Navigating the Evolving Landscape of Cyber Threats: An Update on Cyber-Attacks and Scam Profiles

Dr. Fabian Horton | Risk Manager, LPLC

LEGAL PRACTITIONERS' LIABILITY COMMITTEE

lplc.com.au

WELCOME

Today's Schedule

- Recent Trends in Cyber-Attacks
- Control and Cybersecurity Best Practices
- Future Challenges and Emerging Threats
- Key Messages
- Q&A Session

WHY ARE LAWYERS TARGETS?

Handle lots of money

Hold sensitive information

Interact online a lot

Thought to be unsophisticated online

IT IS YOUR RESPONSIBILITY!

- Duty of care (Duty to warn and keep funds safe)
- Solicitors Conduct Rules 2015 Rule 9.1 - duty of confidentiality
- Trust account - Uniform law s154 - must report any irregularity
- Notifiable Data Breach under *Privacy Act (1988)* (Cth)

It's what clients expect

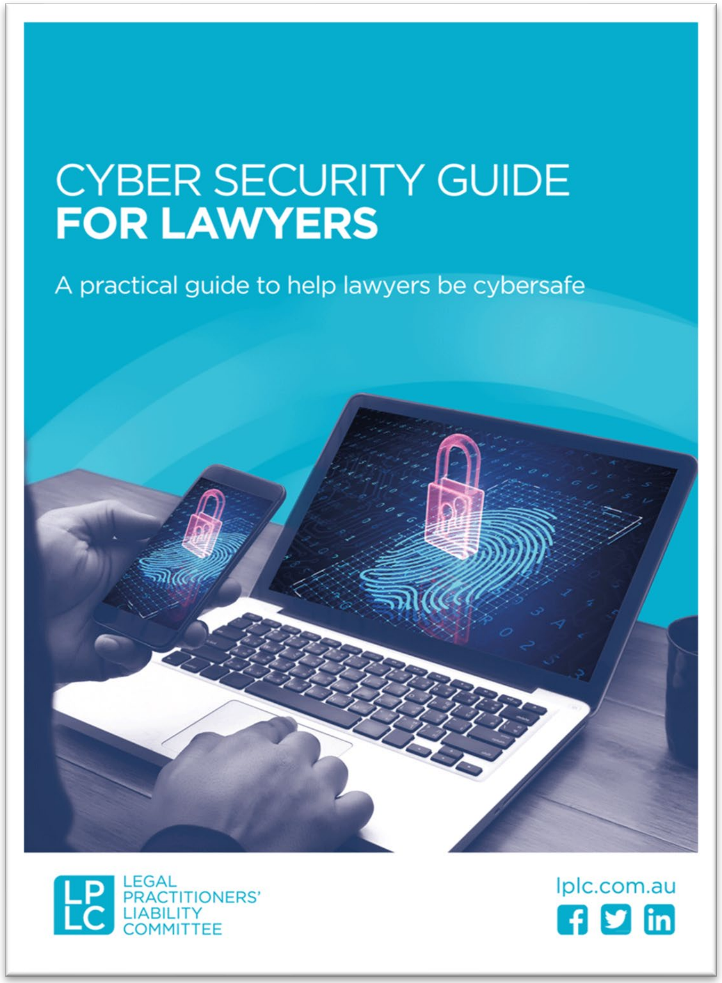
CONSEQUENCES

- Loss of client funds
- Loss of firm funds
- Business interruption
- Failure to keep confidential information safe.
- Fines
- Litigation
- Reputation loss

"I keep our secure files in a coffee can buried behind the office. You can't hack into that with a computer!"

Reputational and business consequences

CYBER SECURITY GUIDE FOR LAWYERS



CYBER SECURITY GUIDE
FOR LAWYERS

A practical guide to help lawyers be cybersafe

LP LC LEGAL PRACTITIONERS' LIABILITY COMMITTEE

lplc.com.au

1. Secure your technology
2. Establish policies and procedures
3. People – a culture of awareness
4. Warn the client
5. An incident response plan

Download at: lplc.com.au

RECENT TRENDS IN CYBER-ATTACKS

DATA BREACH TRENDS AND THREATS

ACROSS ALL ORGANIZATIONS

49%

49% of organizations reported being breached sometime in their history, but recent breach history has decreased from 24% in 2021 to 15% in 2024.

Ransomware attacks are more common, with 28% experiencing an attack (up from 22% last year), but planning is still poor, with only 21% saying they would follow a formal plan in the event of an attack.

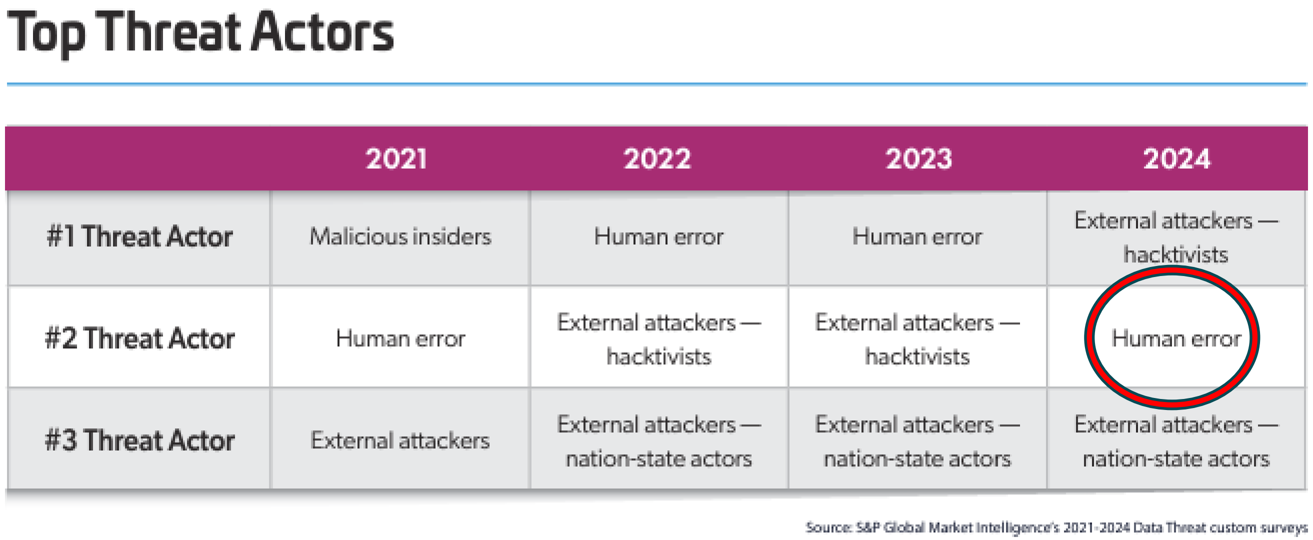
28%

Human factors are still a major cause of cloud data breaches; human error was the leading cause with 31%, and failure to apply MFA to privileged accounts constituted another 17%.

