Lawcover®

GUIDE TO CYBER SECURITY

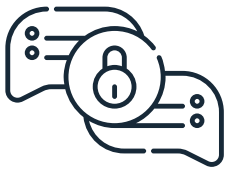
This guide is designed to help law practices navigate the world of cyber security; identify and prioritise their security needs and implement effective defence systems, ongoing protection and appropriate response plans in their own practice.

CONTENTS

INTRODUCTION

The rise in volume and sophistication of cyber-attacks in the legal sector and the accompanying threat to business operations is of a significant concern. Successful cyber-attacks occur with increasing frequency and as the legal industry adapts to a changing environment, so too do cybercriminals.

Lawcover sees the significant reputational and economic impact that a cyber incident has on law practices. The evolving cyber security landscape means that this is an area of risk that is sometimes difficult to navigate. However, there are simple measures that can be taken to help reduce risk, protect your practice and prevent a cyber related breach.



Simple measures can be taken to help reduce risk...

INTRODUCTION

GROUP CYBER RISK POLICY

Lawcover has purchased a group cyber risk insurance policy which provides foundational cover for all Lawcover insured law practices, at no cost. Whether or not your law practice already has a cyber risk policy, this insurance is available to your law practice should you choose to use it. Please see the Lawcover website for details of this insurance cover.

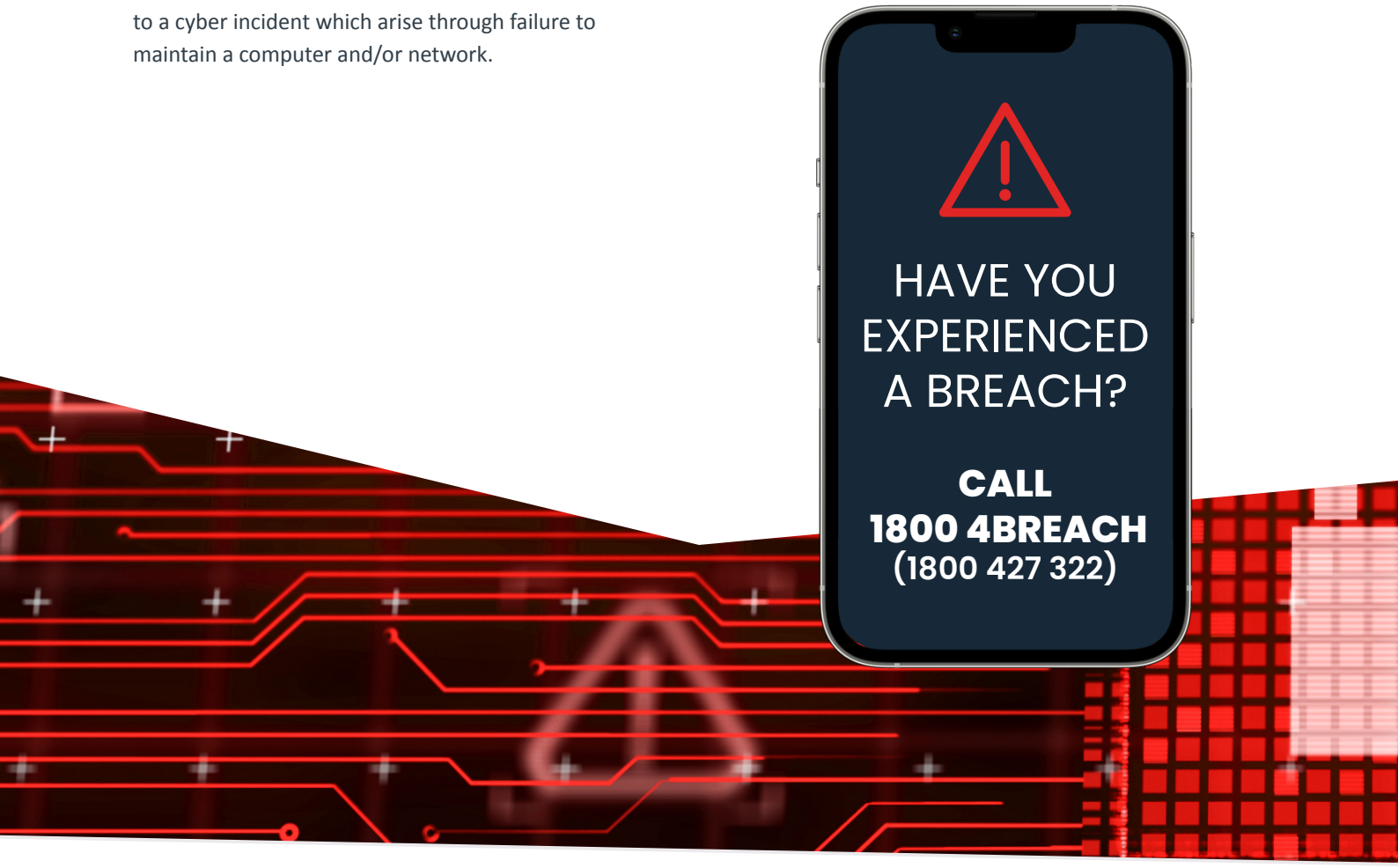
Law practices should consider whether the limit and breadth of cover under the Lawcover group cyber risk policy is appropriate for their practice.

