Cybersecurity for Law Firms: Evolving Scams, Updated Standards

LEGAL PRACTITIONERS' LIABILITY COMMITTEE

lplc.com.au

Acknowledgement of Country

This session is being held on the lands of the Wurundjeri people of the Kulin Nation and on behalf of LPLC, I wish to acknowledge them as the traditional owners of the land.

I also acknowledge the traditional owners of the lands which all of those joining us online today are living, learning and working on.

I would also like to pay my respects to their Elders past and present, and any Elders of other communities who may be present today.

Presenters

Ryan Ettridge from **CyberCert**

Bryan Cavanagh from the **Australian Signals Directorate**

Fabian Horton from **LPLC**

Welcome

Today's Schedule

- Recent Trends in Cyber-Attacks
- Standards and Consultants
- Reporting
- Key Messages
- Q&A Session

Why Cybersecurity Matters More Than Ever

- A continued increase in **digital reliance** – digital identification, transactions, and communications
- Expansion of **attack vectors** incorporating sophisticated AI-powered threats such as real-time malware adaptation, deepfakes, and cybercrime-as-a-service platforms
- Law firms remain prime targets with **specific vulnerabilities** related to funds and data

Why are Lawyers Always Targets?

The Trends

Increasing Attack Types

	2021	2022	2023	2024	2025
#1 Attack Type	Malware	Malware	Malware	Malware	Malware
#2 Attack Type	Ransomware	Ransomware	Ransomware	Ransomware	Phishing
#3 Attack Type	Phishing	Phishing	Phishing	Phishing	Ransomware

Top Threat Actors

	2021	2022	2023	2024	2025
#1 Threat Actor	Malicious insiders	Human error	Human error	External attackers — hacktivists	External attackers — hacktivists
#2 Threat Actor	Human error	External attackers — hacktivists	External attackers — hacktivists	Human error	External attackers — nation-state actors
#3 Threat Actor	External attackers	External attackers — nation-state actors	External attackers — nation-state actors	External attackers — nation-state actors	Human error

Thales: 2025 Threat Report

Key Risk Areas for Law Firms

There are multiple vulnerabilities that criminals exploit.

- Email compromise: modified emails, redirected funds
- Inadequate email protection security software
- Weak password policies
- Lack of Multifactor Authentication (MFA)
- Outdated software and systems
- Inadequate staff training
- Poor backup & incident response planning

Key Risk Areas for Law Firms

Politics Federal Cyber security

The weakest link: Stolen staff passwords now the biggest cyber threat to workplaces

Natassia Chrysanthos

October 13, 2025 — 10.30pm

Save Share A A A 38 View all comments

Australians' stolen usernames and passwords are increasingly being used by cybercriminals to gain access to workplaces, with two in five critical security incidents hitting large companies, governments and academic institutions now coming from compromised accounts or credentials.

China-linked cyber actors are also using Australians' vulnerable home internet connections and smart devices to create larger networks that conceal their identities when they launch cyberattacks across the world.

Key Risk Areas for Law Firms

Annual Cyber Threat Report highlights persistent threat to individuals and across the Australian economy

14 OCTOBER 2025

The Australian Signals Directorate's (ASD) Annual Cyber Threat Report for 2024-25 highlights the persistent threat of malicious cyber activity to the nation, underscoring the urgency of action by all Australians and Australian businesses to raise the nation's cyber defences.

This year's report illustrates how cyber criminals continue to impact many Australians, leveraging new technologies and techniques to expand their destructive attacks and cause widespread financial harm.

It also details how state cyber actors continue to target business and critical infrastructure, as well as all levels of Australian government, in an attempt to conduct espionage, steal sensitive data or posture for disruptive attacks. These findings make it critical that all Australian businesses develop robust business continuity plans for service disruptions caused by a cyber incident.