31%

Thales: 2024 Threat Report

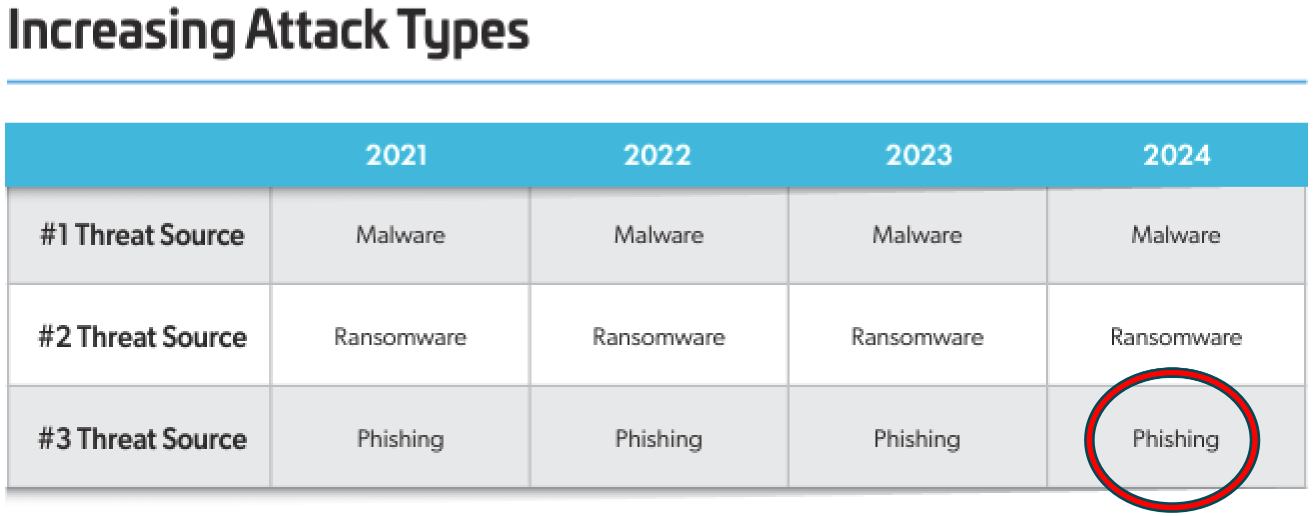
THE TRENDS



Top Threat Actors

	2021	2022	2023	2024
#1 Threat Actor	Malicious insiders	Human error	Human error	External attackers — hacktivists
#2 Threat Actor	Human error	External attackers — hacktivists	External attackers — hacktivists	Human error
#3 Threat Actor	External attackers	External attackers — nation-state actors	External attackers — nation-state actors	External attackers — nation-state actors

Source: S&P Global Market Intelligence's 2021-2024 Data Threat custom surveys

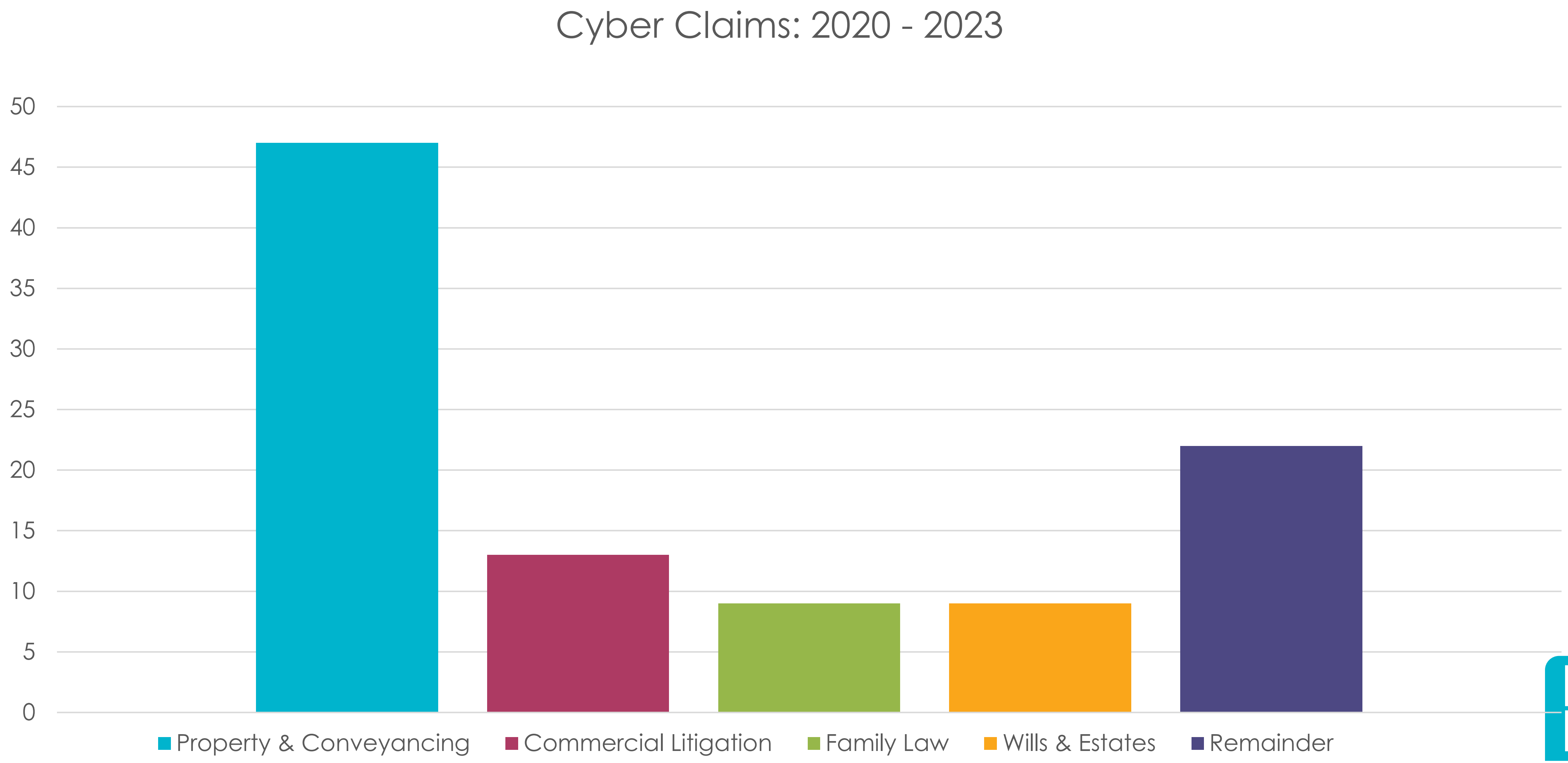


Increasing Attack Types

	2021	2022	2023	2024
#1 Threat Source	Malware	Malware	Malware	Malware
#2 Threat Source	Ransomware	Ransomware	Ransomware	Ransomware
#3 Threat Source	Phishing	Phishing	Phishing	Phishing

