective domain name system (ITSAP.40.019).

- ☐ Do you have anti-virus or anti-malware software installed?
- ☐ Have you enabled automatic updates for security software?
- ☐ Are you using a VPN?
- ☐ Do you have a firewall set up between your corporate network and the Internet?
- ☐ Are you using a PDNS service, such as the Canadian Shield, free from the Canadian Internet Registration Authority (CIRA)?

Train employees on basic cyber security practices

Proper training is one of your first lines of defence against cyber threats. Training ensures that your employees understand the security risks associated with their actions and how to identify cyber attacks they may encounter through email or on the web. To learn more, see Offer tailored cyber security training to your employees (ITSAP.10.093) and Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101).

- ☐ Do your employees know how to identify suspicious links or email attachments?
- ☐ Do you offer cyber security training to all employees?
- ☐ Do your employees know how to respond to unsolicited phone calls, text messages, or emails?
- ☐ Do you have a computer usage policy on safe and appropriate ways to use your network, software, devices, and the Internet (e.g. not using unauthorized USB devices or external memory cards, not downloading applications from non-approved sources)?
- ☐ Do you have a phishing awareness program?

Useful resources for help with securing your mobile devices:

- **Using your mobile device securely (ITSAP.00.001)**
- **Security considerations for mobile device deployments (ITSAP.70.002)**

Have an incident response plan ready

Cyber threats, natural disasters, and unplanned outages impact your network, systems, and devices. While you may think your organization won't experience an incident, many Canadian businesses are experiencing heightened threats or the tangible impacts of cybercrime. By having an incident response plan (IRP), your organization will be prepared to respond to and recover from incidents when they happen. To learn more, see Developing your incident response plan (ITSAP.40.003). A free IRP template is available from ISED's CyberSecure Canada website.

- ☐ Do you have an incident response plan describing how your organization will respond to incidents of varying types and severity?
- ☐ Do you know who is responsible for handling incidents (e.g. internal teams, managed service providers, external support team)?
- ☐ Do you have the contact information for your points of contact (e.g. IT partners, providers, and stakeholders) written down and accessible even if your systems and devices are inaccessible?
- ☐ Have you tested your IRP and updated it with lessons learned?

These foundational security actions will help your organization begin to build its cyber security resilience. However, residual risk will still remain. If your organization has the capacity and is ready to implement more security actions, consider:

- **Outsourcing security to a managed service provider (MSP) or cloud service provider (CSP).** They can remotely manage or host all or part of your organization's information technology (IT) infrastructure, monitor and patch security devices and systems, as well as take actions on your IT systems to prevent compromises. Many of their services are offered on-demand so cost and complexity are scalable according to your organization's needs and resources. To learn more, see Choosing the best cyber security solution for your organization (ITSM.10.023).
- **Setting up a secure administrator workstation** that is isolated from the network and doesn't have web browsing or email enabled. It should be a bare minimum workstation that doesn't have capability to install other software.

You may also want to check out CyberSecure Canada's certification program that helps SMOs implement security controls from Canada's national standard, CAN/CIOSC 104:2021 Baseline cyber security controls for small and medium organizations. The program offers free eLearning modules to help your organization learn how to implement the controls.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada