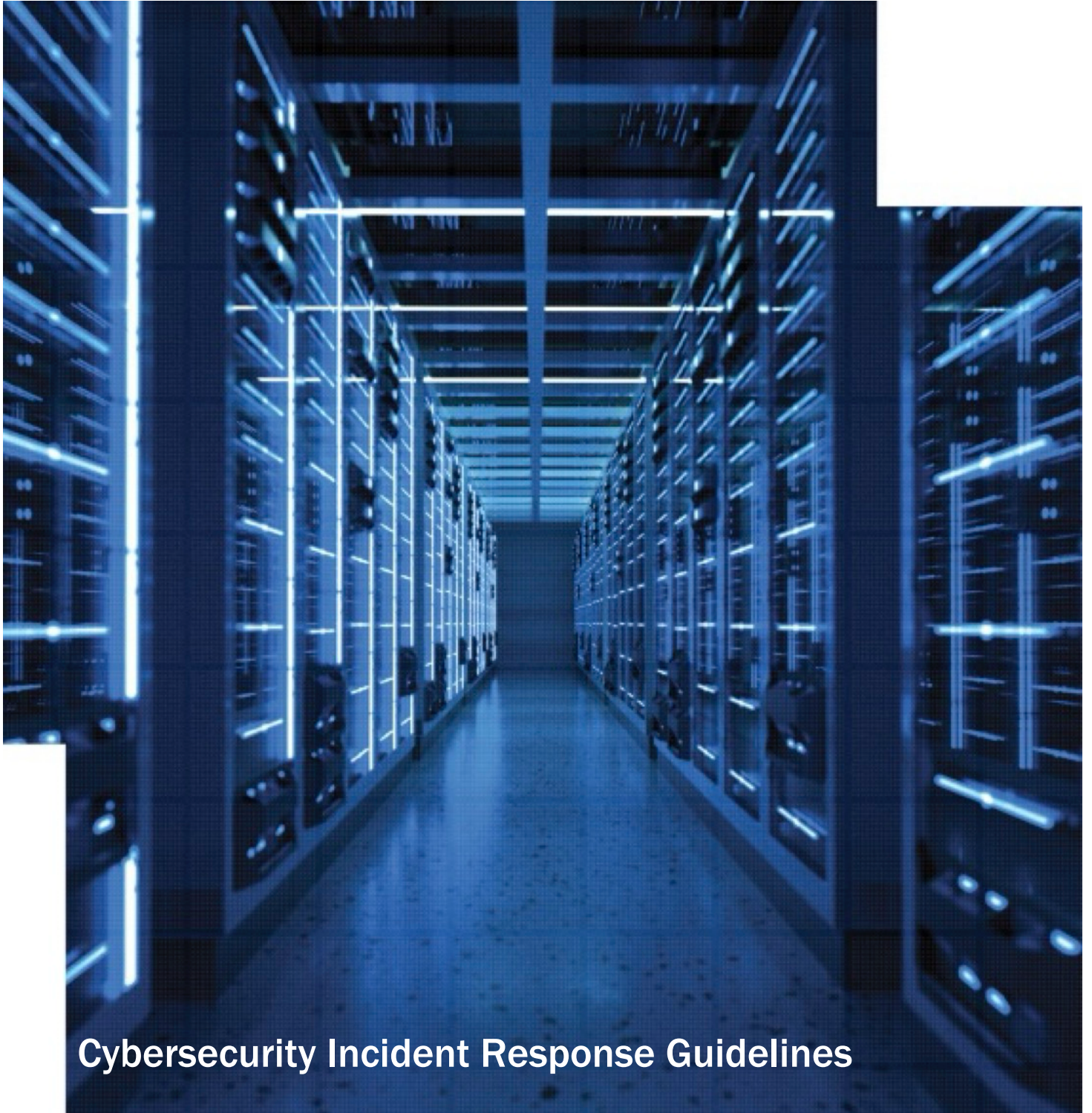




Australian
Bar Association



Cybersecurity Incident Response Guidelines

Australian Bar Association

October 2025

Preparation for Cybersecurity Incidents

1. Fill out key contact information below in advance. Print this information and keep it handy. *Remember: you may not have access to your computer or the information stored on it if a cybersecurity incident occurs.*
2. Confirm with your Clerk, IT support and/or your cyber insurer who will be your first point of contact if an incident is suspected or confirmed, and fill in their contact information below. It may be someone nominated by your Cyber Insurer, or your Clerk, the IT Support or a contracted specialist. Also confirm whether the first point of contact, or another person or firm, will become the 'Lead Responder' who takes responsibility for dealing with the incident.
3. Ensure basic cybersecurity controls are in place (if needed, check with your Clerk or your IT provider):
 - a. Software updates are configured to be applied automatically.
 - b. Multi-factor authentication is enabled for online services such as email and banking, and file storage such as Dropbox.
 - c. Passwords are strong and not reused across different online applications or services.
 - d. Critical data is being backed up, and data that is no longer needed is either securely deleted or archived.
 - e. Anti-virus software is installed and up to date.
4. Review and be familiar with the actions and guidance in this document.
5. Review your State/Territory Bar Association's cybersecurity guidelines (if available).
6. Review and be familiar with your cyber insurance policy.
7. Know whether you are an 'APP entity' with respect to the *Privacy Act 1988* (Cth) and therefore obligated to notify the Office of the Australian Information Commissioner of an 'eligible data breach'.¹
8. Consider undertaking basic cybersecurity awareness with resources such as the Cyber Warden's Foundations Webinar,² the Australian Cyber Security Centre's 'Learn the Basics',³ and the Australian Signals Directorate's 'Essential Eight' strategies.⁴

Note: While these guidelines have attempted to identify relevant legislative requirements, this document has not been formally vetted for compliance with Commonwealth, State, and Territory laws. Practitioners should check whether any laws applicable in their jurisdiction require any additional or different steps to those set out herein.

Key Contact Information

Contact / Role	Name	Telephone	Email
First point of contact for reporting an incident			
Chambers Clerk			
IT support desk			

¹ <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts>

² <https://cyberwardens.com.au/courses/#foundations> (38 minutes). Cyber Wardens is a government funded initiative designed to help small businesses enhance their cybersecurity.

³ <https://www.cyber.gov.au/learn-basics>

⁴ <https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight>



Contact / Role	Name	Telephone	Email
Cyber insurer			