Thales: 2024 Threat Report

LPLC CLAIMS TRENDS



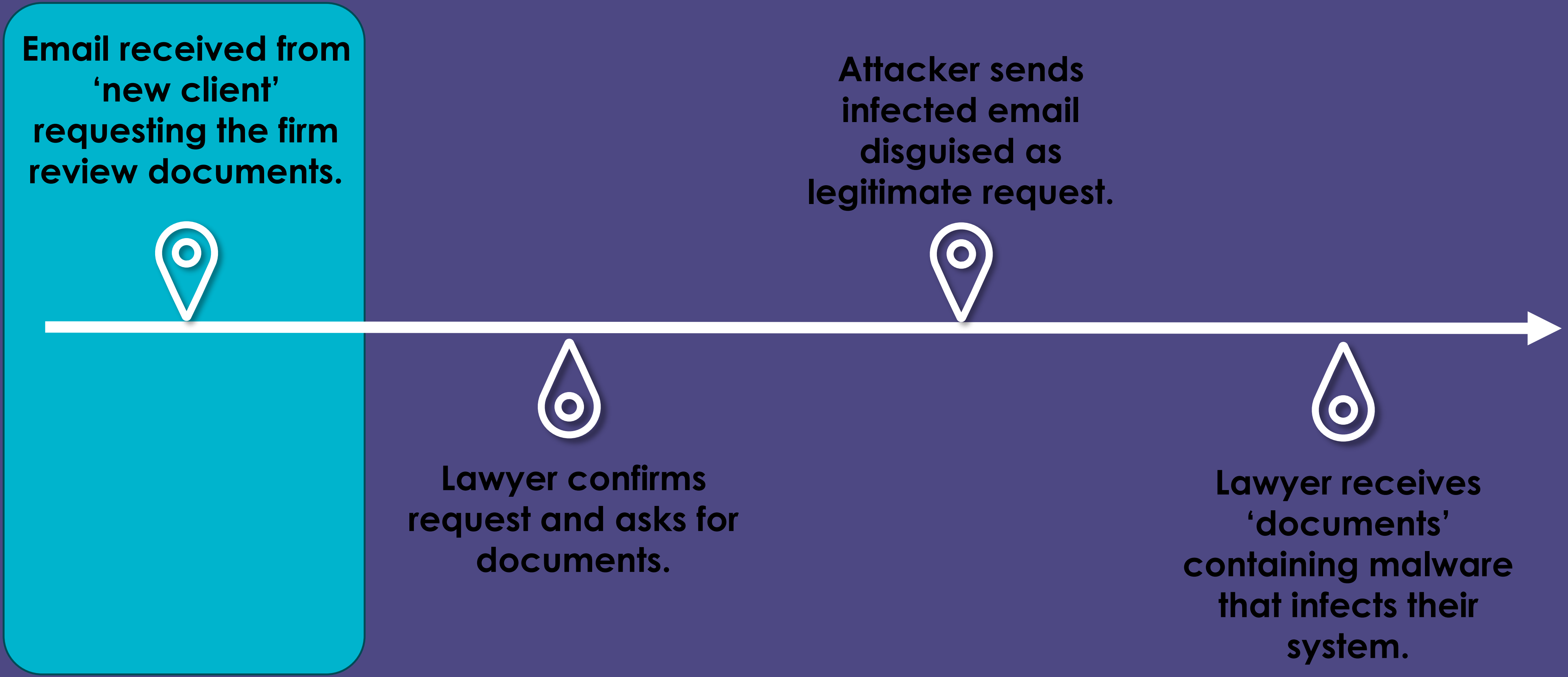
HOW DO THEY GET IN?

There are multiple ways that fraudsters try to access your technology.

Common approaches are:

- **Malware** - someone opens an attachment or link that installs malware
- **Social engineering** - they trick you into giving them details
- **Phishing** – a general email, hoping someone takes the bait
- **Spear phishing** – targeted email such as pretending to be a family member, work colleague, or a business you use like Australia Post.

THE 'YOUR NEW CLIENT' SCAM



Email received from 'new client' requesting the firm review documents.

Lawyer confirms request and asks for documents.

Attacker sends infected email disguised as legitimate request.

Lawyer receives 'documents' containing malware that infects their system.

BUSINESS EMAIL COMPROMISE (BEC) ATTACK

THE COMPROMISE

The attacker obtains access to the lawyer's account via social engineering or malware and determines the best target.

THE SWITCH

The attacker sends a fake email from the compromised account changing banking details. Redirects any incoming email from the target (diversion rules).

THE STEAL

Money from the client is placed into a bank account controlled by the hacker. Fake emails are sent to avoid the lawyer and the client becoming suspicious.

THE DAMAGE

The money is stolen, and the lawyer is left to compensate the client. The lawyer can face disciplinary proceedings.

VLSB CYBER EXPECTATIONS

Minimum Cyber Expectations

System and behavioural controls that law practices should implement

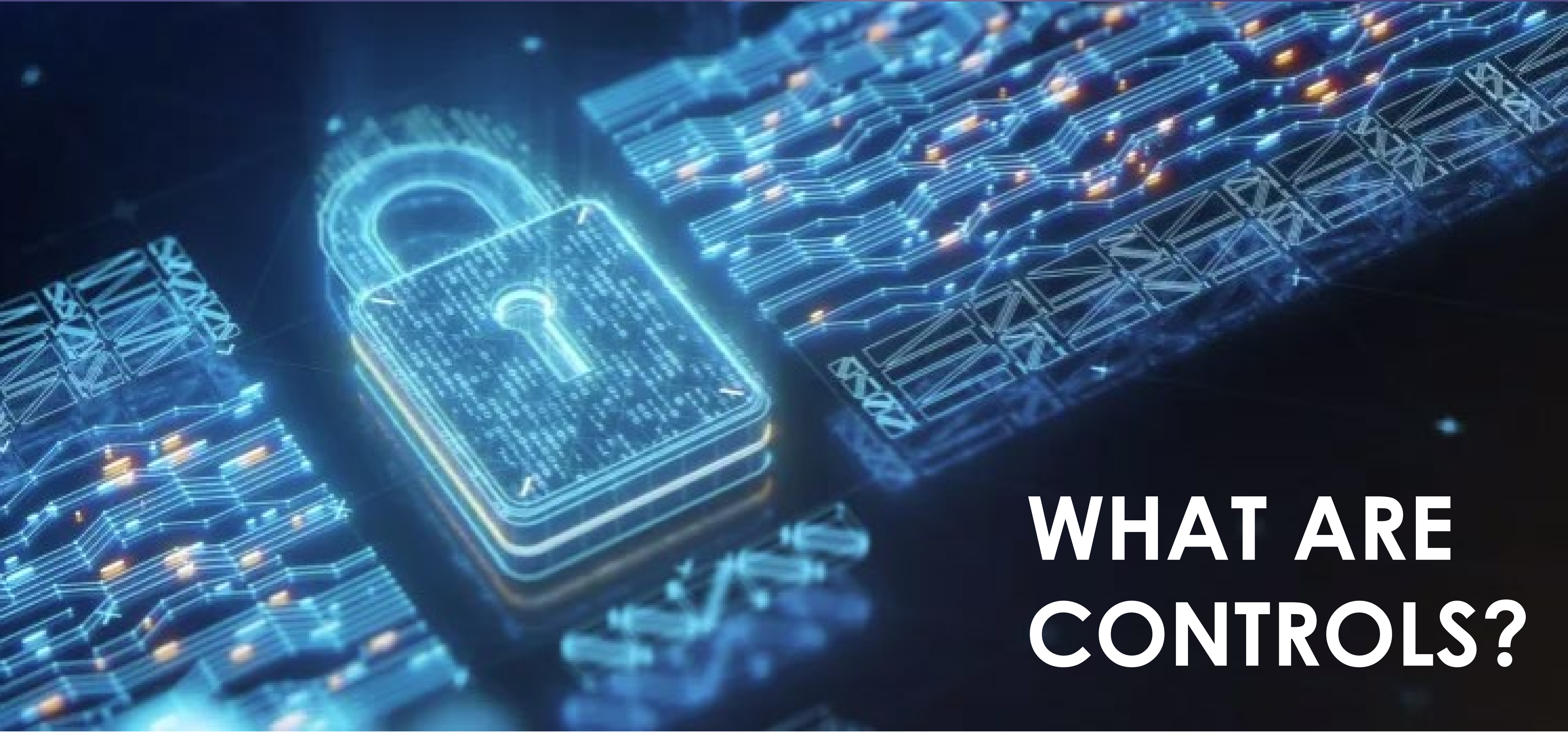
+

Cybersecurity Red Flags and Good Practices

Help lawyers identify warning signs of possible cyber-incidents

CONTROLS AND CYBERSECURITY BEST PRACTICES

VLSB MINIMUM CYBER EXPECTATIONS



WHAT ARE CONTROLS?

TYPES OF CONTROLS

CRITICAL CONTROLS

System controls that can pose a significant risk and should be implemented immediately.

