Don't assume you are cyber-safe!

Ask your IT manager these important questions.

Because your business is riding on it.

The following information has been provided by the Canadian Centre for Cyber Security and is being made available to CKCA Members through our membership in the CCTX.

From the CCCS publication on Baseline Security Controls for SMO

- Do we know which of our assets and information systems are the most critical?
- Do we have an up to date network diagram?
- Have we assessed the potential injury to the confidentiality, integrity and availability of our assets and information systems?
- What are our commitments to continuously improving our cybersecurity posture?
- Do we have an incident response plan that has been tested and updated with lessons learned?
    - Cyber Incident Advice and Guidance : https://cyber.gc.ca/en/incident-management
    - Incident Response Plan Template : https://cyber.gc.ca/en/guidance/developing-your-incident-response-plan-itsap40003
- Do we have a cybersecurity insurance policy? If not, why?
- Do we automatically patch all SW and HW and replace those that are not capable of automatic updates?
- Do we have anti-virus and anti-malware solutions that scan and run automatically? Do we have the appropriate SW firewalls in place?
- Do we use secure configurations for all our devices? Change the default passwords and turn off unnecessary features?
- Have we implemented two factor authentication? Do we have clear policies on password length, reuse and password managers?
- Do we provide cybersecurity awareness training to all employees?
- Do we backup systems that contain essential business information using off-line backups? Have we tested the backups? Are backups stored in an encrypted state?
- Do we enforce separation between work and personal data on mobile devices with access to corporate IT systems?
- Have we isolated internet-facing servers from the rest of the corporate network? Have we implemented protected DNS firewall for outbound DNS requests?
- Do we require VPN connectivity with two factor authentication for all remote access to corporate networks?
- Do we prevent corporate devices from connecting to public wifi?
- Do our websites meet OWASP ASVS Level 1 guidelines?
- Do we require that cloud service providers have a report that states they achieved Trust Service Principles compliance? Is all of our data saved in Canada?
- Do we have a cybersecurity policy?
- Have we assessed our cybersecurity posture? Do we know how well we are doing compared to similar organizations in our Sector in Canada?
- If we are working with managed service provider, are we aware of their cybersecurity posture? Cyber Security Considerations For Consumers of Managed Service
- What security controls are in place to protect against ransomware? Ransomware: How to Prevent and Recover

The NIST Cybersecurity Framework consists of the following 5 elements: Identify, Protect, Detect, Respond, Recover. For each, have we done the following?

Prepared July 2021

Don't assume you are cyber-safe!

Ask your IT manager these important questions.

Because your business is riding on it.

The following information has been provided by the Canadian Centre for Cyber Security and is being made available to CKCA Members through our membership in the CCTX.

Identify: Do we have the ability to manage cybersecurity risks to assets and systems?
Protect: Have we implemented safeguards to ensure delivery of critical services?
Detect: Are we able to identify the occurrence of a cybersecurity event?
Respond: Are we able to take appropriate action if a cybersecurity incident has occurred?
Recover: Do we have business continuity plans that will restore capabilities that might be impaired due to a cyber event?

Resources:
To assist with identifying cybersecurity posture:

- The Canadian Cyber Security Tool (CCST)
- Canadian Cyber Resilience Review (CCRR)
- Network Security Resilience Analysis tool (NSRA)
- Harmonized Threat and Risk Assessment Methodology

To assist with cyber threat awareness, the Cyber Center offer the following products:

- Alerts and Advisories : https://cyber.gc.ca/en/alerts-advisories
- Reports and Assessments : https://cyber.gc.ca/en/reports-assessments
- Publications : https://cyber.gc.ca/en/publications
- Get Cyber Safe : https://www.getcybersafe.gc.ca/en
- Cyber Security Awareness Month : https://www.getcybersafe.gc.ca/en/cyber-security-awareness-month
- Geekweek : https://cyber.gc.ca/en/events/geekweek-7
- Learning Hub : https://cyber.gc.ca/en/learning-hub

To assist with detection, the Cyber Center offers the following services (free). If you are interested in any of these services, please email contact@cyber.gc.ca

- Malware Analysis tool
- Real time IoC threat feed
- Vulnerability notifications

You are encouraged to report any cyber incident to the Cyber Center at:
https://cyber.gc.ca/en/incident-management.

If you want to join a cyber collaboration organization please contact info@cctx.ca

Jennifer J. Quaid
Chief Operating Officer
Canadian Cyber Threat Exchange (CCTX)
Mobile: +1-613-292-7016
jennifer.quaid@cctx.ca
www.CCTX.ca

Canadian Cyber Threat Exchange
Informing Canadian Business

Échange canadien de menaces cybernétiques
Informer les entreprises canadiennes

Prepared July 2021