As well as covering immediate crisis assistance, the cyber risk policy will respond to cyber events such as ransomware and other disruption attacks. However, it is important to note that the cyber risk policy will not respond to problems unrelated to a cyber incident which arise through failure to maintain a computer and/or network.

CRISIS ASSISTANCE

Solicitors' duty of care requires maintenance of client confidentiality, and law practices have an obligation to protect confidential and sensitive information and to respond quickly and appropriately where there is a risk that this information has been or may be disclosed. For this reason, crisis assistance is an important aspect of the cyber risk policy.

In the event of a cyber incident a law practice should call **1800 4BREACH (1800 427 322)** to receive immediate cyber crisis support.



ADDITIONAL MATERIAL

CYBER SECURITY SNAPSHOTS AND STEP BY STEP GUIDES

Detailed instructions to ensure critical aspects of your practice are protected.

Step by step – protect your DATA

Step by step – protect your HARDWARE

Step by step – protect your PASSWORDS

Step by step – protect your EMAIL, CHAT APPS, MESSAGING AND SOCIAL MEDIA

Step by step – protect your MOBILE DEVICE

A range of additional material has been developed to complement law practices. This has been specifically created with the law practice in mind and provides step by step instructions and tips on how to protect critical aspects of your practice.

If you know the threat, you can better defend yourself.

While cyber-attacks take many different forms, they will always have a specific outcome in mind. For this guide, we have covered the key threat types that Lawcover sees in everyday practice.

A critical component of cyber security is understanding the threat landscape and knowing where vulnerabilities lie.

THE THREATS

THREAT TYPES

MALICIOUS SOFTWARE (Malware)

What is it?

Unauthorised software created by cybercriminals used to gain access to valuable data and information.

What do they want?

Business disruption

Data

Identity

Spying and Siphoning

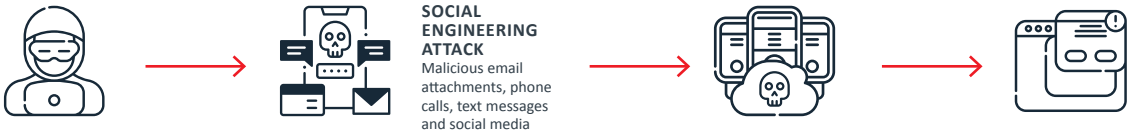
(Identifying weak links and taking resources for use in other criminal activities)

This information is then used for various activities including:

- Business email compromise and email fraud
- Unauthorised access to electronic funds
- Identity theft
- Siphoning sensitive data (e.g. client information)
- Spy and exploit system vulnerabilities.

How do they do it?

1. Attacker looks for weaknesses that can be exploited
2. Attack occurs
3. Access to systems
4. Data taken



SOCIAL ENGINEERING ATTACK
Malicious email attachments, phone calls, text messages and social media

INFRASTRUCTURE WEAKNESS ATTACK

Firewall

Website

Server

THREAT TYPES
MALICIOUS SOFTWARE (Malware)

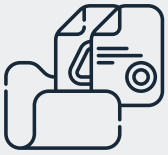
Malware provides criminals with a way to access important information such as bank or credit card numbers and passwords.

Signs your system may be infected with malware

- Your computer is running slower than usual
- Your internet browser has a new homepage or extensions that you haven't added
- You are bombarded with ads
- Your contacts receive spam from your email account
- You see a ransom/fine or warning note when trying to access files.

QUICK TIPS

ESTABLISH WI-FI ROUTER SECURITY



APPLY FILE CONTROLS THAT ONLY ALLOW AUTHORISED ACCESS

PERFORM REGULAR MALWARE SCANS

ONLY INSTALL VERIFIED AND TRUSTED SOFTWARE AND APPS ON YOUR DEVICE

ENSURE MANAGED DETECTION AND RESPONSE TOOLS ARE DEPLOYED TO ENDPOINTS

HAVE AN INCIDENT RESPONSE PLAN AND TEST IT REGULARLY

THREAT TYPES

PHISHING (Scam messages)

Phishing scams often create a sense of urgency, request payment or personal information, arrive unexpectedly and may contain links and attachments.

What is it?

Emails, messages or phone calls that mislead recipients or impersonate entities with the intent to steal money and information.

Malicious links – Take you to imposter websites that steal your information and infect your device with malware.

Malicious attachments – Compromise and takeover your computer.

Requests for sensitive data – Prompt you to fill in user IDs, passwords, financial information, etc.

What do they want?

Passwords | Financial information | Identity | Money

This information is then used for various activities including:

- Email fraud
- Unauthorised access to electronic funds and bank accounts
- Payment of fraudulent invoices
- Access to online accounts (e.g. Gmail, Dropbox, social media)
- Identity theft
- Access to sensitive data for use in other criminal activities.

How do they do it?

