The Canadian Centre for Cyber Security Releases Baseline Controls

Antoine Guilmain and Eliane Ellbogen
Fasken Martineau DuMoulin LLP

The Canadian Centre for Cyber Security Releases Baseline Controls

By: Antoine Guilmain and Eliane Ellbogen

The Canadian government's Canadian Centre for Cyber Security ("CCCS") has released *Baseline cyber security controls for small and medium organizations* in an effort to help small and medium sized businesses improve their cyber security practices and their overall resiliency to cyber security threats.

Small and medium sized businesses face a range of cyber threats in the form of cybercrime, often with immediate financial or privacy implications, such as compromised customer data, financial information, and proprietary information. With this in mind, the baseline controls provide a condensed set of advice, guidance, and security controls on how such businesses can maximize the effectiveness of their cyber security investments. In this bulletin, we review key features of the guidance.

Assessment

Cyber security ostensibly depends on a multitude of factors. As such, businesses are encouraged to apply the controls that are most appropriate for their circumstances and that best suit their cybersecurity needs. Businesses should conduct a five-step assessment to appraise those needs:

1) Size assessment: The proposed baseline controls are intended for businesses with fewer than 499 employees.

2) Information systems and assets fall within the scope of cyber-protection: Information systems and assets refer to all computers, servers, network devices, mobile devices, information systems, applications, services, and cloud applications that are used to conduct business. It is strongly recommended that all information systems and assets be considered within the scope for baseline controls.

3) Value of information systems and assets: The injury level related to the confidentiality, integrity, and availability of information systems and/or data should be assessed. The baseline controls are intended for situations where all potential injuries are at or below a medium threat level.

4) Primary threat of concern: If a business operates in a strategic sector of the economy or faces more advanced cyber security threat levels, it should invest in more comprehensive cyber security measures.

5) Primary cybersecurity investment levels: Someone in a leadership role who is specifically responsible for IT security should be identified. Then, the business's financial spending levels as well as internal staffing levels for IT and IT security should be assessed.

Identification of Baseline Controls

Once the five-part assessment has been conducted, a business is in a position to determine which baseline controls it is relevant to implement to reduce the risk of cyber security incidents and data breaches.

The CCCS proposes the following thirteen baseline controls:

1) Develop an incident response plan: Businesses should have a basic plan for how to respond to incidents of varying severity, namely a written incident response plan (both in soft and hard copy) that details who is responsible for handling incidents including any relevant contact information for communicating to external parties, stakeholders, and regulators. Businesses should also consider purchasing a cyber security insurance policy and implementing a security information and event management system.

2) Automatically patch operating systems and applications: Businesses should enable automatic updates for all software and hardware or establish full vulnerability and patch management solutions, as well as conduct risk assessment activities.

3) Enable security software: Businesses should configure and enable anti-virus and anti-malware software that update and scan automatically, on all connected devices.

4) Securely configure devices: Businesses should implement secure configurations for all devices, namely changing default passwords, turning off unnecessary features, and enabling relevant security features.

5) Use strong user authentication: Businesses should implement two-factor authentication wherever possible and require it for important accounts, namely financial accounts, system administrators, cloud administration, privileged users, and senior executives. Businesses should also have clear policies on password protection and only enforce password changes on suspicion or evidence of compromise.

6) Provide employee awareness training: As a first line of defence, businesses should train employees on basic security practices and focus on practical and easily implementable measures, such as effective password policies, identification of malicious emails and links, approved software, appropriate usage of the Internet, and safe use of social media.

7) Backup and encrypt data: Businesses should backup systems that contain essential business information at a secure offsite location and ensure that recovery mechanisms operate as expected. Backups should be stored in an encrypted state, with restricted access for testing or restoration activities only.

8) Secure mobility: Businesses should implement a mobility management solution for all mobile devices and decide on an ownership model for mobile devices. Whether mobile devices are business or employee-owned, there should be a separation between work and personal data, including apps, email accounts, and contacts. Businesses should ensure that employees download mobile apps from a list of trusted sources and require that all mobile devices store sensitive information in a secure, encrypted state. Businesses should

also require users to disable automatic connections to open networks, avoid connecting to unknown Wi-Fi networks, limit the use of Bluetooth and NFC for the exchange of sensitive information, and use corporate Wi-Fi or cellular data network connectivity rather than public Wi-Fi.

9) Establish basic perimeter defences: Businesses should have a dedicated firewall, with a DNS firewall for outbound DNS requests to the Internet, and activate software firewalls on devices within their networks. Businesses should require secure connectivity to all corporate IT resources and VPN connectivity with two-factor authentication for all remote access into corporate networks. Only secure Wi-Fi, never public Wi-Fi networks, should be used. Businesses should follow the Payment Card Industry Data Security Standard for all point-of-sale terminals and financial systems and further isolate these systems from the Internet and should ensure the implementation of DMARC on all of the business's email services.

10) Secure cloud and outsourced IT services: Businesses should require that all their cloud service providers comply with Trust Service Principles or, alternatively, evaluate their comfort level with how and where their outsourced IT providers handle, access, store, and use their sensitive information. Businesses should also ensure that their IT infrastructure and users communicate securely with the cloud.

11) Secure websites: Businesses should ensure that their websites meet the Open Web Application Security Project's *Application Security Verification Standard* guidelines.

12) Implement access control and authorization: Businesses should follow the principle of least privilege, where users have only the minimal functionality required to perform their tasks. Administrative accounts should face further restrictions where only administrative actions (and not user-level activities like browsing the web or accessing email) are permitted. Larger businesses should implement a centralized authorization control system.

13) Secure portable media: Businesses should limit the use of portable media to commercial encrypted drives provided by the business and have strong asset controls and require the use of encryption on all such devices. These controls should include the proper disposal of portable media, including the use of the wipe functions provided by some devices.

Generally speaking, to avoid suffering costly reputational damage, productivity losses, intellectual property theft, operational disruptions, much less costly recovery expenses, it is recommended that businesses adopt the thinking that they will inevitably suffer a data breach at some point and should thus be in a position to detect, respond, and recover accordingly. Businesses looking to go beyond the proposed baseline controls are encouraged to look to more comprehensive cyber security measures, such as the Center for Internet *Security Controls*, the NIST *Cyber Security Framework*, ISO/IEC *Information technology – Security techniques – Information security management systems – Requirements* or CCCS *IT Security Risk Management: A Lifecycle Approach*.