



LEGAL
PRACTITIONERS'
LIABILITY
COMMITTEE

CYBER SECURITY GUIDE FOR PRACTITIONERS

A practical guide to help practitioners
be cybersafe

lplc.com.au



Law firms of all sizes, including sole practitioners, are targeted every day by cyber criminals from all over the world. Most law firms transact large amounts of money and hold confidential information that criminals can sell or use to extort a ransom payment.

Failure to protect your business and your clients' money and information could be costly both financially and to your firm's reputation.

Basic information for everyone

Every staff member in a law firm is responsible for keeping the firm safe from cyber-attack. There are many things that everyone can do, and this guide addresses the six important areas to focus on to help lock the door on cyber-crime. It is important that everyone in a firm understands what the risks are and what part they must play to keep the firm safe.

The Australian Cyber Security Centre website is a good place for everyone to start to review basic information about protecting your business online. Register for the Australian Cyber Security Centre's Alert Service to receive updates on scams, risks and preventative action to protect your firm and your clients.

It is everyone's business

Cybersecurity is not just an IT issue. It is an essential part of today's legal practice and everyone in your firm has a critical role in preventing cyber-crime. There is no silver bullet to protect your firm and your client's money. The concept of cybersecurity must be built into everything people do in a law firm.

The approach to cybersecurity needs to be multi-pronged. This guide sets out six key areas to address, underlines why they are important, what can be done and how to do it. Included in this guide are links to valuable resources and information.

Building on VLSB+C Minimum Cybersecurity Expectations

The VLSB+C Minimum Cybersecurity Expectations are minimum requirements that every Victorian law practice should implement. These expectations establish the baseline cybersecurity controls that legal practitioners should not operate without.

Read more here: <https://lsbc.vic.gov.au/practitioners/practising-law/cybersecurity/minimum-cybersecurity-expectations>

Building on this foundation, the LPLC offers practical uplift recommendations that enhance and extend the VLSB+C controls. These recommendations are informed by professional indemnity claims data, emerging cyber threat intelligence, and industry best practices specifically tailored to the legal profession.

The LPLC's approach provides a structured pathway for law practices to strengthen their cybersecurity posture while maintaining practical implementation that suits firms of all sizes.

1. Protect access to your system



Focus

Human/system interaction - who can get into your systems and how they do it.

Includes controls from VLSB+C minimum cybersecurity expectations:

- Use of strong, unique passwords or passphrases.
- Multi-factor authentication (MFA) for all personal and professional accounts and services.
- Password managers to generate and store secure passwords.
- Don't reuse passwords across accounts.
- Role-based access control – give people access only to what they need.
- Review and revoke access when roles change or people leave.
- Do not use shared logins. If required use an enterprise password manager.
- Don't use administrator accounts for daily tasks.
- Regularly audit staff email rules and forwarding settings to detect unauthorised redirection.

Why this matters

Your technology infrastructure represents the digital gateway to your practice's communications, financial data, and confidential information. Law firms are specifically targeted because cybercriminals understand the high-value data that flows through all legal practices on a daily basis. Implementing robust technology security controls is both a professional obligation and a business necessity.

LPLC enhanced controls

Strong passwords (VLSB+C uplift: passwords and logins)

- Install an enterprise grade password manager for ease of use in the creation and storage of high-strength passwords.

Multi-factor authentication (VLSB+C uplift: multi-factor authentication)

- Implement multi-factor authentication for all devices and cloud-based systems.
- Ensure MFA is operational for both your work and personal devices and accounts.
- Look to implement location-based or phishing-resistant MFA systems.
- Consider moving to a Zero Trust Security Model and other secure alternatives like FIDO2 authentication or hardware security keys.
- For more information search 'Multi-Factor Authentication' on www.cyber.gov.au.