1. Attacker sends an email to the victim
2. Victim clicks on the email and goes to the phishing website
3. Attacker collects victim's credentials/ sensitive information (e.g online banking details)
4. Attacker uses victim's credentials/information to access bank accounts, user accounts, other online accounts (for example)

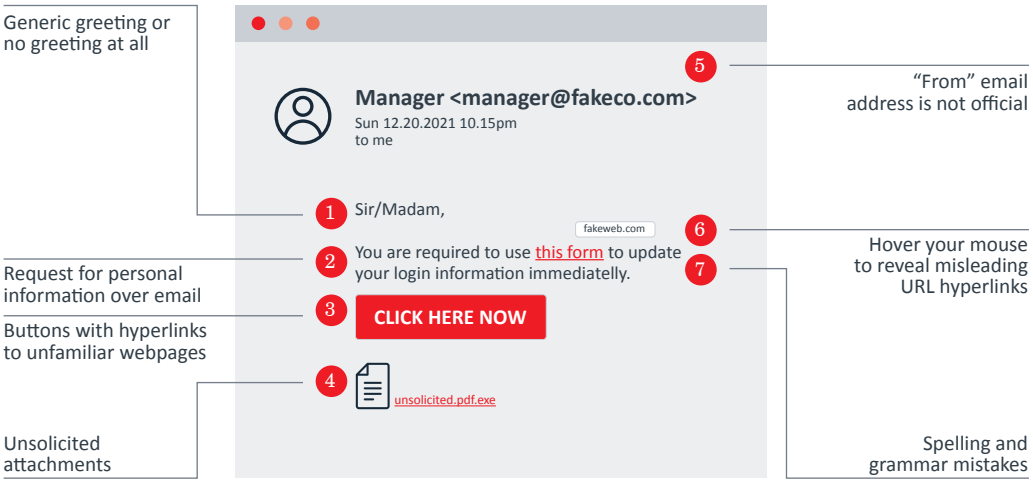
ATTACKER | LEGITIMATE WEBSITE

THREAT TYPES
PHISHING
(Scam messages)

What does it look like?

- Your computer is running slower than usual
- Your internet browser has a new homepage or extensions that you haven't added
- You are bombarded with ads
- Your contacts receive spam from your email account
- You see a ransom/fine or warning note when trying to access files.

Signs of a phishing email



QUICK TIPS

INSTALL FILTERS ON YOUR EMAIL TO PREVENT SPAM

PHONE TO CHECK EMAILED BANK ACCOUNT DETAILS

EDUCATE AND TRAIN STAFF TO RECOGNISE SUSPICIOUS EMAILS

IF UNSURE, DELETE THE EMAIL. DON'T OPEN IT

REPORT PHISHING EMAILS - A 3RD PARTY OPTION WOULD ALERT AND DELETE FROM THE USERS INBOX

HAVE AN INCIDENT RESPONSE PLAN AND TEST IT REGULARLY

THREAT TYPES

RANSOMWARE

What is it?

Ransomware is a type of malware designed to encrypt files on your device, rendering files and systems unusable. Cybercriminals then demand a ransom to fix the problem.

What do they want?

Money

A low-risk, high-reward income stream for cybercriminals, ransomware is easy to develop and distribute.

Ransoms are typically paid using an online digital currency or cryptocurrency such as Bitcoin, which is very difficult to trace.

Paying a ransom does not guarantee your files will be restored, nor does it prevent the publication of any stolen data or its on-sale for use in other crimes.

If you experience a ransomware incident contact Lawcover on 1800 4BREACH immediately.

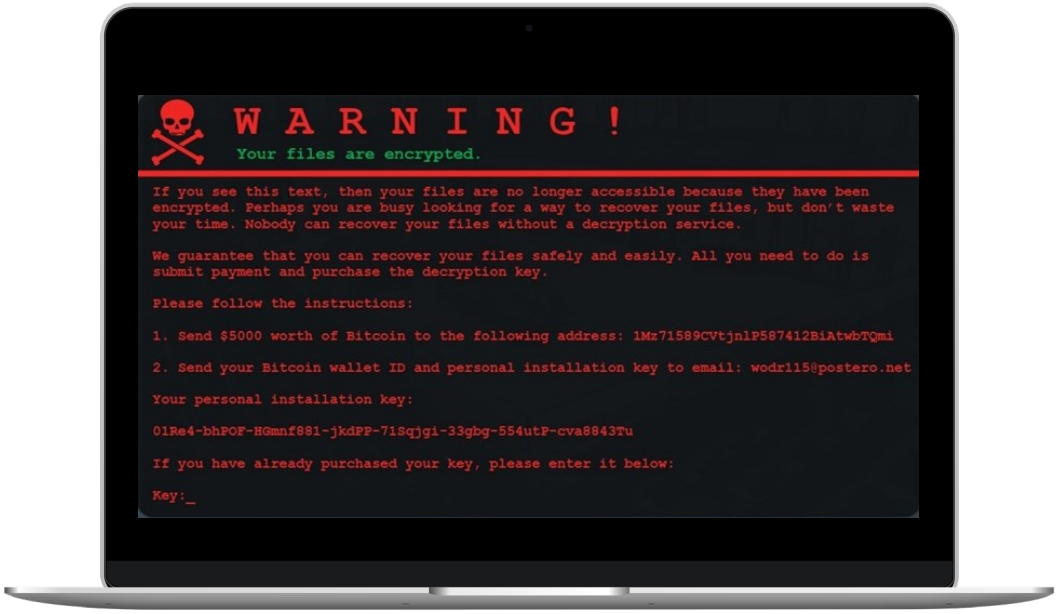
How do they do it?