SYSTEM CONTROLS

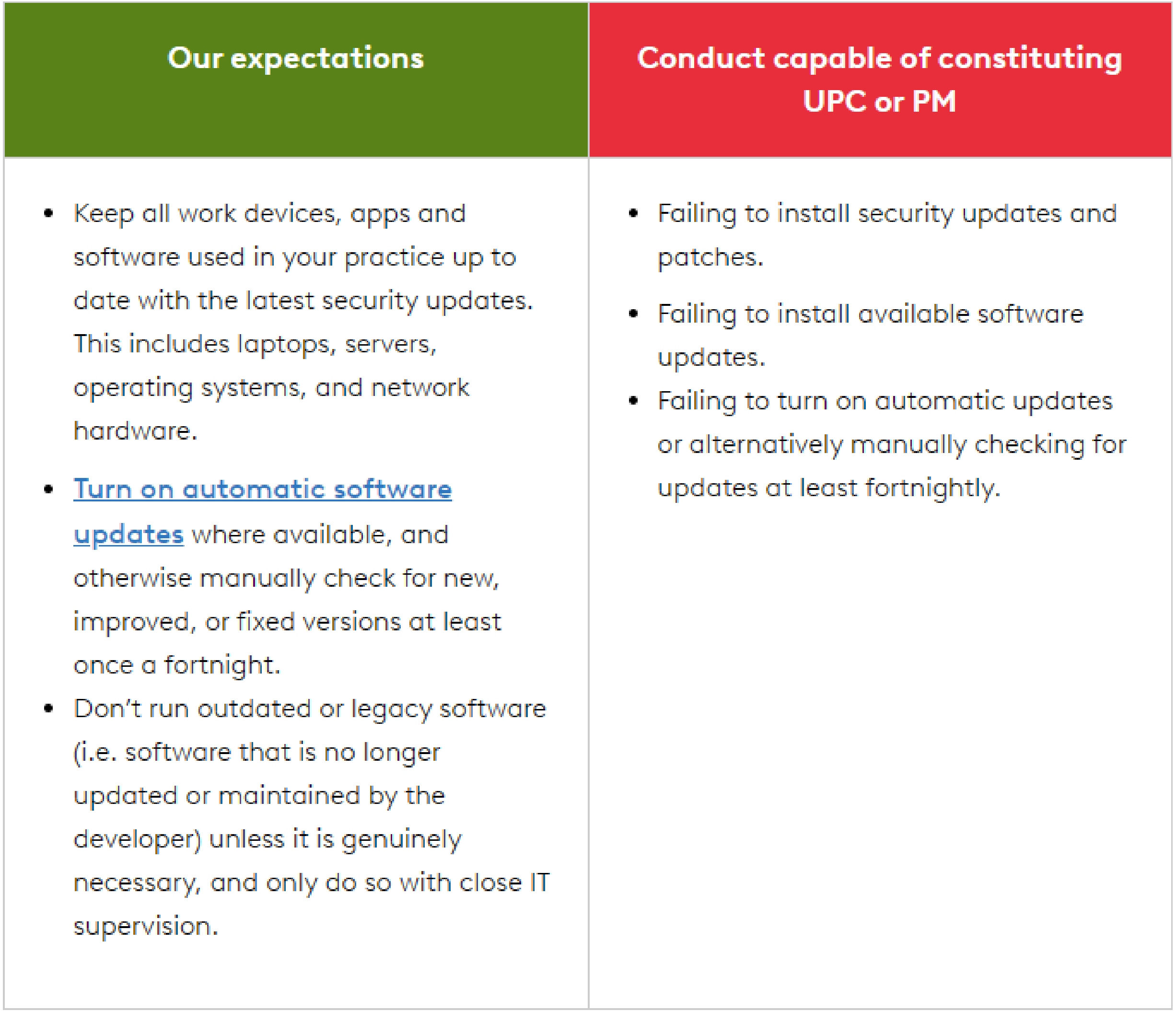
The technical safeguards used within an organisation's system to protect against threats and vulnerabilities.

BEHAVIOURAL CONTROLS

Focus on influencing and regulating human behaviour to minimise security risks

EXPECTATIONS AND POTENTIAL FOR UPC OR PM

To help law practices protect their clients' data and meet their legal and ethical obligations, the following tables set out minimum cybersecurity expectations. They also list examples of unacceptable cybersecurity practices that we consider capable of amounting to unsatisfactory professional conduct (UPC) or professional misconduct (PM).



Our expectations	Conduct capable of constituting UPC or PM
• Keep all work devices, apps and software used in your practice up to date with the latest security updates. This includes laptops, servers, operating systems, and network hardware. • Turn on automatic software updates where available, and otherwise manually check for new, improved, or fixed versions at least once a fortnight. • Don't run outdated or legacy software (i.e. software that is no longer updated or maintained by the developer) unless it is genuinely necessary, and only do so with close IT supervision.	• Failing to install security updates and patches. • Failing to install available software updates. • Failing to turn on automatic updates or alternatively manually checking for updates at least fortnightly.

MINIMUM CYBERSECURITY EXPECTATIONS

Control	Expectations	Conduct
Critical		
Security Updates	3	3
Passwords and logins	7	6
Multi-factor authentication	1	3
System		
Security software	4	3
Access control	6	3
Devices	6	6
Information Security	5	2
Backups	6	3
Behavioural		
Training	5	2
Client or bank verification	5	6
Incident response and reporting	7	3

PLEASE NOTE!

- The following discussion is an outline of the issues contained in the VLSB Minimum Cyber Expectations. It does not cover every issues.
- Practitioners should read the VLSB Minimum Cyber Expectations along with any supporting documents.

CRITICAL CONTROL

CRITICAL CONTROLS

System controls that can pose a significant risk and should be implemented immediately.

SECURITY UPDATES (PATCHING)

Expectation

- Keep all software updated.
- Turn on automatic software updates or check regularly.
- Don’t run outdated or legacy software.

Potential for UPC or PM

- Failing to install security updates and patches.
- Failing to install available software updates.
- Failing to turn on automatic updates or alternatively manually checking for updates at least fortnightly.

PASSWORDS AND LOGINS

Expectation

- Use strong passwords or passphrase.
- Don't use weak or repeated passwords.
- Use a password manager.
- Change passwords regularly.
- Change passwords is you believe there is a compromise.

Potential for UPC or PM

- No or weak passwords.
- Reusing or lending passwords.
- Insecure handling of passwords or devices.

MULTI-FACTOR AUTHENTICATION (MFA)