Bank(s) / Financial institution(s)			

Other relevant contacts

(Include anyone to whom you have notification obligations under written confidentiality agreements, eg if loss of or access to data is suspected or occurs. Ideally, keep copies of those agreements together, in a place you can easily locate.)

Other relevant contact information

Contact / Role	Name	Telephone	
Australian Cyber Security Centre	ACSC	1300 292 371	https://cyber.gov.au/report
Reporting a data breach	OAIC		https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach
IDcare (for small business)		1800 595 170	https://www.idcare.org/





Cybersecurity incident response action plan

If you suspect or detect a cybersecurity Incident

Step	Action	Guidance	Guidance notes
1	Initial containment	<p>Disable network access by either disconnecting the network cable from the computer or disconnect from the wireless network.</p> <p>GO TO STEP 2</p>	<ul style="list-style-type: none"> Shutting the system down may result in a loss of evidence. It is not advisable to shut down the computer at this stage. Call your IT support provider for instructions if needed.
2	Record incident context	<p>Record key details such as:</p> <ul style="list-style-type: none"> Date and time. Nature of the incident (i.e. what unusual or suspicious activity you are observing). Nature of any data considered at risk or compromised. <p>GO TO STEP 3</p>	<ul style="list-style-type: none"> It is recommended to write this information down rather than entering it into a file on the computer. (You may lose access to your computer and the files on it.) Keep the information to the salient points and act with urgency.
3	Report the incident (internally)	<p>Report the suspected or actual incident to the first point of contact using the pre-filled information from the table above.</p> <p>GO TO STEP 4</p>	<ul style="list-style-type: none"> Follow technical advice from your first point of contact (including if they escalate the incident to another 'Lead Responder'). If you need to log a service desk ticket to report the incident, use the contact details pre-filled in the table above. If possible, avoid using the device that you think may have been compromised.
4	Incident qualification	<p>Jointly with the Lead Responder, determine if the event is an actual cybersecurity incident.</p> <p><u>If the event is not a cybersecurity incident:</u></p> <p>GO TO STEP 5</p> <p><u>If it is a cybersecurity incident, or it is uncertain:</u></p> <p>GO TO STEP 6</p>	<ul style="list-style-type: none"> In some cases, it may be immediately clear that the event is a cybersecurity incident, but in other cases it may not be clear whether it is just a hoax. For example, if ransomware has locked your computer and is displaying a message demanding payment to 'unlock' your files, and you cannot access those files, then there is clearly an incident. On the other hand, an email saying that a hacker has hacked your computer, or has copies of your confidential files, may be a hoax.