1. Victim receives email containing Malware, or has a vulnerability in their asset allowing attackers to gain a foothold in the network
2. Malware downloads malicious files (codes)
3. Malicious codes encrypt victim's files
4. Ransom notice with deadline and instructions for payment sent
5. Demand ransom payment to unlock/decrypt files

THREAT TYPES
RANSOMWARE

What does it look like?

You may see a ransom or warning note similar to the one below when trying to access your system, files or device. Files may be inaccessible and have odd file extension names, for example: “file.wannacry” rather than “file.pdf”.



QUICK TIPS

BACK UP YOUR FILES REGULARLY

INSTALL FIREWALLS AND ENABLE AUTOMATIC UPDATES

PRACTICE SAFE BROWSING HABITS

DON’T CLICK THE EMAIL LINK

HAVE AN INCIDENT RESPONSE PLAN AND TEST IT REGULARLY

THREAT TYPES

BUSINESS EMAIL COMPROMISE (BEC)

> Every BEC attack can look different.

What is it?

Emails that are sent fraudulently by cybercriminals impersonating a real business, organisation, employee, client or contact. Emails typically request personal details, a change in bank account details, or urgent invoice payments.

What do they want?

Money

Sensitive Information

How do they do it?

1. Cybercriminals collect information to create a profile of key targets. (e.g. Does the target conduct regular financial transactions?)
2. Using a fake or hacked email address, an email impersonating an individual or entity is sent to the target. Emails may request a change in details (e.g. bank account details) or urgent payment of an invoice
3. The victim is convinced they are conducting a legitimate transaction and transfers funds (for example) to the requested bank account or pays the urgent invoice
4. Funds are transferred unknowingly to the cybercriminal

IDENTIFY TARGET

SOCIAL ENGINEERING

INFORMATION EXCHANGE

TRANSFER

THREAT TYPES
BUSINESS EMAIL COMPROMISE (BEC)

What does it look like?

Depending on the target and what outcome is sought, every BEC attack can look different. However, there are some red flags to look out for:

- Requests for personal information. These may be bank account details, identity documents, contact details etc
- Atypical payment requests
- Use of urgent language. Usually demanding immediate payment of an invoice or bill
- Advance fee request without having any product or service delivered first
- Spelling mistakes or odd grammar
- Sudden changes to details or instructions (e.g. a change to bank account details).

QUICK TIPS

PHONE AND VERIFY BANK DETAILS BEFORE TRANSFERRING FUNDS

BLOCK AND REPORT UNWANTED CONTACTS OR SPAM

TRAIN STAFF TO RECOGNISE IMPERSONATION TACTICS

ESTABLISH CLEAR PROCEDURES FOR ELECTRONIC FUNDS TRANSFERS

BE WARY OF LAST MINUTE CHANGES (E.G. CONTACT DETAILS OR BANK ACCOUNT DETAILS)

THREAT TYPES

INSIDER THREATS

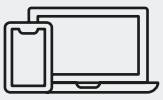
Accidental insider threats are a major cybersecurity risk for law practices. Unlike malicious actors who intentionally cause harm, accidental insiders are employees or users who unknowingly compromise security. Although their actions are unintentional, the impact can be severe.

Common examples include clicking on malicious links, misconfiguring systems, or inadvertently sharing sensitive information. A lack of awareness around cyber security best practices often leads to careless behaviour, such as neglecting to follow protocols or failing to update software. Additionally, sensitive data may be mistakenly shared with unauthorised individuals via email, cloud platforms, or even AI tools, putting client confidentiality and law practice reputation at risk.

How can a law practice protect against insider threats?

Comprehensive Training:

Regular cybersecurity training programs can educate employees about best practices, such as recognising phishing attempts, strong password hygiene, and secure data handling



Awareness Campaigns:

Continuous campaigns can reinforce security awareness and promote a culture of security

Access Controls:

Implementing robust access controls, such as role-based access and multi-factor authentication, can limit unauthorised access

Data Loss Prevention (DLP) Solutions:

DLP tools can monitor and control data movement, preventing accidental data leaks

THREAT TYPES

INSIDER THREATS

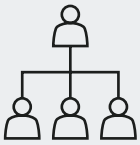
How can a law practice protect against insider threats?