Joint media release

The Hon Richard Marles MP

Deputy Prime Minister

Minister for Defence

Media contact

dpm.media@defence.gov.au

02 6277 7800

Key Risk Areas for Law Firms

Policy Foreign Affairs & Security Cyber warfare

Cybersecurity chief warns AI-powered hacking will be the new normal

Michael Read *Foreign affairs and defence correspondent*

Oct 12, 2025 – 8.00pm

Listen to this article
6 min

The country's most senior cybersecurity official has warned widespread adoption of artificial intelligence by criminal groups will supercharge a wave of hacking that is already overwhelming major businesses, making attempts at stealing personal information almost impossible to detect.

Lieutenant General Michelle McGuinness, the National Cyber Security Coordinator, met with the major banks and hosted a discussion with 1000 businesses last week as the government ramps up efforts to stop hacking.

Evolving Scams & Attack Trends

The evolving attack types.

- **Phishing more sophisticated**: AI-powered campaigns
- **Business Email Compromise**: MFA session compromise
- **Domain Spoofing**: malicious lookalike domains targeting the legal sector
- **Ransomware**: systems inaccessible and stolen data
- **Insider Threats**: deliberate and accidental

Real-World Impact

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

Reputational and business consequences

STANDARDS

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

Expectations and Standards

VLSB+C	LPLC	DSI SMB1001	ACSC
Minimum Expectations	Cyber Guide	Dynamic, Certfiable Standard	Essential Eight
For lawyers	For lawyers	Industry Versions	For anyone
Red flag guidance	Risk management content	Guidelines for SMBs	Precedents and guidelines

Why have standards?

Built on a foundation of threat analysis

- Evidence based controls formed from root-cause analysis
- Cross Industry intelligence and monitoring

Material business advantages

- Expectation compliance (fulling existing obligations)
- Shows reasonable care in protecting data and reducing exposure

Connection between standards and measurable risk reduction

- Measurable security baseline, enabling progress tracking and comparison
- Risk quantification enable formal risk assessment
- Incident rate reduction demonstrated through fewer successful attacks

Multiple standards, tiered models, uplift paths

- **Progressive implementation**: Enable **staged investment** aligned with growth and threat evolution
- **Risk-appropriate scaling**: Different standards suit **different firm sizes** and risk profiles
- **Continuous improvement**: **ongoing enhancements** rather than one-time compliance
- **Resource optimisation**: prioritise **highest-impact controls first**, then build coverage over time
- **Future-proofing**: ensure security **measures scale** with evolving threats and business growth