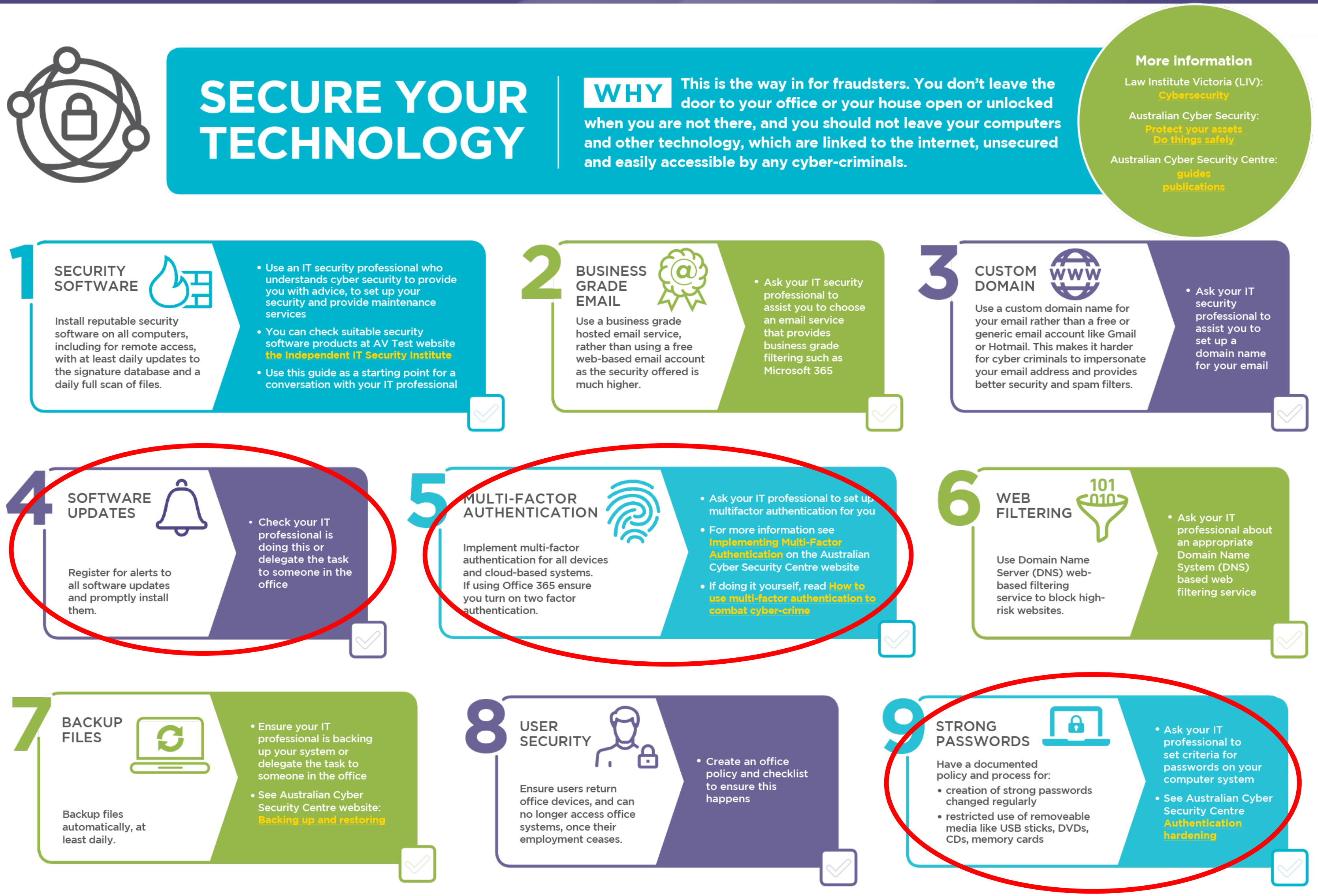
Expectation

- Turn on multi-factor authentication (MFA) on all online accounts and services where it is available.
- Do not disable MFA or ignore the option to turn it on.

Potential for UPC or PM

- Disabling MFA or failing to activate MFA where it is available.
- Sharing MFA codes with others.
- Approving unexpected or unknown sign in attempts in your MFA application or device.

SECURE YOUR TECHNOLOGY



SECURE YOUR TECHNOLOGY

WHY This is the way in for fraudsters. You don't leave the door to your office or your house open or unlocked when you are not there, and you should not leave your computers and other technology, which are linked to the internet, unsecured and easily accessible by any cyber-criminals.

More information

Law Institute Victoria (LIV):
Cybersecurity

Australian Cyber Security:
Protect your assets
Do things safely

Australian Cyber Security Centre:
guides
publications

1 SECURITY SOFTWARE

Install reputable security software on all computers, including for remote access, with at least daily updates to the signature database and a daily full scan of files.

- Use an IT security professional who understands cyber security to provide you with advice, to set up your security and provide maintenance services
- You can check suitable security software products at AV Test website **the Independent IT Security Institute**
- Use this guide as a starting point for a conversation with your IT professional

2 BUSINESS GRADE EMAIL

Use a business grade hosted email service, rather than using a free web-based email account as the security offered is much higher.

- Ask your IT security professional to assist you to choose an email service that provides business grade filtering such as Microsoft 365

3 CUSTOM DOMAIN

Use a custom domain name for your email rather than a free or generic email account like Gmail or Hotmail. This makes it harder for cyber criminals to impersonate your email address and provides better security and spam filters.

- Ask your IT security professional to assist you to set up a domain name for your email

4 SOFTWARE UPDATES

Register for alerts to all software updates and promptly install them.

- Check your IT professional is doing this or delegate the task to someone in the office

5 MULTI-FACTOR AUTHENTICATION

Implement multi-factor authentication for all devices and cloud-based systems. If using Office 365 ensure you turn on two factor authentication.

- Ask your IT professional to set up multifactor authentication for you
- For more information see **Implementing Multi-Factor Authentication** on the Australian Cyber Security Centre website
- If doing it yourself, read **How to use multi-factor authentication to combat cyber-crime**

6 WEB FILTERING

Use Domain Name Server (DNS) web-based filtering service to block high-risk websites.

- Ask your IT professional about an appropriate Domain Name System (DNS) based web filtering service

7 BACKUP FILES

Backup files automatically, at least daily.

- Ensure your IT professional is backing up your system or delegate the task to someone in the office
- See Australian Cyber Security Centre website: **Backing up and restoring**

8 USER SECURITY

Ensure users return office devices, and can no longer access office systems, once their employment ceases.

- Create an office policy and checklist to ensure this happens

9 STRONG PASSWORDS

Have a documented policy and process for:

- creation of strong passwords changed regularly
- restricted use of removeable media like USB sticks, DVDs, CDs, memory cards

- Ask your IT professional to set criteria for passwords on your computer system
- See Australian Cyber Security Centre **Authentication hardening**

SYSTEM CONTROLS

SYSTEM CONTROLS

The technical safeguards used within an organisation's system to protect against threats and vulnerabilities.

SYSTEM CONTROLS

Expectation

- Security software: Install, run, and update security and anti-virus software.
- Access control: Limit access to data and don't share accounts.
- Devices: Encrypt information and create cyber resilient ecosystems.

Potential for UPC or PM

- Ignoring security warnings.
- Sharing accounts or allowing unauthorised access to information.
- Leaving device unattended and without cyber protection.

INFORMATION SECURITY

Expectation

- Encrypt files and communications (unless authorised otherwise).
- Erase or destroy devices no longer required.
- Review client information and other sensitive information to determine if it is still required. Erase if not required.

Potential for UPC or PM

- Storing your client data on unencrypted drives.
- Retaining client files indefinitely, without good reason.