Role-based access control (VLSB+C uplift: access control)

- Limit staff's access to files and applications on the computer system to what is necessary for their role ('need to know') including principals where appropriate.
- Provide remote access only where necessary and specify conditions of use.
- Specify conditions for use of personal devices for work purposes. This may include the use of a work-approved VPN, or a device which has been approved and secured under a BYOD policy.

Example policy line: "Day-to-day work must be performed using standard user accounts with role-based access control; privileged elevations require documented approval. Administrator accounts may only be used for administrative tasks."

When to use a cybersecurity / IT professional

- Firm-wide rollout of an enterprise password manager with groups, policies and audit logs.
- Implementing role-based access control (e.g. finance vs general staff permissions) in Microsoft 365, document management systems, cloud storage and backup systems.
- Setting up conditional access, location-based or phishing-resistant MFA and exploring Zero Trust / FIDO2 or hardware keys.
- Centralised monitoring of suspicious sign-ins, MFA fatigue attacks and anomalous login locations.

Questions / discussion points for the professional

"Given our size and systems, what is a suitable enterprise password manager, and can you:

- *Set our system up with groups (principals, practitioners, support, accounts)?*
- *Enforce strong password policies and MFA?*
- *Give us a simple admin guide for adding/removing staff?"*

"Can you configure conditional access so logins from unusual countries or locations are blocked or require extra verification, and admin accounts are more tightly locked down?"

"What would be the minimum, safe approach for us to adopt hardware security keys (FIDO2) for principals and key accounts?"

2. Keep your systems secure and up to date



Focus

System-based security measures - how you keep your technology hardened against threats.

Includes:

- Apply security updates (patches) regularly – automatically if possible.
- Install and run security/antivirus software with up-to-date virus definitions.
- Set up web filtering to avoid risky content.
- Apply application control (only approved programs can run).
- Turn on automatic screen locking when devices are idle.
- Use only genuine, licensed software.
- Avoid using legacy or unsupported systems unless absolutely necessary.

Why?

Outdated software and operating systems create security gaps that hackers actively target. Maintaining updated and secure systems prevents cybercriminals from exploiting known vulnerabilities to access your practice. Law firms using unsupported software are vulnerable because cybercriminals know these systems have unpatched vulnerabilities that can be easily exploited to gain unauthorised access to your systems and information.

LPLC enhanced controls

Software updates (VLSB+C uplift: security updates)

- Consider the implementation of software vulnerability management tools that automatically scan IT environments for security weaknesses.

Security software (VLSB+C uplift: security software)

- Have reputable security software on all computers (including for remote access) with at least daily updates to the software's signature database and a daily full scan of files.
- Check suitable security software products at the AV Test website of the Independent IT Security Institute <https://www.av-test.org/en/antivirus/business-windows-client/>
- Consider uplifting to an enterprise grade Endpoint Detection and Response (EDR) security solution with real time behavioural analysis.

Network protection (same as VLSB+C: security software point 4)

- Use Domain Name Server (DNS) web-based filtering to block high-risk websites.
- Install a firewall on individual devices. Have the setup and configuration confirmed by your IT professional.

3. Keep information safe and private



Focus

Information security - how sensitive data is stored, shared, and protected.

Includes:

- Avoid free or generic email addresses (e.g. Gmail).
- Restrict the use of removable media such as USB drives.
- Encrypt sensitive documents when storing or sending them.
- Limit sending sensitive documents via email; instead, share them through a secure cloud platform.
- Ensure all external drives are secure.
- Delete or de-identify old client data when no longer required.
- Implement data classification – know what data is sensitive.

Why?

As a legal practitioner, you have both professional and statutory duties to safeguard client information from unauthorised access, disclosure, and loss. Failure to implement adequate information security controls can result in the exposure of sensitive client communications, financial records, and confidential case details. Such breaches can lead to professional disciplinary action, civil liability, regulatory fines, and irreparable damage to your professional reputation.

LPLC enhanced controls

Business grade email (LPLC recommendation)

- Use a business grade hosted email service, rather than using a free web-based email account as the security offered is much higher.
- Install email attachment and link scanning to automatically check emails for malicious files (attachments) and unsafe URLs (links).