If the event is NOT a cybersecurity Incident

<p>5 Event is not a cybersecurity incident</p> <p>Notify the first point of contact, and any others involved (as needed), that the event is not a cybersecurity incident.</p> <p>Record relevant information relating to the event to help with decisions about any similar future events.</p> <p>END</p>	<ul style="list-style-type: none"> ▪ If a ticket was raised with the IT Service Desk, close the ticket.
---	--

If the event IS or may be a cybersecurity Incident

<p>6 Incident analysis and impact</p> <p>Work with the Lead Responder and the first point of contact to gauge the nature and impact of the incident.</p> <p>Notify your cyber insurer.</p> <p>Continue to record information obtained from Lead Responder and your own observations, including determinations and key decisions made, and nature of information affected. Record times to allow a timeline to be created later if needed.</p> <p>GO TO STEP 7</p>	<ul style="list-style-type: none"> ▪ The incident impact is used to determine the urgency of response, the communication strategy and notification obligations. ▪ Questions such as the following help assess the impact: <ul style="list-style-type: none"> – Is the incident a data breach? i.e., does the incident relate to unauthorised access to, disclosure of, or loss of data? – If so, is the data confidential or personal information? If it is personal information, what kind of information is affected? – What stakeholders (and how many) have been affected by the incident? – How severely has the incident affected your business? – Does the incident involve funds transfer? ▪ Record-keeping is important to support post-incident review activities as well as providing a record to support any investigation. It is also likely to assist with dealing with any claim on your cyber insurance policy. If possible, allocate the responsibility for record-keeping to a colleague, Chambers staff or the IT Service provider. ▪ Depending on your cyber insurance policy, your insurer may recommend incident response specialists.
--	--





7 Containment / evidence collection / communication

Work with the Lead Responder (and other resources) to contain the incident. Work with your cyber insurer to gather any additional evidence needed.

With support from your cyber insurer and / or incident response specialists, manage communications. This will include:

- Any key stakeholders pre-filled in the table above (e.g. your Chambers Clerk and colleagues) and external (e.g. Australian Federal Police, Bar Association).
- Any affected clients or opposing parties. Consider whether you have notification obligations under any written confidentiality agreements. If necessary, review the agreements collected as part of the preparatory steps in the table above.
- Any relevant Courts. Check whether any Courts (especially those which routinely deal with sensitive personal information) have formal notification requirements.

GO TO STEP 8 and

IF the incident involves a data breach:

GO TO STEP 9 and

IF the incident involves ransomware:

GO TO STEP 10

CONTAINMENT

- Containment actions are implemented to minimise the damage, prevent the incident from spreading or escalating, and prevent the attacker from destroying evidence of their attack.
- The Lead Responder may need to call upon additional technical resources to develop and implement the containment plan. This may include third-party incident response specialists. Your cyber insurer may also allocate personnel to support the incident response activities.
- Containment activities may include revoking access, changing passwords, disabling network access, disabling software components or applications and notifying staff and colleagues to increase vigilance and to avoid taking action that could worsen the situation (e.g. clicking on email links).
- If the incident has involved a transfer of funds, contact your financial institution to notify of the incident and to block the transfer.

EVIDENCE COLLECTION

- Consideration needs to be given to the collection, preservation and analysis of digital evidence to support incident investigation. That includes the effect that containment activities may have on the availability and integrity of evidence.
- Evidence will need to be gathered throughout the incident to support incident resolution and investigation. Evidence may also be needed for legal proceedings and to fulfill regulatory reporting obligations.
- The Lead Responder and other personnel as assigned by your cyber insurer (if appropriate) should define what evidence is required to be captured based on the incident type, and how that evidence will be preserved and analysed.

COMMUNICATION

- Communication must be conducted throughout the incident lifecycle.
- The nature (content and timing) of the communications will depend on the incident type, impact and response stage. Additional communications may be needed for a data breach, especially if 'Personal Information' is involved – see Step 9.