BACKUPS

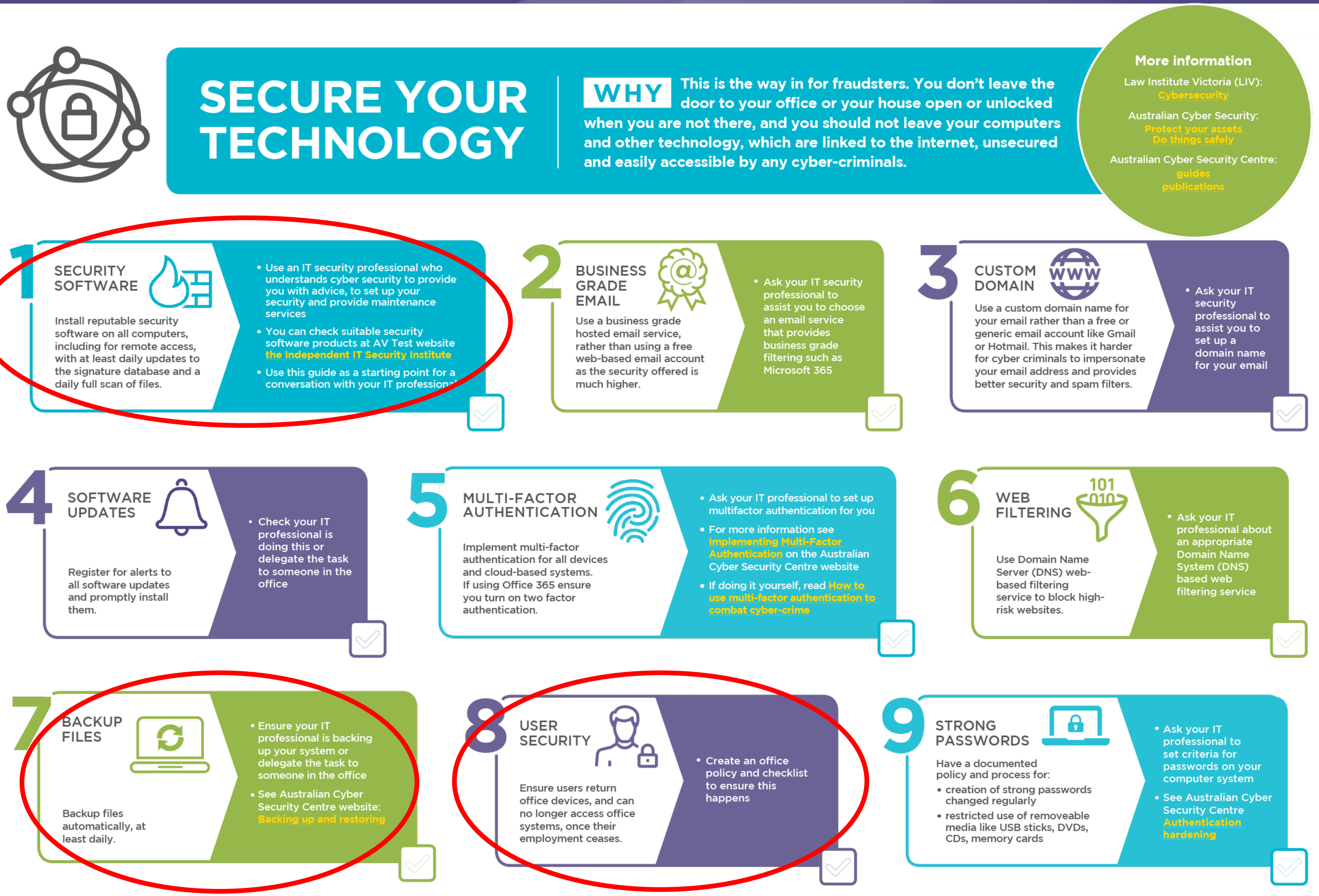
Expectation

- Backup and encrypt files regularly.
- Don’t store backup with primary data.
- Retain backups and logs for an appropriate period.

Potential for UPC or PM

- Not backing up your data.
- Storing backup data unencrypted.
- Failing to retain data, documents, and logs as needed (subject to the information security expectations)

SECURE YOUR TECHNOLOGY



SECURE YOUR TECHNOLOGY

WHY This is the way in for fraudsters. You don't leave the door to your office or your house open or unlocked when you are not there, and you should not leave your computers and other technology, which are linked to the internet, unsecured and easily accessible by any cyber-criminals.

More information

Law Institute Victoria (LIV):
Cybersecurity

Australian Cyber Security:
Protect your assets
Do things safely

Australian Cyber Security Centre:
guides
publications

1 SECURITY SOFTWARE

Install reputable security software on all computers, including for remote access, with at least daily updates to the signature database and a daily full scan of files.

- Use an IT security professional who understands cyber security to provide you with advice, to set up your security and provide maintenance services
- You can check suitable security software products at AV Test website the Independent IT Security Institute
- Use this guide as a starting point for a conversation with your IT professional

☑

2 BUSINESS GRADE EMAIL

Use a business grade hosted email service, rather than using a free web-based email account as the security offered is much higher.

- Ask your IT security professional to assist you to choose an email service that provides business grade filtering such as Microsoft 365

☑

3 CUSTOM DOMAIN

Use a custom domain name for your email rather than a free or generic email account like Gmail or Hotmail. This makes it harder for cyber criminals to impersonate your email address and provides better security and spam filters.

- Ask your IT security professional to assist you to set up a domain name for your email

☑

4 SOFTWARE UPDATES

Register for alerts to all software updates and promptly install them.

- Check your IT professional is doing this or delegate the task to someone in the office

☑

5 MULTI-FACTOR AUTHENTICATION

Implement multi-factor authentication for all devices and cloud-based systems. If using Office 365 ensure you turn on two factor authentication.

- Ask your IT professional to set up multifactor authentication for you
- For more information see Implementing Multi-Factor Authentication on the Australian Cyber Security Centre website
- If doing it yourself, read How to use multi-factor authentication to combat cyber-crime

☑

6 WEB FILTERING

Use Domain Name Server (DNS) web-based filtering service to block high-risk websites.

- Ask your IT professional about an appropriate Domain Name System (DNS) based web filtering service

☑

7 BACKUP FILES

Backup files automatically, at least daily.

- Ensure your IT professional is backing up your system or delegate the task to someone in the office
- See Australian Cyber Security Centre website: Backing up and restoring

☑

8 USER SECURITY

Ensure users return office devices, and can no longer access office systems, once their employment ceases.

- Create an office policy and checklist to ensure this happens

☑

9 STRONG PASSWORDS

Have a documented policy and process for:

- creation of strong passwords changed regularly
- restricted use of removeable media like USB sticks, DVDs, CDs, memory cards

- Ask your IT professional to set criteria for passwords on your computer system
- See Australian Cyber Security Centre Authentication hardening

☑

KEY MESSAGES FOR SYSTEM CONTROLS

1. Data encryption is now expected (mentioned 8 times).

2. A level of technology understanding will be needed for some expectations.

3. No longer a set-and-forget situation. Security control must be constantly reviewed, maintained, and updated.

BEHAVIOURAL CONTROLS

BEHAVIOURAL CONTROLS

Focus on influencing and regulating human behaviour to minimise security risks

TRAINING

Expectation

- Educate new and existing staff on cybersecurity.
- Provide ongoing regular ongoing training.

Potential for UPC or PM

- Not educating staff on how to identify, report, and respond to cyberattacks.
- Not providing your staff with up-to-date cybersecurity training.

AN INCIDENT RESPONSE PLAN

Expectation

- Create, implement, and keep up-to-date an incident response plan.
- Ensure all staff are aware of the response plan
- Report cyber-incidents to ACSC, banks, PEXA, LPLC, VLSB, and clients.

Potential for UPC or PM

- Not establishing a cyber-incident response plan.
- Not reporting and managing security incidents promptly. We will take into account if you have reported incidents to us promptly when considering whether disciplinary action is warranted.
- Underreporting or covering up incidents.

AN INCIDENT RESPONSE PLAN

HAVE AN INCIDENT RESPONSE PLAN FOR PROMPT ACTION

WHY Cyber-attacks or incidents are now an inevitable reality for everyone, even law practices, as more 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 taking action 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.

1 DOCUMENT A PLAN

Document what to do if a cyber incident occurs.

- authorise appropriate people to act immediately
- specify a contact for urgent IT assistance
- document a procedure in the event trust money is paid to the wrong account, including:
  - if it is a PEXA transaction, contact PEXA first
  - who to contact at the firm's bank
  - immediately contact the sending and receiving banks putting both on notice money has been wrongly paid
  - contact LPLC to notify a possible claim
- See Law Council of Australia **Cyber Precedent** website: **What to do if you are cyber-attacked**
- See the information at **Australian Cyber Security** website: **Recover and get help**
- See LPLC list of **Cyber-crime bank contact details**
- See LIV **Cybersecurity information**
- Check your IT provider's response capability
- Consider buying a cyber insurance policy with immediate incident response capability particularly for ***Privacy Act 1988 (Cwlth) data breaches***
- See **LPLC's cyber insurance information.**

☑

2 DOCUMENT PROCEDURES TO HELP CLIENTS

Document what to do if your client pays money to the wrong account.