Custom domain (LPLC recommendation)

- Use a custom domain name for your email rather than a free or generic email account like Gmail or Yahoo Mail. This makes it harder for cyber criminals to impersonate your email address and provides better security.
- Be aware of spoofing tactics employed by hackers.

Device security (VLSB+C uplift: devices)

- Ensure users return office devices, and can no longer access office systems, once their employment ceases.
- If personal devices are used for work purposes, ensure that the personal devices have a comparable level of cybersecurity protection as the work devices.

Client information (VLSB+C uplift: information security)

- Consider the firm's Privacy Act obligations and where necessary create a publicly available policy.
- Allocate responsibility to a staff member for detecting and reporting breaches.
- Specify how personal information is to be collected, stored, used and deleted, or de-identified, at the end of the information lifecycle.

AI tools and client information (LPLC recommendation)

- Do not enter confidential client information, personal information, privileged material or commercially sensitive information into an unapproved AI product.
- Before using an AI-enabled product, consider whether the provider stores information, where it is stored, how long prompts, inputs and outputs are retained, and whether the provider may use information to train or improve its systems.
- Apply the practice's information-classification, retention, deletion and secure-sharing requirements when using AI tools.
- De-identify information where practical and appropriate.

4. Manage your cybersecurity responsibilities



Focus

Management-level controls - how your practice governs and monitors cybersecurity.

Includes:

- Create and review cybersecurity policies and procedures.
- Set clear rules for how information is collected, stored, shared and disposed.
- Have a backup strategy – at least daily, stored separately and encrypted.
- Test that you can restore from backups regularly.
- Assign a staff member responsible for cyber risk management.
- Conduct regular access reviews and staff offboarding.
- Review and monitor third-party providers and software tools.
- Apply data retention and deletion policies.
- Purchase cyber insurance if appropriate.
- Schedule annual policy and system reviews.

Why?

Written policies clarify what should happen and how people need to act. It gives you the opportunity to consider the risks and put in place strategies to prevent problems before they happen. Written policies and procedures about cyber risk issues provide clarity on how and what every staff member is expected to do to minimise the risk of a cyber incident.

LPLC enhanced controls

Backup Files (VLSB+C uplift: backups)

- Backup files automatically, at least daily.
- Have backup files stored automatically to the cloud.
- If you use cloud-based storage, ensure you backup your data to another tenancy or a local (on-prem) drive.
- Follow the 3-2-1 rule: Keep three copies of data on two different types of media, with one copy stored off-site.
- Consider offline (occasionally connected) and air-gapped (permanently isolated) backup options for data no longer required for daily operations but still required to be retained.
- Ensure your IT professional is backing up your system or delegate the task to someone in the office.

Note: A cloud environment is not necessarily backed up and can be the subjected to ransomware attacks. If you use a cloud tenancy to store your data, you should treat it like any other form of storage and not rely on it as your sole data storage solution.

Centralised information (VLSB+C uplift: incident response and reporting)

- Have a centralised place for storing cyber risk information, including the firm's cyber action plans, policy and up-to-date points of contact which can be accessed by all staff.
- Keep paper copies of the firm's cyber action plans and policy in a readily accessible place.

Staff training (VLSB+C uplift: staff training)

- Schedule regular (bimonthly) cyber security training for all staff including work experience students and interns.
- Undertake professionally developed cybersecurity training from a reputable provider.

Approve and govern AI tools (LPLC recommendation)

- Establish an AI-use policy that identifies approved AI tools, permitted uses, prohibited uses and the categories of information that may be entered into each tool.
- Keep an approved-tool register, including AI features embedded in existing products such as legal research, document review, transcription, email and practice-management systems.
- Before approving an AI product, undertake appropriate legal, privacy, security and vendor-risk review. Consider the provider's security arrangements, data handling, integrations, access controls, incident notification processes and ability to disable or remove the product if necessary.
- Ensure client-facing AI tools, including chatbots, client-support agents and smart intake forms, are assessed for cybersecurity risks before deployment, particularly where they receive untrusted user input or connect with internal systems or client data.