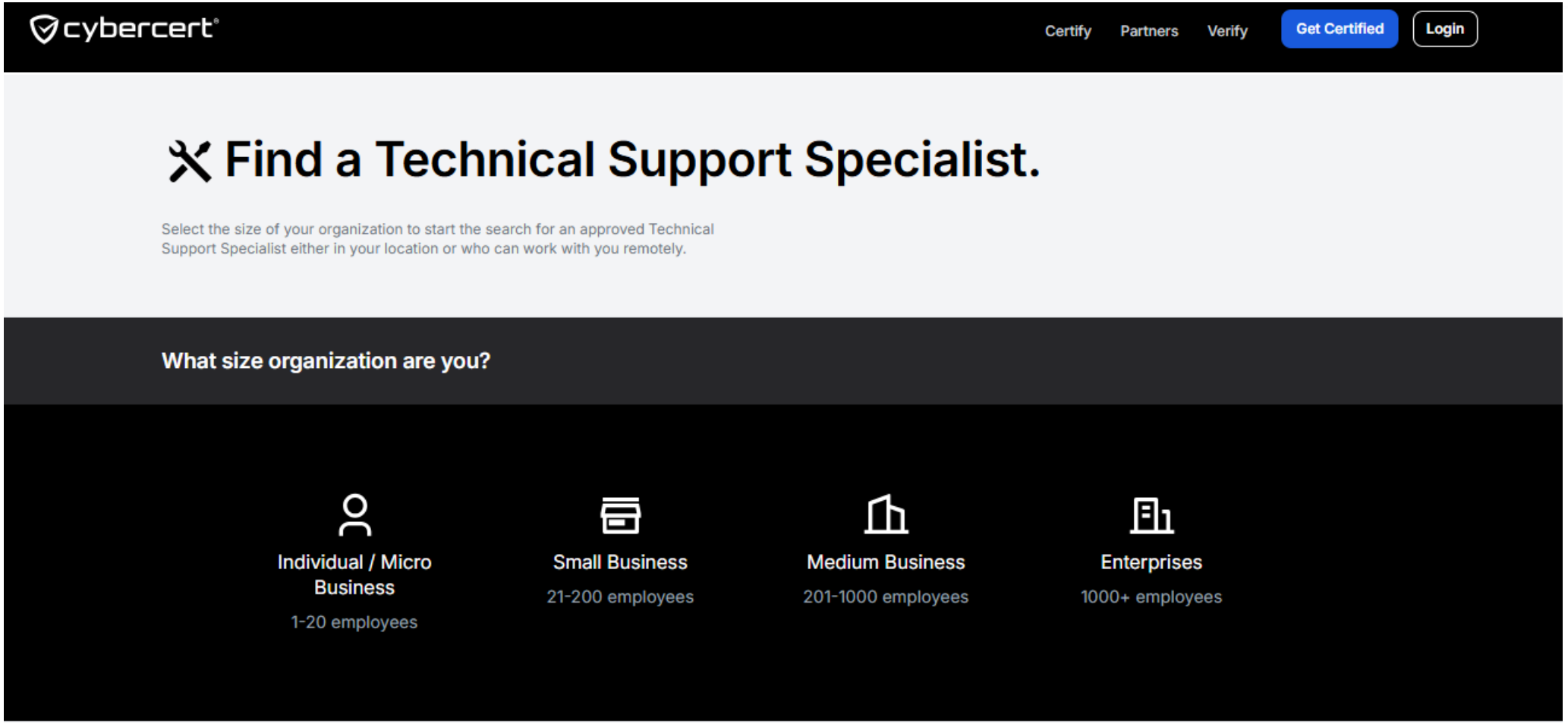
Attaining a standard

- Undertake your risk assessment
- Flexibility to achieve optimum result – controls from different standards/levels
- Extensive flexibility benefits including:
  - scalable implementation,
  - risk-based approaches,
  - multiple compliance pathways,
  - cost-effectiveness

Why cybersecurity consultants matter

- Many controls are technically complicated
- Most breaches trace to unimplemented basics: MFA, patching, staff action
- Consultants assist with technical audits
- CyberCert partners: certified, practical solutions, ongoing support
- Boost compliance, trust, and cyber-insurance eligibility

Finding support



REPORTING

Reporting

Why Report to ASD?