Your 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

☑

3 TEST PLANS AND PROCEDURES

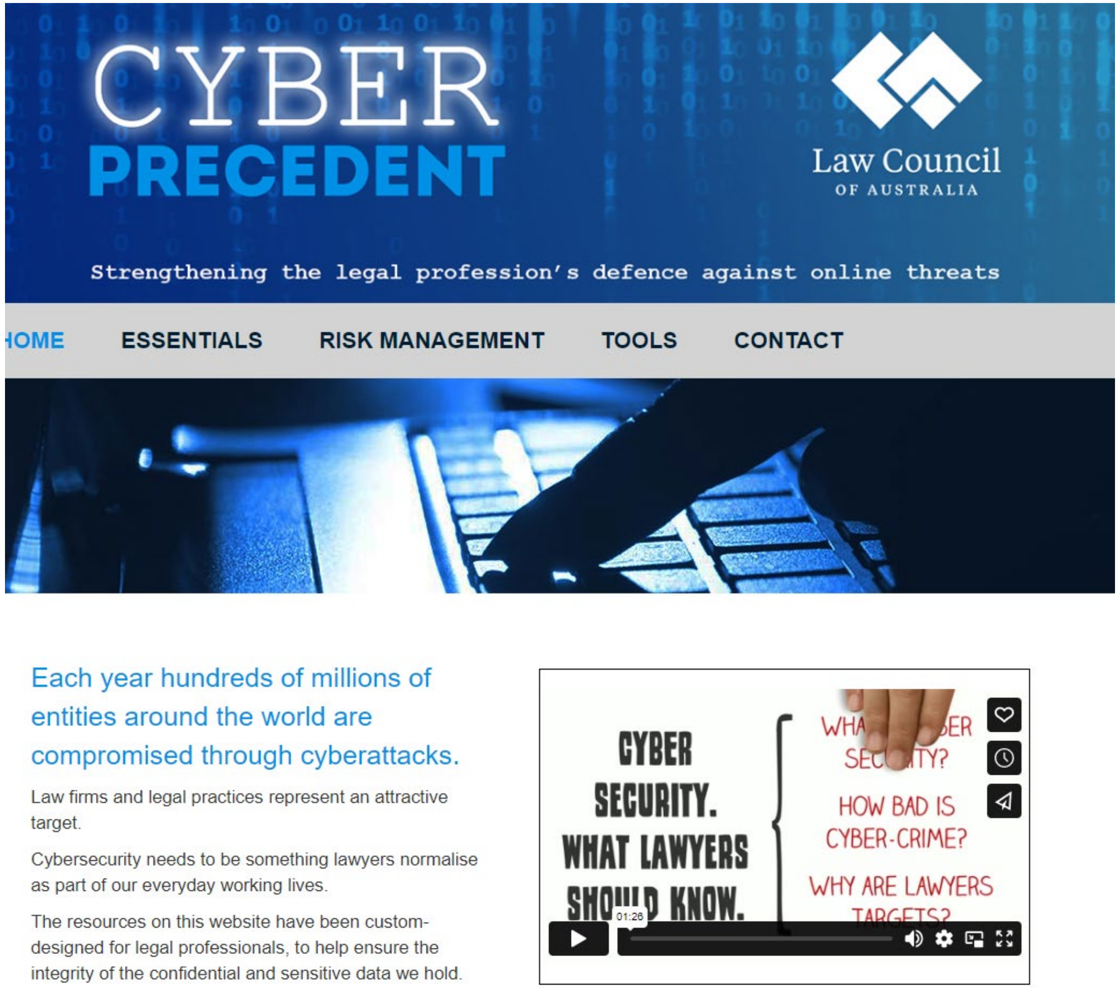
Test that everyone is clear about what they are required to do if something goes wrong.

- Hold a training session
- Develop a scenario that might happen
- Practice how the scenarios would be handled

☑

LPLC

INCIDENT RESPONSE AND REPORTING

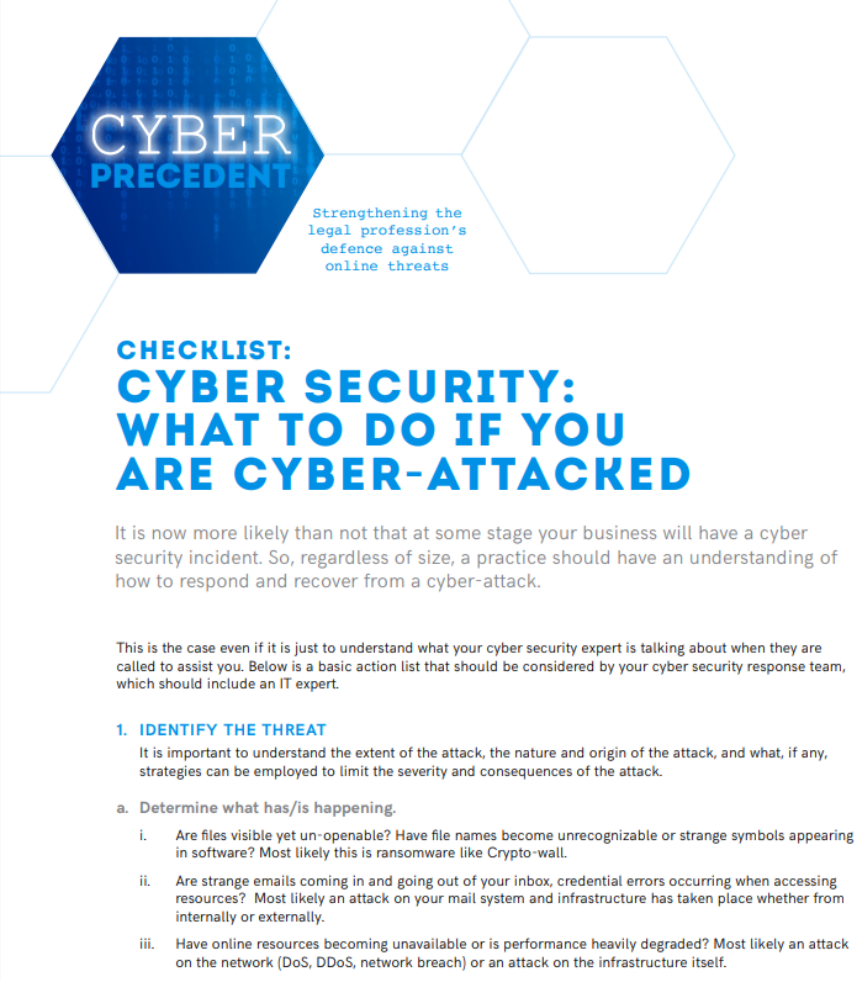


Each year hundreds of millions of entities around the world are compromised through cyberattacks.

Law firms and legal practices represent an attractive target.

Cybersecurity needs to be something lawyers normalise as part of our everyday working lives.

The resources on this website have been custom-designed for legal professionals, to help ensure the integrity of the confidential and sensitive data we hold.


CYBER
PRECEDENT
Strengthening the legal profession's defence against online threats

CHECKLIST: CYBER SECURITY: WHAT TO DO IF YOU ARE CYBER-ATTACKED

It is now more likely than not that at some stage your business will have a cyber security incident. So, regardless of size, a practice should have an understanding of how to respond and recover from a cyber-attack.

This is the case even if it is just to understand what your cyber security expert is talking about when they are called to assist you. Below is a basic action list that should be considered by your cyber security response team, which should include an IT expert.

1. IDENTIFY THE THREAT

It is important to understand the extent of the attack, the nature and origin of the attack, and what, if any, strategies can be employed to limit the severity and consequences of the attack.

a. Determine what has/is happening.

i. Are files visible yet un-openable? Have file names become unrecognizable or strange symbols appearing in software? Most likely this is ransomware like Crypto-wall.

ii. Are strange emails coming in and going out of your inbox, credential errors occurring when accessing resources? Most likely an attack on your mail system and infrastructure has taken place whether from internally or externally.

iii. Have online resources becoming unavailable or is performance heavily degraded? Most likely an attack on the network (DoS, DDoS, network breach) or an attack on the infrastructure itself.