5. Protect clients and respond quickly to incidents



Focus

Client protection and incident response - how you prevent and react to cyber threats.

Includes:

- Create and document a cyber incident response plan.
- Establish policies and procedures for dealing with data and cyber matter.
- Require phone, in-person, or video call verification (Call before you pay) of payment instructions.
- Hold practice drills to test your firm's readiness.
- Know who to contact (e.g. bank, PEXA, LPLC) in case of an incident.
- Notify clients promptly if their data is compromised.
- Maintain a central list of emergency contacts and cyber action plans.

Why?

Cyber-attacks or incidents are now an inevitable reality for everyone, and cyber-criminals see law firms as a soft and lucrative target. It is important to **ACT QUICKLY** to limit any potential damage if you discover you have sent money to a fraudster's bank account or your computer system has been compromised resulting in data breaches and or your system locked. Having a plan will make acting faster and easier, reduce some of the stress and may well be an essential prerequisite for making a claim against any cyber insurance policy the firm has.

LPLC enhanced controls

Electronic funds transfers safety (VLSB+C uplift: client or bank verification)

- Do not act on any instructions received solely via email. Always verify instructions by telephoning the person on the telephone number you received at the commencement of the matter.
- Any emailed payment details must be verified by phone or in person before transferring funds in accordance with LPLC's recommended process
<https://lplc.com.au/resources/practitioner/cyber-fraud-dont-fall-for-it>
- Ensure that the person who verifies any bank details is the same person who makes the transfer.

Document a plan in case of incident (VLSB+C uplift: incident response and reporting)

- Document what to do if a cyber incident occurs. Authorise appropriate people to act immediately and have clearly defined escalation procedures.
- Specify a contact for urgent legal assistance.
- Specify a contact for urgent IT assistance.
- Comprehensive incident response planning should address multiple incident types including account and system compromises, data breaches, ransomware, denial of service attacks, and insider threats.
- Check your IT provider's response capability.
- Consider buying a cyber insurance policy with immediate incident response capability.

AI-related incidents (LPLC recommendation)

- Include AI-related scenarios in cyber incident planning, such as confidential information being entered into an unapproved tool, unauthorised access to an AI account, a compromised AI integration, or a client-facing AI tool being manipulated to disclose information or perform an unintended action.
- Ensure staff know how to promptly report suspected AI-related data exposure or security incidents so the practice can assess, contain and respond to them.

Document procedures to help clients

- Document what to do if your client pays money to the wrong account. The plan should include:
 - Immediately contacting your client and asking them to reverse the transaction with their bank.
 - Asking your client for a copy of the email they acted on.
 - Obtaining instructions to enable you to put the receiving bank on notice that money has been wrongly paid.
 - Notifying LPLC of a possible claim.

Test plans and procedures

- Test everyone knows what they are required to do if something goes wrong:
 - Hold training sessions.
 - Develop and practice a scenario that might happen.
 - Practice how the scenarios would be handled.

Resources

- See Law Council Cyber Precedent <https://cyberprecedent.com.au/lawcouncil/images/cyber/CP-What-to-Do.pdf>
- See LPLC list of Cyber-crime bank contact details <https://lplc.com.au/resources/checklists/cybercrime-bank-contact-list>
- See LPLC's cyber insurance information <https://lplc.com.au/resources/faq/marsh-chubb-cyber-insurance-policy-faqs>

6. Build a cyber-safe culture



Focus

Behavioural control - how people think and act in relation to cyber risk.