Regular Security Audits:

Conducting regular security audits can identify and address potential vulnerabilities

Incident Response Plan:

A well-defined incident response plan can help mitigate the impact of security breaches, including those caused by accidental insider threats



Employee Onboarding and Offboarding:

Clear procedures should be in place for onboarding and offboarding employees to ensure proper access privileges and data handling

VULNERABILITIES

CYBER RISK AREAS

Hardware, Computers and IT systems

A law practice's computers, servers, storage, mobile devices and network are all vulnerable to cyber-attack. Issues and attacks can occur when the network has not been properly secured and the security settings on the device are not configured correctly.

Staff and contractors

Without proper training staff can be a significant vulnerability. Cybercriminals will exploit staff who do not think before clicking on weblinks, email attachments and even social media videos. Passwords in the workplace may be weak, re-used and shared as staff prioritise convenience over security. Insider threat from staff is also an issue if policies and procedures are not effective. However, if trained correctly staff can become your strongest ally against cyber-attacks.

Personal mobile phones and devices

Personal devices such as smart phones, tablets and laptops are increasingly used for work purposes, especially for the mobile workforce. These are easier to attack than corporate IT equipment, which often has more restrictions and protections. Personal mobile phones may be allowed to connect to the office Wi-Fi, which can provide cybercriminals with access to critical data and information.

There are many aspects of a law practice that are vulnerable to cyber-attack. However, there are a number of key areas that are consistently targeted and that should be factored into any cyber protection. This list is not exhaustive, and you should consider your own practice circumstances when assessing cyber security.

CYBER RISK AREAS

Cloud portals and platforms

It is increasingly common for a law practice to use cloud portals/services and platforms provided by third-party software suppliers for document management (e.g. a document management system) and practice management. This can become a vulnerability if supplier due diligence is not thorough and security updates are not applied and maintained.

Remote and home working

Staff working remotely, when travelling or at home, are more inclined to make compromises on security by using personal email accounts, unsecure connections, personal social media accounts and browsing unrestricted websites.

Data transfer and storage

Transferring data as an email attachment creates an exposure risk and relaxed access management rules mean that personal data is easily found on networks. Practices may unconsciously allow staff to use cloud services to transfer information. Dropbox, Gmail, and Hotmail, for example, are cloud services that staff may use to transfer information.

Finance

Any area that handles money, financial transactions, bank details, invoices or payments is a target for cybercriminals. Law practices are particularly vulnerable in this area due to the large financial transactions that are processed as a part of everyday practice.

Refer to Lawcover's step by step guides for more information on how to reduce vulnerabilities and improve security of your systems.

ONGOING PROTECTION

DEVELOPING A CYBER SECURITY STRATEGY

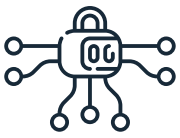
Generally, a cyber security strategy will allow a law practice to:

- Understand workloads and specific risks
- Identify vulnerabilities
- Put appropriate protection measures in place
- Monitor threats
- Enable early detection
- Respond swiftly
- Prevent future attacks.

Where to start?

Every law practice is different and each practice should consider its own circumstances when formulating a cyber security strategy. However, the following framework may provide a good starting point.

A cyber security strategy is a proactive plan of action designed to maximise the security and resiliency of your practice. It provides structure and clarity to help ensure the practice is protected and equipped to handle whatever new types of threats come along.



While you can never eliminate threats entirely, a cyber security strategy is a big part of reducing your risk.

DEVELOPING A CYBER SECURITY STRATEGY

ACTION	STEPS TO BE TAKEN
Risk based assessment	Undertake a thorough risk-based assessment of your practice information security requirements. Take steps to make information/ cyber security part of your normal business risk management procedures. Train and educate staff in cyber security principles to ensure they become part of your practice culture.
Asset audit	Your practice is only secure if every asset is protected. You need to know what you are protecting if protection measures are to be effective. Carry out an audit of any assets that are potentially at risk – identify financial, personal and other information assets that are critical, and the IT services you rely on.
Vulnerability assessment	Undertake an assessment of your cyber security resilience and identify where you may have vulnerabilities and take appropriate remedial action. Assess all the IT equipment within your practice, including mobile and personal IT devices. Understand the technical and organisational risks to these and how these risks are currently managed.
Expert advice	Decide whether you need to seek expert advice and assistance to undertake the risk and vulnerability assessments, and to get the right protection and security controls in place. Regardless of whether your IT is outsourced or inhouse, sometimes it can be useful to get external expertise.
Risk framework and governance	Put in place technical and practice measures to satisfy the security obligations relating to personal data and to control the risk of cybercrime. Monitor their effectiveness on an ongoing basis.
Accountability	Appoint a senior member of staff to oversee data and cyber security. Ensure they have the right resources and support to do this job.

