Cyber Security

Malcolm Heath, Practice Risk Manager

Presentation outline

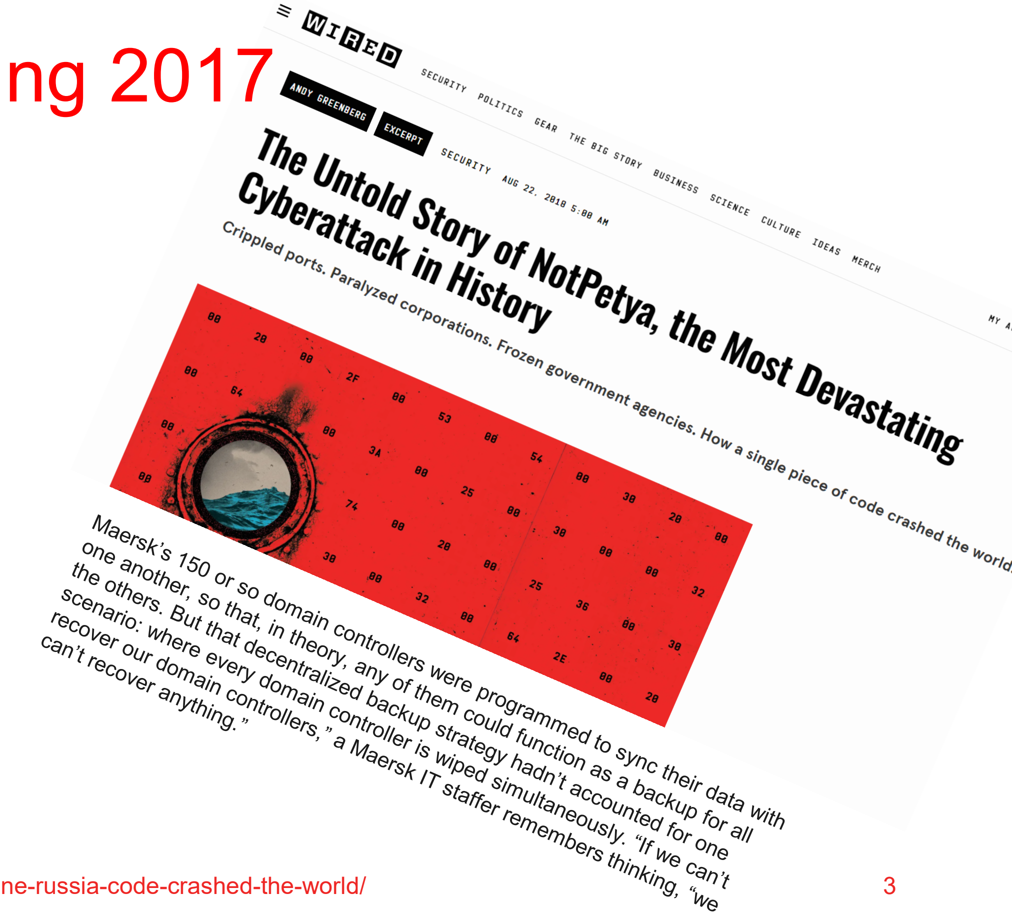
- Cyber Crime – a short history
- Data breaches and notifications
- Confidential information and community concerns
- Working with government
- Penalties
- Supply chain risks
- Opportunities through adversity

NotPetya - Maersk Shipping 2017

– "Close to a fifth of the entire world's shipping capacity, was dead in the water"

– Thank goodness for Ghana

– Learning from "black swan" events



≡ WIRED

SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH

MY A

ANDY GREENBERG EXCERPT SECURITY AUG 22, 2018 5:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