<p>8 Eradication</p>	<p>Work with the Lead Responder to eliminate the cause and results of the incident.</p> <p>ONCE INCIDENT ERADICATION IS COMPLETED, GO TO STEP 10</p>	<ul style="list-style-type: none"> ▪ Eradication involves taking steps to ensure the attacker cannot maintain a presence on the affected computer. This usually includes deleting malware, disabling compromised accounts and updating software to remove vulnerabilities. ▪ In some scenarios, the system may need to be rebuilt from a clean installation. This may be required if it cannot be guaranteed that the system has been secured and the attacker completely eradicated.
<p>9 Data breach assessment</p>	<p>Work with the Lead Responder, your cyber insurer and associated specialists such as forensics and legal advisors to identify whether a data breach has occurred, and if so, to undertake an assessment of it.</p> <p>A data breach is when there is unauthorised access to, or disclosure of, personal information held by a person (or information is lost in circumstances where unauthorised access or disclosure is likely to occur)</p> <p>If you have obligations under the Privacy Act (i.e. you are an APP entity), the assessment needs to determine if the breach qualifies as a ‘notifiable data breach’. That is when:</p> <ul style="list-style-type: none"> • The data breach is likely to result in serious harm to any of the individuals to whom the information relates. • The APP entity has been unable to prevent the likely risk of serious harm with remedial action. <p>Even if you are not an APP entity, you may need to contact individuals whose information you hold if that information has been, or may have been, compromised.</p> <p>You should work with your cyber insurer to determine whom to notify, how and when.</p> <p>GO TO STEP 9a</p>	<ul style="list-style-type: none"> ▪ The assessment of the data breach needs to be conducted as expeditiously as possible. ▪ Gather as much information as possible about the data breach to help understand the risk of harm to affected individuals. ▪ When conducting the assessment, consider: <ul style="list-style-type: none"> – The type or types of personal information involved in the data breach. – The circumstances of the data breach, including its cause and extent. – The nature of the harm to affected individuals, and if this harm can be removed through remedial action. ▪ For additional guidance on steps that can be taken to minimise harm to individuals in the event of a data breach, see Guidance for entities in preparing for and responding to cyber incidents OAIC <p>APP ENTITIES AND ‘NOTIFIABLE DATA BREACHES’</p> <ul style="list-style-type: none"> ▪ If you are an ‘APP Entity’ and therefore subject to the requirements of the National Data Breach scheme, you have 30 days to conduct the assessment to determine if the breach is an eligible data breach. See Part 4: Notifiable Data Breach (NDB) Scheme OAIC ▪ See also Notifiable data breaches OAIC for more information on notifiable data breaches.





9a Data breach Notification

If you are an APP Entity:

- if the breach has been determined to meet the criteria of an eligible data breach, individuals at risk of serious harm and the OAIC must be notified as soon as practically possible.
- Even if the breach does not meet the criteria for an eligible data breach, you may still need to contact affected individuals or organisations.
- Work with your cyber insurer (and any legal advisers and crisis management specialists) to prepare the communications.

If you are not an APP Entity, work with your cyber insurer (and any legal advisers and crisis management specialists) to prepare communications to affected individuals or organisations.

IF A RANSOMWARE PAYMENT IS REQUESTED, GO TO STEP 10

ONCE INCIDENT ERADICATION IS COMPLETED, GO TO STEP 11

- When notifying individuals (and if necessary the OAIC), include the following:
 - your name and contact details.
 - a description of the data breach.
 - the kinds of information involved.
 - recommendations about the steps individuals should take in response to the data breach (see below).
- If you need to notify the OAIC, use their online form at [OAIC Web Form](#)
- The recommended steps that individuals should take in response to their data being breached includes:
 - Secure your accounts by changing passwords and implementing multi-factor authentication where possible.
 - Monitor financial accounts and credit activity.
 - Be aware of phishing attempts.
 - Provide contact information for support services such as [IDcare](#).

10 Ransomware

If a ransomware payment is demanded, consult with your cyber insurer (and any legal advisers and crisis management specialists) before making a ransomware payment.

If a ransomware payment has been made, a ‘reporting business entity’ must report that fact within 72 hours: sec 27 of the *Cyber Security Act 2024* (Cth).

ONCE INCIDENT ERADICATION IS COMPLETED, GO TO STEP 11

- The *Cyber Security (Ransomware Payment Reporting) Rules 2025* currently place the mandatory reporting obligation for ransomware payments on businesses with more than \$3m turnover.
- Recent guidance suggests that once a ransomware payment is made, the attackers may demand a second or even third payment.





<p>11 Incident closure</p>	<p>Work with the Lead Responder and other parties such as the incident response specialists to notify relevant parties as needed that the incident has been resolved.</p> <p>GO TO STEP 12</p>	<ul style="list-style-type: none"> ▪ Parties to be notified may include those notified in Step 7 above, such as your Chambers Clerk, relevant bar association, cyber insurer and other stakeholders that have been identified.
<p>12 Post-incident review, reporting and lessons learned</p>	<p>With support from the Chambers Clerk, first point of contact, the Lead Responder and other involved personnel, hold a post-incident review (PIR) meeting as soon as practical after the incident has been resolved.</p> <p>Consider sharing lessons learned with the ABA.</p> <p>Implement any identified and agreed opportunities for improvement to minimise the risk of future incidents.</p> <p>END</p>	<ul style="list-style-type: none"> ▪ The PIR is intended to answer key questions such as: <ul style="list-style-type: none"> – Exactly what happened, and at what times? – What was the root cause of the incident, and could this have been avoided? What steps have been taken to prevent a repeat? – Have all legal/regulatory requirements been met? – How well did all parties perform in dealing with the incident? – Was communication accurate, complete and timely? – How could information sharing with external authorities such as the ACSC and OAIC be improved?