DEVELOPING A CYBER SECURITY STRATEGY

ACTION	STEPS TO BE TAKEN
Cyber security policies	Prepare and issue clear policies and procedures on all key aspects of data and cyber security. All staff should be made aware of their security obligations and the policies that apply to them. As a starting point consider including: **Device Security** To ensure the security of your law practice's mobile devices, such as laptops, tablets, mobile devices and smartphones, implement robust security measures. Prioritise strong password policies and regular software updates to protect against vulnerabilities, encrypt sensitive data to safeguard it from unauthorised access, enable remote wiping capabilities to protect data in case of device loss or theft, maintain a detailed inventory of all practice-owned devices and enable tracking in case of lost or stolen devices. **Data Security** Categorise data based on sensitivity to determine appropriate security measures, establish guidelines for handling and sharing sensitive client information, implement regular backups and a robust disaster recovery plan. If using cloud storage, ensure its secure and compliant with Australian privacy laws. Regularly educate employees on security best practices, including phishing and social engineering threats and encourage employees to report suspicious activities promptly. **Network Security** Use strong authentication methods like multi-factor authentication to protect network access. Employ strong encryption protocols (like WPA3) for Wi-Fi networks, mandate the use of VPNs for remote access to the practice network, discourage the use of public Wi-Fi. **Incident response** Develop a comprehensive plan for responding to security incidents. Establish procedures for reporting, investigating, and containing security breaches and implement processes for collecting and analysing digital evidence. **Compliance** Adhere to Australian privacy laws, such as the Privacy Act 1988, to protect client data and comply with relevant cyber security regulations and standards.

DEVELOPING A CYBER SECURITY STRATEGY

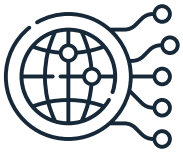
ACTION	STEPS TO BE TAKEN
Monitoring and review	Review your systems and procedures regularly and respond to any changes or problems you identify, including attacks or disruption to your practice. Ongoing monitoring – test, monitor and improve your security controls regularly to manage any change in the level of risk to your IT equipment, services and information. Disposing of programs or physical devices – remove any software or equipment that you no longer need, ensuring that it contains no sensitive information. Managing user access – review and manage any change in user access, such as the creation of accounts when staff members join the practice and deactivation of accounts when they leave.
Cyber incident management	Having a Cyber Incident Response Plan in place is essential, if your practice is disrupted or attacked. This plan will help guide your response, ensuring that adequate measures are taken to contain the threat, and a quick recovery is possible in the event protection controls don't prevent an incident occurring.
Record keeping	Keep records. This should include details and evidence of: your risk-based assessments; the technical and organisational measures taken to protect the security of personal and client data; your processes for testing, assessing and evaluating the effectiveness of those measures, and cyber-incident management.

RESPONDING TO A CYBER INCIDENT

CYBER INCIDENT RESPONSE PLAN

In addition to an overall cyber security strategy, a law practice should have a cyber incident response plan in place. This plan will guide you through a cyber incident and help to ensure an effective response and quick recovery in the event protection controls don't prevent an incident occurring.

The cyber incident response plan should align with your practice's emergency, crisis and business continuity arrangements as well as other relevant arrangements. It should support staff to fulfil their roles by outlining their responsibilities and all legal and regulatory obligations in responding to a cyber incident.



Managing responses to cyber incidents is the responsibility of every law practice.

CYBER INCIDENT RESPONSE PLAN

Broadly, a Cyber Incident Response Plan should detail your response mechanisms, so that you are ready to respond.

This may include the following steps:

Identification	Verify whether an event is a security incident. A rapid triage is needed to understand what has happened and to filter out false positives. Details should include what actions need to be taken in the first, third and 24 hours after a breach.
Containment	Isolate affected systems to prevent further damage (it is important to note that the computer or device displaying the symptom (for example) may only be part of the problem). This is a critical step which should be done by someone with adequate cyber security experience.
Elimination	Find the source or root cause of the incident and ensure it is removed from affected systems. Be satisfied that the attack has ended, and that any malicious software and connections have been removed. This should be done by someone with adequate cyber security experience to ensure that: - The criminals are not still in your system and accessing your data. - You do not lose the footprint showing where the criminals have been and what data they have taken.
Categorisation and reporting	Determine exactly what data or assets have been accessed or stolen. All cyber incidents or breaches should be documented. Review whether the matter should be reported to any of the following: Office of the Information Commissioner (OAIC), Lawcover, The Law Society of NSW (or relevant State or Territory Law Society), your bank, the police, ReportCyber (cyber.gov.au/report), clients, employees, contractors, and anyone else who may be affected. Revisit this as further information emerges.
Recovery	Resuming normal operations of affected systems after ensuring no threat remains. Revisit this as further information emerges.
Lessons learned	A post incident review will allow you to learn from the incident and improve future protections, monitoring and response efforts.

Note: Any plan should be tested and reviewed regularly.

CYBER INCIDENT RESPONSE PLAN

Preparation

An effective response plan requires preparation. The greater the preparation the easier it will be to cope with any cyber breach when it occurs. The development of a cyber security strategy (see page 18) will inform your cyber incident response plan and both documents should work together to ensure thorough coverage.

Audit your systems and data

You need to have an understanding of all your systems that could be affected by an attack and where your data is stored.

- Identify the critical services, data locations and third parties you rely on
- Assess your vulnerabilities as regards your policies, technology, and staff
- Review backup and recovery procedures.

Create a response team

A response team will help steer your practice through any cyber-attack. The team should be proportionate to the size and complexity of your practice. It may include external contractors if you outsource your IT and cyber security. This team will be responsible for coordinating damage limitation, incident investigation and key communications if a cyber security incident occurs.

