clia

[CANADIAN LAWYERS INSURANCE ASSOCIATION]

CYBER COVERAGE ELIGIBILITY REQUIREMENTS

MANDATORY PROGRAM

Good data, computer and network hygiene is critical for any business. The following minimum standards are necessary for coverage respond:

Eligibility Requirement	Why its Required	Helpers for Lawyers
Backup Controls: Weekly backups of data, stored offsite, and tested at least annually.	Backups ensure that your organization can be restored after a ransomware attack. It is important that one set of regular backups is kept completely disconnected from your organization's network.	Backing up data is a minimum IT "hygiene" requirement. If a lawyer/law firm is unsure if they back their data up, they should reach out to an IT provider. Most IT providers should be able to assist in setting up data backups. Ridge Canada recommends **inCyber** for assistance on a fixed fee consultation.
Patching: Application of critical patches to your systems, anti-virus software, and anti-spyware software must be made within two weeks of release.	Patching repairs any vulnerabilities that are discovered in your systems and software over time.	There are multiple patch management software applications that IT or security teams can leverage, and in many cases, this is as simple as turning on an automatic update feature.
Anti-Virus/Firewalls: Installation and maintenance, and active monitoring within reasonable business practices, of firewalls and endpoint protection (also known as anti-virus and anti-spyware)	Firewalls and endpoint protection help to prevent unwanted access to IT systems.	A firewall is typically a part of the hardware provided by the internet company you use. End point protection (such as antivirus software) including the free Windows Defender software included with Windows is typically automatically installed or can easily be installed on the firm's systems/computer to protect them from intruders and viruses. Lawyers/law firms should ensure these are turned on and in place.

Eligibility Requirement	Why its Required	Helpers for Lawyers
Multifactor Authentication (MFA): MFA is an authentication method that requires the user to provide two or more verification factors to gain access. MFA must be enabled on email accounts and for remote network access (also known as VPN or Virtual Private Networking, or remote desktop access).	Hackers are gaining unauthorized access to networks by stealing log-in credentials, often times through phishing. By requiring multi-factor authentication, you drastically reduce the likelihood of an unauthorized third-party in possession of a username and password from accessing your computer email and network.	If you use Office 365, you can click **here** for instructions on setting up MFA. If you use Gmail, go to this link for support on MFA **https://safety.google/authentication/** If you use an email system other than Microsoft or Gmail, you should contact your service provider for guidance on turning MFA on.
Email Scanning: Email scanning must be enabled on your mail services to ensure each email is scanned before entering your inbox or leaving your sent box for malicious attachments, links, or other content.	Phishing emails continue to exploit people within organizations. Scanning inbound and outbound emails for malicious links, attachments, and content helps strengthen overall defence of the organization by drastically reducing the amount of harmful messages that reach your inbox.	If you use outlook or Gmail, you should check your settings to see if e-mail scanning is enabled. It should automatically be turned on but if not, you should turn it on. For Microsoft support on email scanning click **here**. For Google support on email scanning click **here**. If you use a different email system, you should contact your service provider for guidance on turning this feature on.
Employee Awareness Training: Engage in cyber awareness training on at least an annual basis.	Employees continue to be the most exploitable element of organizational security in Canada; therefore, it is imperative they are trained properly.	The training is not prescriptive, and it could take any form, including law society courses, third party CPD courses, or in-house training, that would qualify as training. There are a number of free online options available for cyber awareness training. The following training has been approved by the cyber insurer: **https://www.clia.ca/loss-prevention#cyber**

EXCESS CYBER STAND-ALONE PROGRAM

Law firms are required to go through an application process for the cyber stand-alone insurance. Law firms applying for insurance must meet certain requirements (typically more extensive than the mandatory requirements) in order to be eligible for insurance. If the applicant fails any of the underwriting questions, they may still be eligible for cyber insurance but with additional underwriting, or they may not be eligible and will be required to make changes to their IT systems and/or processes.

If you would like the underwriting questions for the excess program please reach out to Dave Jackson @ **djackson@clia.ca**