Top measures to enhance cyber security for small and medium organizations

CANADIAN CENTRE FOR CYBER SECURITY

February 2024 | ITSAP.10.035

Looking for steps you can take to protect your organization's networks and information from cyber threats? To get you started, we have summarized the 13 security control categories that are identified in our *Baseline Cyber Security Controls for Small and Medium Organizations*. By implementing these controls, you can reduce your risks and improve your ability to respond to security incidents. We encourage you to adopt as many as possible to enhance your cyber security.

How to use these controls

These controls are not a one-size-fits-all approach to cyber security. They are guiding principles that you can use to create your organization's own cyber security framework.

You should scope and tailor these controls based on your organization's needs and requirements. Implement as many of these controls as possible to enhance your cyber security posture and help minimize the risk of cyber attacks. Start with the following 4 controls to strengthen your organization's security:

- develop an incident response plan
- patch operating systems and applications
- enforce strong user authentication
- backup and encrypt data

Before implementing the controls, keep the following tips in mind:

- identify the critical information assets and systems to which you will apply these controls
- understand the main threats to your organization
- identify your valuable information and systems and apply risk management plans to enhance your security posture
- implement some or all of these controls and you will see a significant impact on improving your organization's resilience and protection against cyber threats

Develop an incident response plan

If you have a plan, you can quickly respond to incidents, restore critical systems and data, and keep service interruptions and data loss to a minimum. In a small organization, for example, this could include having a list of people to call when an incident occurs. Your plan should include strategies for backing up data.

Developing your IT recovery plan (ITSAP.40.004)

Developing your incident response plan (ITSAP.40.003)

Have you been hacked? (ITSAP.00.015)

How to prevent and recover from ransomware (ITSAP.00.099)

Patch operating systems and applications

When software issues or vulnerabilities are identified, vendors release patches to fix bugs, address known vulnerabilities, and improve usability or performance. Where possible, activate automatic patches and updates for all software and hardware to prevent threat actors from exploiting these issues or security vulnerabilities.

How updates secure your devices (ITSAP.10.096)

Enforce strong user authentication

Implement user authentication policies that balance security and usability. Ensure your devices authenticate users before they can gain access to your systems. Wherever possible, use two-factor authentication (2FA) or multi-factor authentication (MFA).

Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)

Steps for effectively deploying multi-factor authentication (ITSAP.00.105)

Best practices for passphrases and passwords (ITSAP.30.032)

Rethink your password habits to protect your accounts from hackers (ITSAP.30.036)

Backup and encrypt data

Copy your information and critical applications to 1 or more secure locations, such as the cloud or an external hard drive. If a cyber incident or natural disaster happens, these copies can help you continue business activities and prevent data loss. Backups can be done online or offline and can also be done in 3 different iterations: full, differential or incremental. Test your backups regularly to ensure you can restore your data.

Tips for backing up your information (ITSAP.40.002)

Using encryption to keep your sensitive data secure (ITSAP.40.016)

Communications Security Establishment
Centre de la sécurité des télécommunications

Cat. No. D97-1/10-035-2024E-PDF ISBN 978-0-660-69930-1

Canada

CANADIAN CENTRE FOR CYBER SECURITY

Top measures to enhance cyber security for small and medium organizations

February 2024 | ITSAP.10.035

Activate security software

Activate firewalls and install anti-virus and anti-malware software on your devices to thwart malicious attacks and protect against malware. Ensure you download this software over a secure network and from a reputable provider. Install Domain Name System (DNS) filtering on your mobile devices to block out malicious websites and filter harmful content.

Preventative security tools (ITSAP.00.058)

Protective domain name system (ITSAP.40.019)

Secure portable media

Storing and transferring data using a portable media device, like a USB key, is convenient and cost-effective. However, it can be prone to loss or theft. Maintain an inventory of all assets. Use encrypted portable storage devices, if possible, and sanitize devices properly before reusing or disposing of them.

Security tips for peripheral devices (ITSAP.70.015)

Sanitization and disposal of electronic devices (ITSAP.40.006)

Access control and authorization

Apply the principle of least privilege to prevent unauthorized access and data breaches. Employees should only have access to the information that they need to do their jobs. Each user should have their own set of login credentials and administrators should have separate administrative accounts and general user accounts.

Managing and controlling administrative privileges (ITSAP.10.094)

Train your employees

Tailor your training programs to address your organization's cyber security protocols, policies and procedures. Depending on the size of your organization, training could be developed in-house or purchased through a reputable vendor. Having an informed workforce can reduce the likelihood of cyber incidents.

Offer tailored cyber security training to your employees (ITSAP.10.093)

Configure devices securely

Take the time to review your device's default settings and make modifications as required. At a minimum, we recommend changing default passwords (especially administrative passwords), turning off location services and disabling unnecessary features.

Cyber security at home and in the office: secure your devices, computers and networks (ITSAP.00.007)

Secure websites

Protect your website and the sensitive information it collects. Encrypt sensitive data, ensure your certificates are up to date, use strong passwords or passphrases on the back-end of the site, and use HTTPS for your site. If you have outsourced your website, ensure your site's host has security measures in place.

Website defacement (ITSAP.00.060)

Secure cloud and outsourced services

Get to know a service provider before you contract them. Make sure the service provider has measures in place to meet your security requirements and needs. Know where a service provider's data centres are located. Different countries have different privacy laws and data protection requirements.

Benefits and risks of adopting cloud-based services in your organization (ITSE.50.060)

Models of cloud computing (ITSAP.50.111)

Cyber Security Considerations for Consumers of Managed Services (ITSM.50.030)

Secure mobile devices

Choose a device deployment model. Will your organization provide employees with corporately owned devices, or will you allow employees to use personal devices for work? Ensure employees can only use approved applications and can only download applications from trusted sources.

Security considerations for mobile device deployments (ITSAP.70.002)

Establish basic perimeter defences

Defend your networks from cyber threats. For example, use a firewall to defend against outside intrusions by monitoring incoming and outgoing traffic and filtering out malicious sources. Use a virtual private network (VPN) when employees are working remotely to secure the connection and protect sensitive information.

Virtual private networks (ITSAP.80.101)

Security tips for organizations with remote workers (ITSAP.10.016)

Communications Security Establishment
Centre de la sécurité des télécommunications