- Identify team members and roles and responsibilities, including authority levels for specific actions such as notifying of a breach or instructing technical response experts or external parties
- Establish response guidelines by considering and discussing possible scenarios with staff
- Establish an emergency contact procedure. There should be one contact list with names listed by contact priority
- How do you define risk? You should consider and define a protocol that helps identify whether a threat is low risk, medium risk or high risk.

Communications

Identify stakeholders and when they should be informed – staff, clients, third party suppliers, police etc. Notify Lawcover as soon as possible – call **1800 4BREACH (1800 427 322)** to receive immediate cyber crisis support.

Training and Testing

Staff – All staff need to know how to recognise a cyber breach, what their immediate response is and who they should contact. Ideally you can set out a description process to easily describe a cyber incident in a way that everyone will understand. Staff should also be familiar with your response team's plan.

Response team - The response team need to know that processes work, which means that these should be tested frequently. This helps to identify any gaps which can then be remedied in advance of the real thing. For example, the location of the incident response plan. Most will store the plan on a main server for all to access. However, in the event of a cyber incident, the main server may not be accessible which means the plan is not accessible. Think about these types of scenarios and have backups.

Backup and recovery

Effective backups are an important ingredient of incident response.

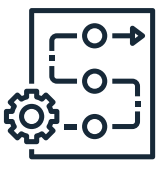
CYBER INCIDENT RESPONSE PLAN

Ongoing staff training and awareness

To safeguard your practice data and defend against cyber threats, it's crucial to educate your staff on safe practices Promoting a culture of awareness and encouraging the reporting of suspicious activity will help to secure the practice and identify threats before they develop further.

Key areas for education and ongoing awareness include:

- **Strong password/passphrases:** Encourage the use of strong, unique passphrases for each user and account
- **Password managers:** Use a reliable password manager to securely store complex passwords
- **Regular password changes:** Implement a policy that ensures passwords are changed regularly
- **Recognise Phishing Attempts:** Train staff to identify common phishing tactics, such as suspicious emails, urgent requests, and unexpected attachments
- **Verify Sender Identity:** Train staff to verify email addresses before sending. When receiving emails exercise caution if the sender is unfamiliar
- **Avoid clicking on suspicious links:** Emphasise the importance of not clicking on links or downloading attachments from unknown sources
- **Email etiquette:** Advise staff to avoid sharing sensitive information via email, especially when using unencrypted email
- **Email encryption:** Consider using email encryption tools to protect confidential communications
- **Email security settings:** Configure email clients with strong security settings, such as spam filters and malware scanners
- **Client data protection:** Train staff on the importance of protecting client confidentiality and complying with data privacy regulations
- **Secure data storage:** Ensure that sensitive data is stored securely on encrypted devices and cloud storage solutions
- **Data sharing best practices:** Establish policies for the sharing of data with third parties, including secure file transfer methods
- **Professional online presence:** Encourage staff to maintain a professional presence online including website communications, social media and chat apps (e.g. WhatsApp)
- **Privacy settings:** Advise staff to review and adjust their privacy settings on social media platforms
- **Avoid sharing sensitive information:** Implement policies regarding the posting of content on social media platforms and websites. This should include not sharing any sensitive information
- **Scheduled training and education sessions:** Conduct regular training and education sessions to keep staff updated on the latest cyber threats and best practices
- **Simulated phishing attacks:** Conduct simulated phishing attacks to test employees' awareness and response. Use the results to inform further education and awareness.



Define a protocol that helps identify whether a threat is low, medium or high risk.

QUESTIONS TO ASK YOUR IT PROVIDER

There are some important questions a law practice should ask of their IT provider regarding cybersecurity. The below is not a comprehensive list and should be refined depending on your specific requirements, but it should provide a solid overview of how your IT Service provider is protecting your data.

By asking these questions, you can gain a better understanding of your IT provider's cybersecurity capabilities and ensure that your practice is adequately protected from cyber threats.

? **Security certifications:**

Does your company hold any relevant security certifications (e.g., ISO 27001, SOC 2)?

? **Incident Response Plan:**

What is your incident response plan in case of a cyberattack? How often is it tested and updated?

? **Staff education and training:**

How do you train your staff on cyber security best practices? Are there regular training and education sessions they can attend? Can they facilitate a schedule of phishing simulations/testing?

? **Third-party risk management:**

How do you assess and manage the security risks posed by third-party vendors and suppliers?

? **Data backup and recovery:**

What is your backup and recovery strategy? How often are backups performed, and how are they stored and protected?

? **Business continuity plan:**

Do you have a business continuity plan in place to minimise disruption in the event of a cyberattack?

? **Network security:**

What measures do you have in place to protect your network from unauthorised access and cyberattacks (e.g., Firewalls, Intrusion Detection Systems, Intrusion Prevention Systems)?

? **Endpoint security:**

How do you protect your endpoints (computers, laptops, mobile devices) from malware and other threats?