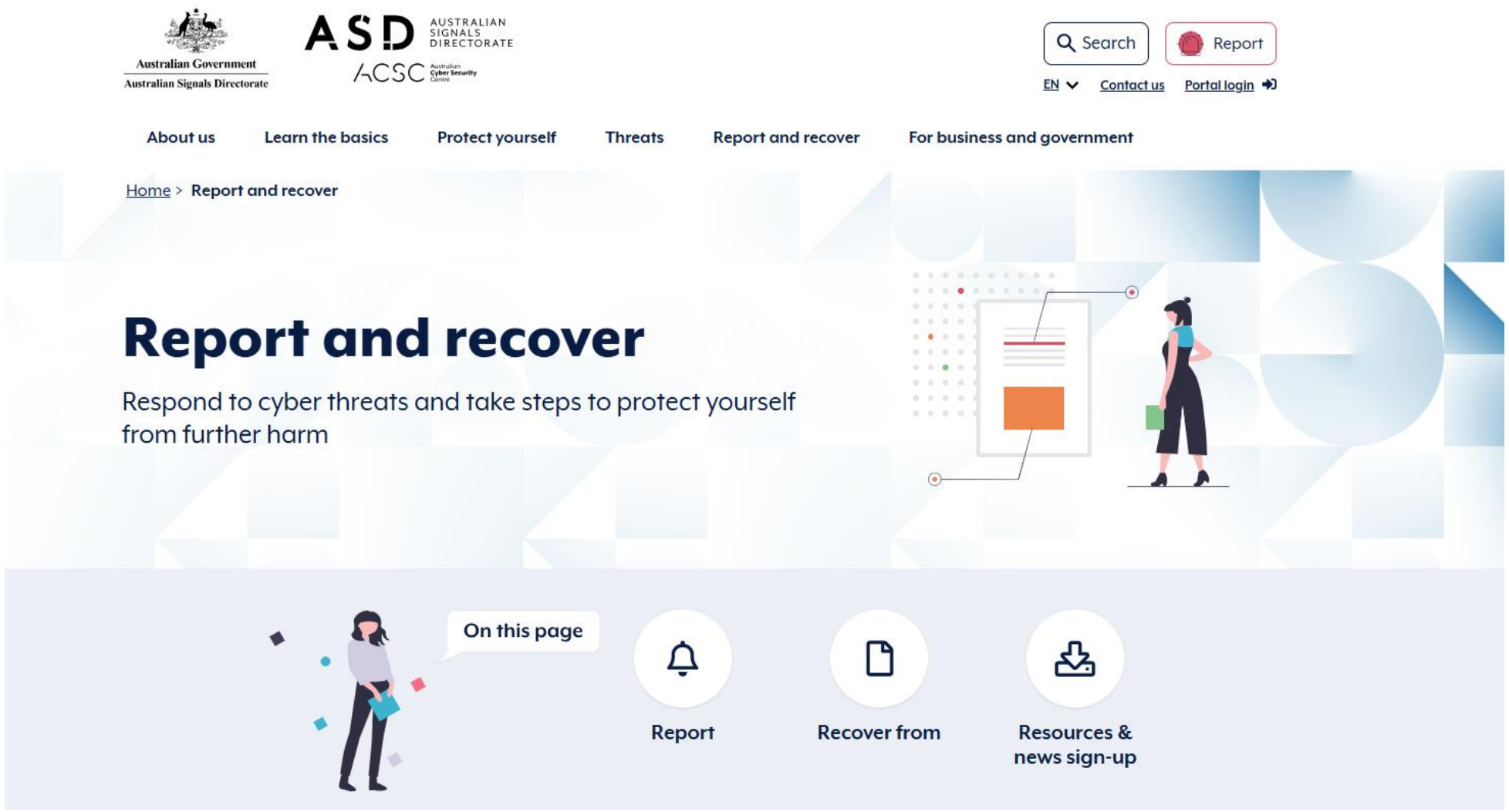
- ASD not a regulator: **focus on technical assistance**, not compliance enforcement
- 24/7 **technical support** available: ASC Hotline 1300 CYBER1 (1300 292 371)
- Early reporting improves outcomes: **Timeliness is critical** in incident management
- Strengthens **national cyber security**: help protect others