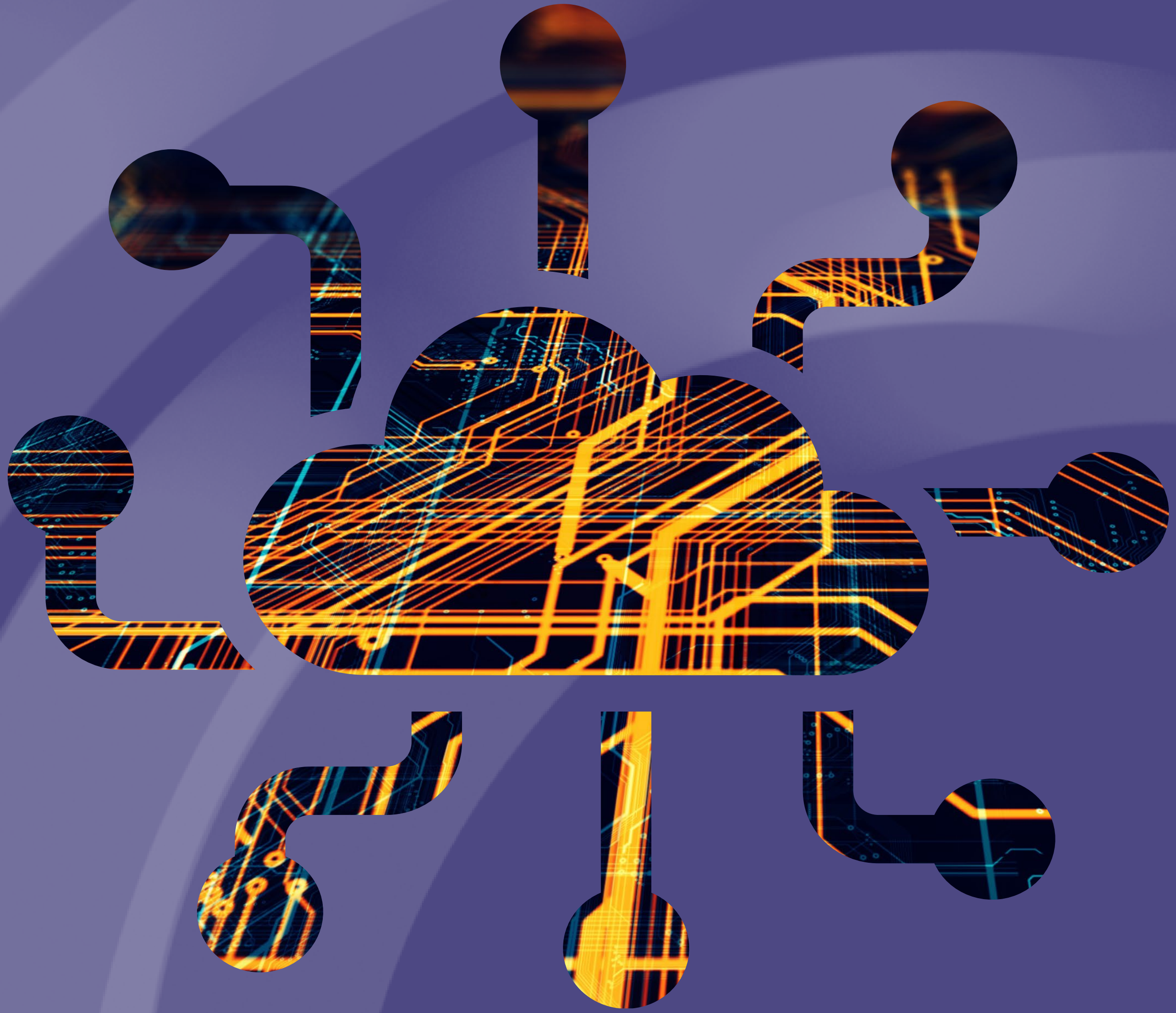
KEY MESSAGES FOR BEHAVIOURAL CONTROLS

1. Train staff and keep them updated.

2. Have a response procedure for when a cyber incident occurs.

3. Create and maintain a reporting culture.

FUTURE CHALLENGES AND EMERGING THREATS



SOPHISTICATED SOCIAL ENGINEERING

Issues:

- Attacks often bypass traditional security measures by exploiting human vulnerabilities.
- Leveraged by advanced techniques such as psychological profiling, data mining, and AI to craft convincing messages.

When: Now

Tip: Develop a culture of scepticism with the firm for cyber related issues.

MORE TARGETED SPEAR PHISHING

Issues:

- Extensive research to gather information about their targets.
- Impersonation of trusted entities or using familiar context.
- Automated tools and machine learning algorithms enable attackers to scale spear phishing campaigns while maintaining a high level of customisation and effectiveness.

When: 1-2 years

Tip: Advanced email security solutions, user training, and proactive threat intelligence.

INCREASED USE OF DEEP FAKES

Issues:

- Democratisation of deep fake tools and the availability of large datasets facilitate the creation of convincing fake content.
- Traditional methods of verifying content become less reliable.
- Automated tools and machine learning enable scale spear phishing campaigns while maintaining a high level of customization and effectiveness.

When: 1-5 years

Tip: Combination of tech solutions, policies, and media literacy to raise awareness and build resilience against manipulation and misinformation.

FURTHER POINTS TO REMEMBER

- Lawyers work in an information business. Secure your main asset.
- Have a **playbook** for when things go wrong. Practice your playbook.
- Always be on the lookout. Mistakes happen when you are busy.
- Update your both your **professional and personal** cyber security posture.
- Be careful what you share on social media.
- Don’t use unknown USB drives or external hard drives with your work computer
- Don’t use unsecure public Wi-Fi without a VPN.

LP
LC

DETERRENT EXCESS

5.5 Payment or electronic funds transfer

Payment or electronic funds transfer

Any payment or electronic funds transfer made on the basis of a purported instruction or authorisation which the Firm failed to take reasonable steps to verify.

DETERRENT EXCESS

Identify: Don’t accept email requests on face value. The email asking you to re-direct money might look genuine, but it could have been sent by a hacker.

Verify: Call the sender personally to check authenticity. Use a number you know, not one suggested in the email. Ask for the account number, write it down, then compare with the email.

Note: Make a file note that you made the call and confirmed the payment instructions, so you can prove it.

Warn: Tell the client they might also be targeted with fake emails from you and not to act on email payment directions without calling to check. Put this in your engagement letters.

Check: Involve a second person in the process and don’t action payment requests without proof that steps two and three have happened.

DETERRENT EXCESS

5.6 Absence of multi-factor authentication

Unauthorised access to an email account used by any Insured, where access to that email account after 30 June 2023 did not require at least two different factors of authentication.

NEXT ACTION STEPS

TAKE TRAINING

HIRE CONSULTANTS

READ LPLC RISK GUIDES

HELP IS AVAILABLE

- This is all very doable.

- There are a lot of resources and help available.

- Call the LPLC if you have a suspected cyber breach. Consider if you should be informing the VLSB.

Q&A TIME

Let us know in the chat if you have any questions.

GET THE LATEST LPLC NEWS AND ALERTS

Subscribe to the latest risk management updates, events, news and alerts by visiting:

lplc.com.au/subscribe

If you have a specific risk management question or need some help finding resources, you can contact us by phone on **03 9672 3800**, during business hours or via email at lawyersrisk@lplc.com.au

Thank you

LPLC
LEGAL
PRACTITIONERS'
LIABILITY
COMMITTEE

lplc.com.au