QUESTIONS TO ASK YOUR IT PROVIDER

Email security:

What measures do you have in place to protect against email threats like phishing and spam?

Logging:

Do you have a SIEM or SOAR for detecting and alerting any anomalous issues?

Data encryption:

Do you encrypt sensitive data both at rest and in transit?

Access controls:

How do you manage user access to systems and data? Are there strong password policies and multi-factor authentication in place?

Vulnerability management:

How do you identify and address vulnerabilities in your systems and software?

Penetration testing:

Do you conduct regular penetration testing to identify weaknesses in your security defences and how do you respond to findings?

Data privacy compliance:

How do you comply with relevant data privacy regulations (e.g., Privacy Act, Health Records Act, Consumer Law etc)?

Incident reporting:

What is your policy for reporting data breaches and security incidents to relevant authorities?

Insurance coverage:

Do you have adequate cyber insurance coverage to protect against financial losses in case of a cyberattack?

Proactive monitoring:

How do you proactively monitor your network and systems for signs of malicious activity?

QUESTIONS TO ASK YOUR IT PROVIDER

Threat intelligence:

How do you stay informed about the latest cyber threats and vulnerabilities?

Communication and transparency:

How will you communicate with us in case of a security breach?

Experience and expertise:

What is your experience in providing cyber security services to law practices?

GLOSSARY

Authentication: Verifying a user's identity.

Authorisation: Granting permissions to access specific resources.

Cloud Security: Protecting data and applications in the cloud.

Code Review: The process of examining code for errors and security vulnerabilities.

Cyber Insurance: Insurance coverage for cyberattacks and data breaches.

Cyber Threat: A potential danger to a computer system or network.

Cyberattack: A malicious act targeting computer systems or networks.

Cybercrime: Criminal activity that involves computer networks or devices.

Cybersecurity: The practice of protecting computer systems and networks from digital attacks.

Data Breach: The unauthorised access to or disclosure of sensitive information.

Data Privacy: The protection of personal information.

Data Protection Regulations: Laws and regulations governing the collection, storage, and processing of personal data.

Denial of Service (DoS) Attack: An attack that overwhelms a system or network with traffic, making it inaccessible.

Digital Forensics: The process of collecting and analysing digital evidence.

Distributed Denial of Service (DDoS) Attack: A DoS attack launched from multiple sources.

Encryption: Converting data into a code to prevent unauthorised access.

Endpoint Security: Protecting devices like computers and mobile phones.

Exploit: A technique used to take advantage of a vulnerability.

Firewall: A security system that monitors and controls network traffic.

GDPR (General Data Protection Regulation): A European Union law on data protection and privacy.

Incident Response Plan: A plan outlining the steps to be taken in response to a security incident.

Intrusion Detection System (IDS): A system that monitors network traffic for signs of intrusion.

Intrusion Prevention System (IPS): A system that actively blocks intrusion attempts.

Malware: Malicious software designed to harm computer systems.

Network Security Appliance: A hardware device that provides network security functions.

Patch Management: Applying software updates to fix vulnerabilities.

Phishing: A cyberattack where attackers attempt to deceive victims into revealing sensitive information.

Ransomware: Malware that encrypts a victim's files and demands a ransom for decryption.

Secure Coding Practices: Coding techniques that help prevent vulnerabilities.

Social Engineering: The psychological manipulation of people to gain access to sensitive information or systems.

Two-Factor Authentication (2FA): Requiring two forms of identification.

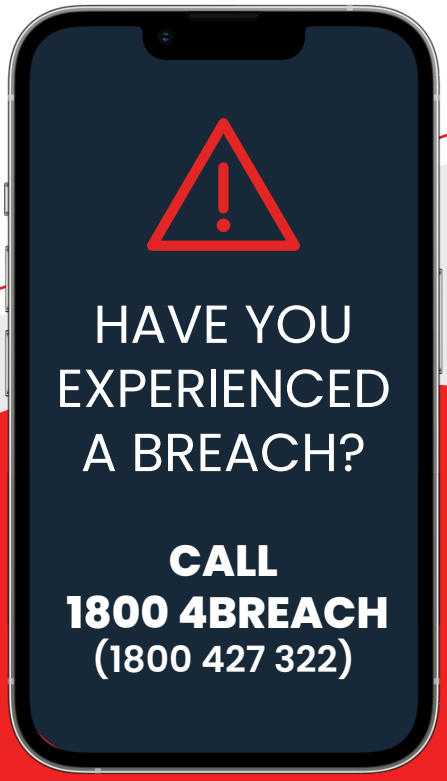
Virus: A type of malware that replicates itself and spreads to other computers.

Vulnerability: A weakness in a computer system or network that can be exploited.

Web Application Firewall (WAF): A security system that filters and monitors HTTP traffic.

Worm: A self-propagating malware that can spread across networks.

Zero-Trust Security: A security model that assumes no one is trustworthy.



Lawcover®

Lawcover Insurance Pty Ltd | ABN 15 095 082 509
Phone (02) 9286 8877 | practicesupportservices@lawcover.com.au | lawcover.com.au