Reporting

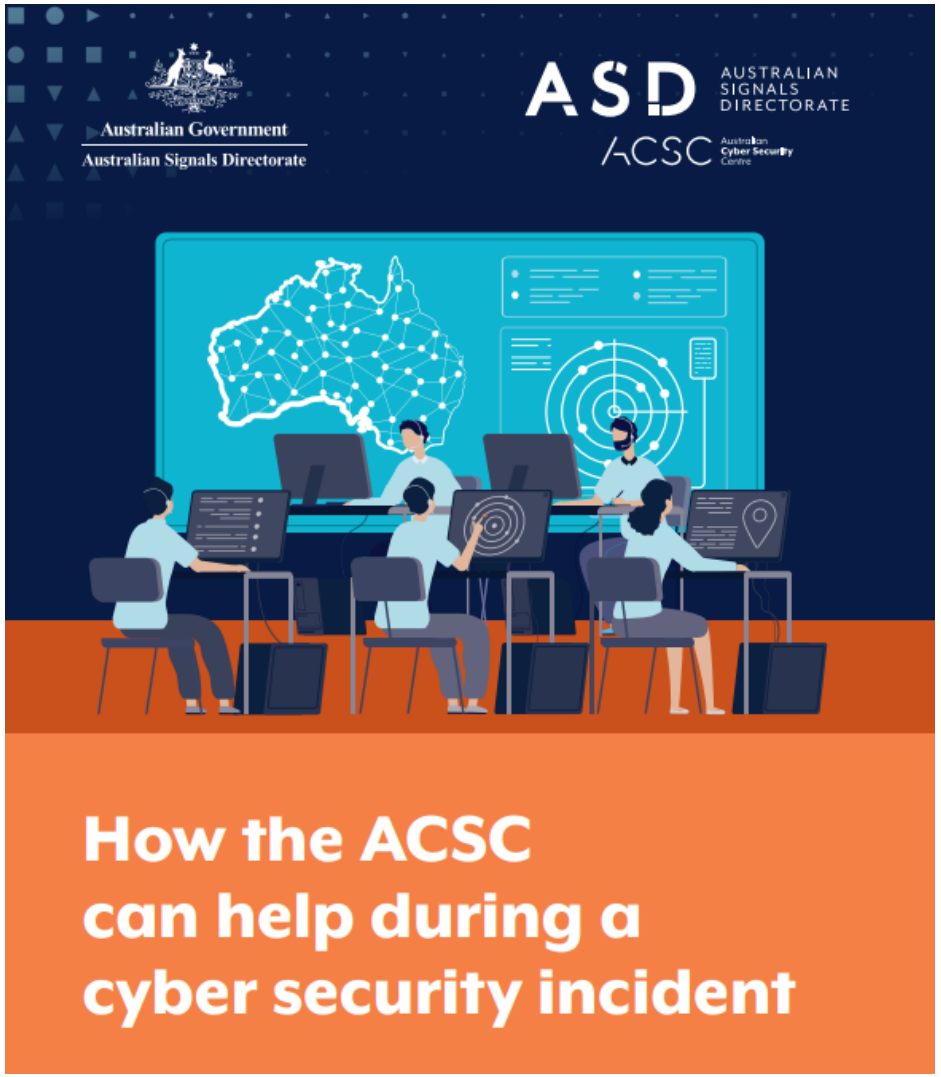
What Types of Incidents Should Be Reported?

- Ransomware attacks
- Data exposure, theft or leak
- Phishing/spear-phishing
- Malicious code/malware
- Intentional or malicious unauthorised access
- Denial of service attacks
- Any irregular cyber activity that causes concern