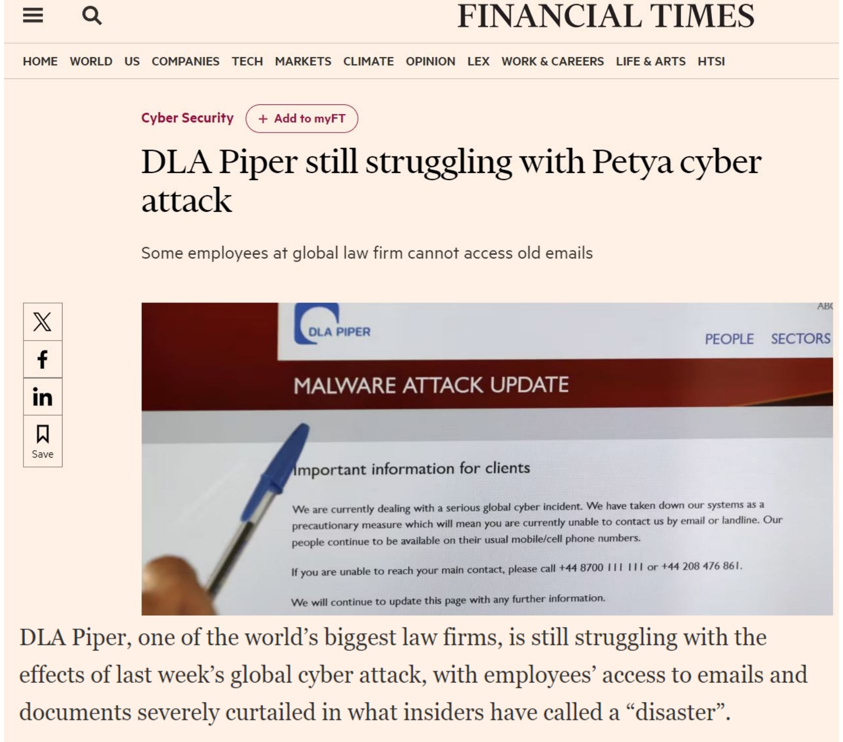
Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world

Maersk's 150 or so domain controllers were programmed to sync their data with one another, so that, in theory, any of them could function as a backup for all the others. But that decentralized backup strategy hadn't accounted for one scenario: where every domain controller is wiped simultaneously. "If we can't recover our domain controllers," a Maersk IT staffer remembers thinking, "we can't recover anything."

Ref:https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

NotPetya - DLA Piper 2017

- 3,600 lawyers in 40 countries, revenue of USD$2.5b
- For two days after the attack, all emails and phones were knocked
- One week on "employees' access to emails and documents severely curtailed"
- Learning from "black swan" events



DLA Piper still struggling with Petya cyber attack

Some employees at global law firm cannot access old emails

Important information for clients

We are currently dealing with a serious global cyber incident. We have taken down our systems as a precautionary measure which will mean you are currently unable to contact us by email or landline. Our people continue to be available on their usual mobile/cell phone numbers.

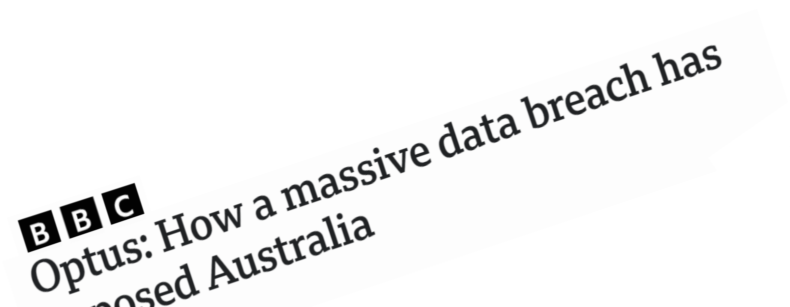
If you are unable to reach your main contact, please call +44 8700 111 111 or +44 208 476 861.

We will continue to update this page with any further information.

DLA Piper, one of the world's biggest law firms, is still struggling with the effects of last week's global cyber attack, with employees' access to emails and documents severely curtailed in what insiders have called a "disaster".

https://www.ft.com/content/1b5f863a-624c-11e7-91a7-502f7ee26895

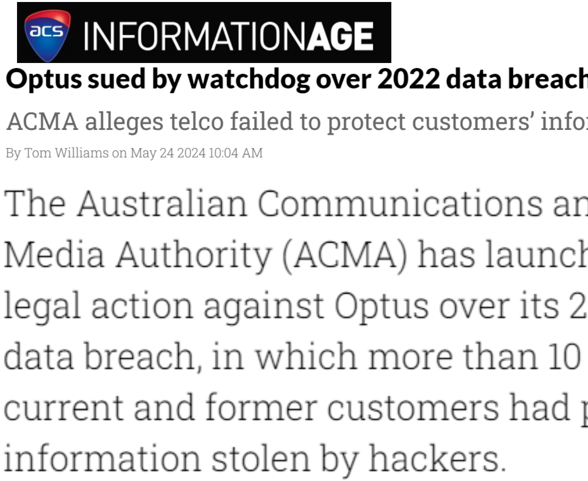
The alarm bells - Medibank Private & Optus