Includes:

- Explain and warn clients about email fraud and cyber risks
- Add email footers warning about cyber fraud
- Train all staff (including temps and interns) on cybersecurity basics
- Update training annually and when new threats emerge
- Consider using gamification approaches to cybersecurity training
- Encourage a 'pause before you act' culture around email and web use
- Conduct phishing simulations and spot checks
- Display cyber risk reminders in the office
- Promote a "see something, say something" mindset

Why?

Many cyber incidents, particularly business email compromise, occur because someone clicked on a link that allowed the cyber-criminal into the firm's computer system. Cyber-criminals use sophisticated social engineering to entice people to click. When working at a fast pace it is easy to not stop to think about possible cyber risks in routine work. Developing a culture in the office of healthy scepticism and a 'pause before you act' approach for anything internet related is important to avoid getting caught out. Don't become a casualty of a casual attitude.

LPLC enhanced controls

Create a secure email and browsing culture

- Always verify emailed payment details before transferring funds.
- Create policies, procedures and checklists to ensure payment details are verified.
- Never open unknown attachments or links from unknown senders.
- Regularly audit staff email settings, particularly forwarding rules, security settings, and sign-in activity (recent logins) to ensure their emails are not being redirected by cyber-criminals.
- Don't use public wi-fi for work purposes.
- Use a VPN whenever accessing the internet away from your secure office internet connection.
- Be alert to anything unusual or suspicious and check it appropriately.
- Conduct audits to ensure the process is being followed.
- Prominently display LPLC's Cyber Risk poster at your premises.

Explain risks to clients (VLSB+C uplift: client or bank verification)

- Explain the risks of fraudulent emails to clients in your first face-to-face meeting.
- Use the LPLC client brochure 'Cyber security - how to protect yourself'
<https://lplc.com.au/client-resources/cyber-security-protect-client-brochure/>

Confirm risks (VLSB+C uplift: client or bank verification)

- Confirm the risks of fraudulent emails to clients in writing.
- Update your precedent letter of engagement.

Verify email requests (VLSB+C uplift: client or bank verification)

- As part of your retainer, tell clients, and confirm it in writing, that you require them to verify any email requests by your firm for payment before transferring money.
- Include in your first interview checklist and your precedent letter of engagement information about verifying transfer requests.

Include a warning message (VLSB+C uplift: client or bank verification)

- Add a warning to your email footer about the risks of relying on payment details in email.
- See LPLC article Protect your clients from cyber fraud <https://lplc.com.au/resources/lplc-article/protect-your-clients-from-cyber-fraud>
- Download and use LPLC's 'Call before you pay' email footer or develop your own
<https://lplc.com.au/resources/practitioner/call-before-you-pay>

AI enhanced cyber-attacks (LPLC recommendation)

- Be alert to AI-enhanced or AI-generated material, including highly convincing phishing emails, fake documents, spoofed websites, altered images and voice simulations.
- AI can enable cybercriminals to produce personalised scams at greater speed and scale. Do not treat polished writing, familiar language, apparent urgency or a recognisable voice as proof that a communication is genuine.
- Pause and independently verify unusual, sensitive or payment-related requests using a trusted contact method. Continue to follow the practice's "call before you pay" procedures.

AI awareness and human review (LPLC recommendation)

- Train staff on the practice's AI-use policy, approved tools and rules for handling confidential and client information.
- Encourage staff to report unapproved AI use, suspicious AI-generated content and potential data exposure without delay.

While this guide provides practical steps to strengthen your practice's cybersecurity posture, implementing and maintaining robust cybersecurity controls requires ongoing expertise and vigilance.

The LPLC strongly recommends engaging a qualified cybersecurity professional to conduct a comprehensive security assessment of your practice, assist with implementing the controls based on a relevant standard, and provide ongoing monitoring and maintenance services. A cybersecurity professional can also provide rapid response capability when incidents occur.

This guide represents the LPLC's uplift of the VLSB+C Minimum Cybersecurity Expectations. The VLSB+C expectations are controls that every Victorian law practice should implement. The LPLC provides these enhanced controls to help practices strengthen their cybersecurity posture beyond the minimum expectations.