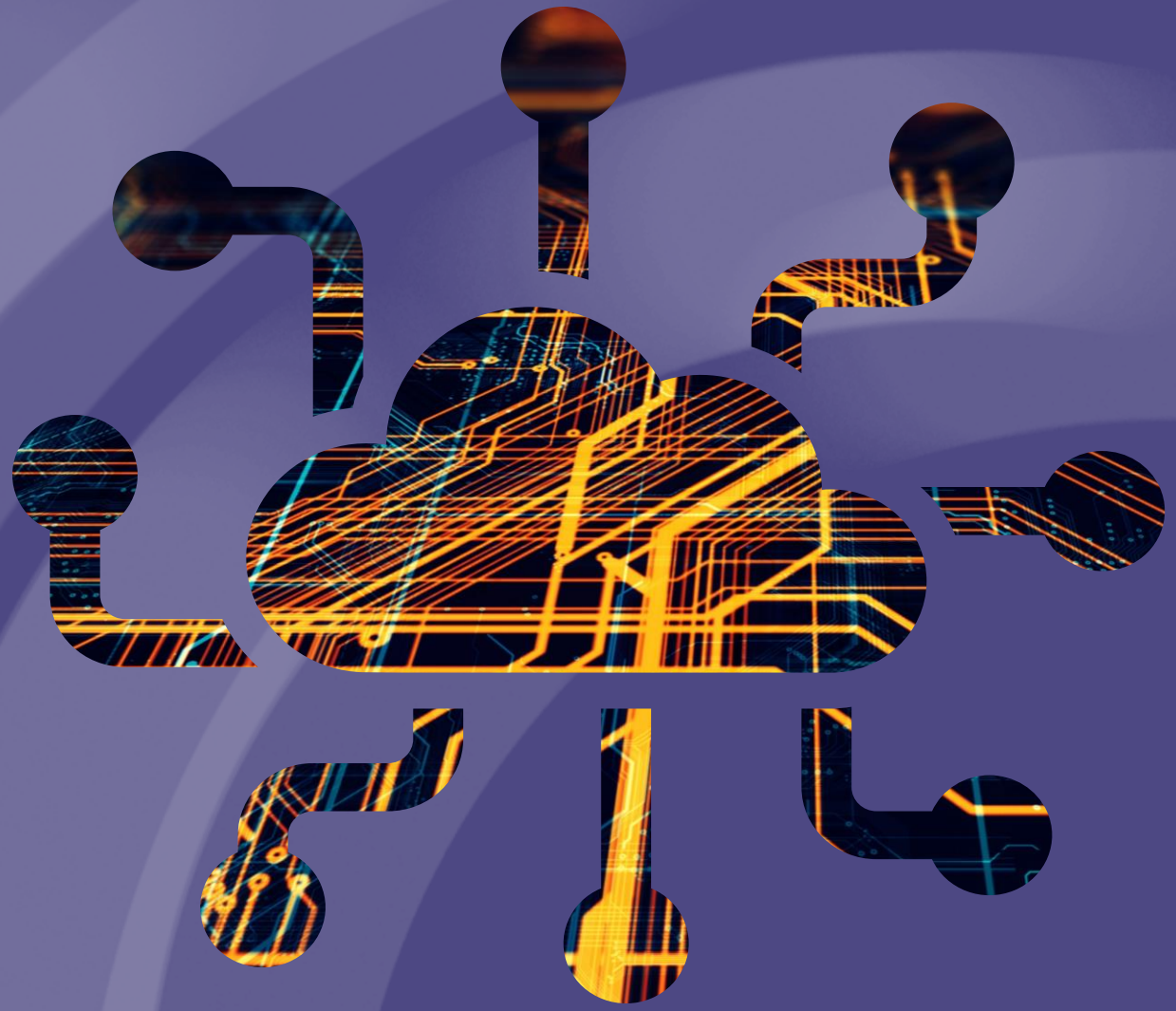
Reporting


Australian Government
Australian Signals Directorate
ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre
Search
Report
EN
Contact us
Portal login
About us
Learn the basics
Protect yourself
Threats
Report and recover
For business and government
Home > Report and recover
Report and recover
Respond to cyber threats and take steps to protect yourself from further harm
On this page
Report
Recover from
Resources & news sign-up

Reporting


Australian Government
Australian Signals Directorate
ASD
AUSTRALIAN SIGNALS DIRECTORATE
ACSC
How the ACSC can help during a cyber security incident

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 customization 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.

Key Messages

Cyber warnings

- In all correspondence, particularly email footer
- Explain the issues in the initial correspondence (retainer letter)
- Verbally explain the issues in early meetings

Call before you pay

- Understand your process and what you are trying to do
- Don’t blindly follow the process and see the gaps

Key Messages

Key Messages

Monitor logs and systems

- Have specific processes for checking
- Have a dedicated team member responsible for task
- If expertise is not available in the firm, get outside assistance

Cyber resiliency (How to manage the fallout)

- How well to you respond / unwind the situation
- Can I get assurance over the process that we are implementing
- Policy looks amazing but are you able to pivot.

Points to Remember

- Lawyers work in an **information business**. Secure your main asset.
- **Double deductible** if you don't have MFA.
- 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.

Points to Remember

The underlying issue is to

understand the digital/cyber paradigm

that we operate in so that if something happens that is not ‘within the playbook’ there is a greater chance of recognising the issue.

NEXT ACTION STEPS

NEXT ACTION STEPS

TAKE TRAINING

HIRE CONSULTANTS

READ THE RISK GUIDES

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

LEGAL PRACTITIONERS' LIABILITY COMMITTEE

lplc.com.au