BBC

Optus: How a massive data breach has exposed Australia

29 September 2022



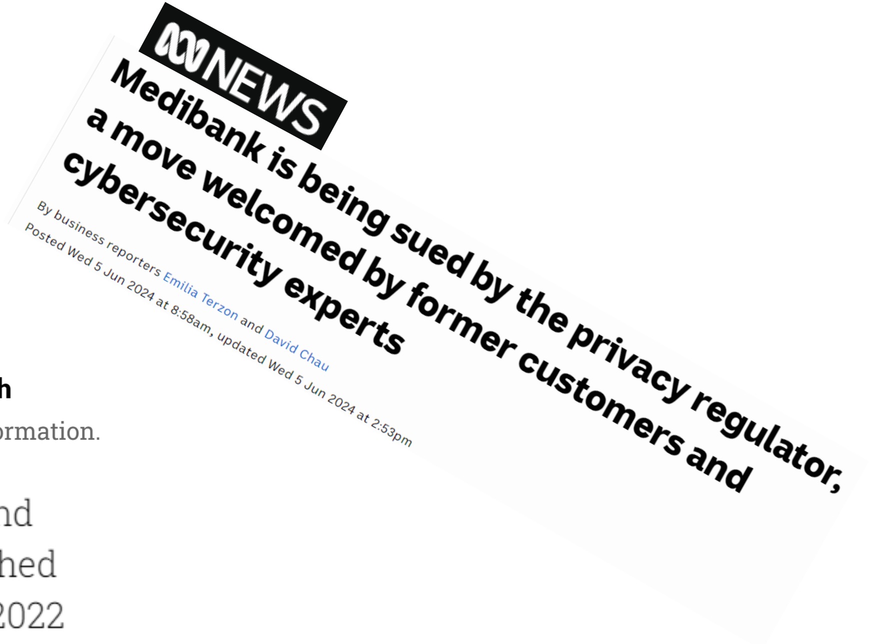
INFORMATIONAGE

Optus sued by watchdog over 2022 data breach

ACMA alleges telco failed to protect customers' information.

By Tom Williams on May 24 2024 10:04 AM

The Australian Communications and Media Authority (ACMA) has launched legal action against Optus over its 2022 data breach, in which more than 10 million current and former customers had personal information stolen by hackers.



ABC NEWS

Medibank is being sued by the privacy regulator, a move welcomed by former customers and cybersecurity experts

By business reporters Emilia Terzon and David Chau

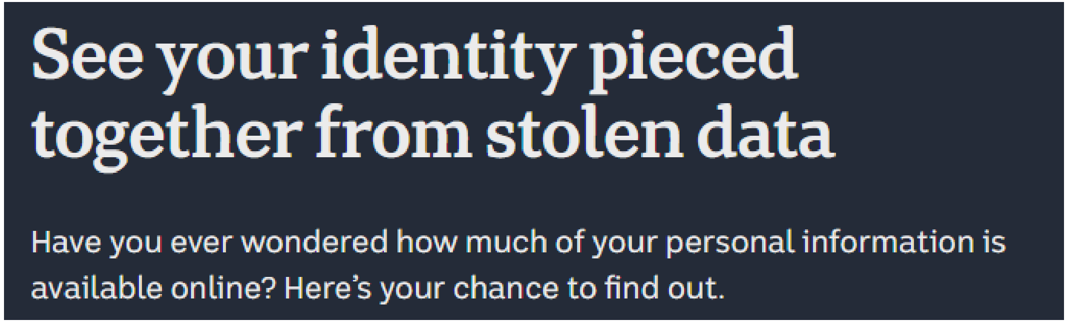
Posted Wed 5 Jun 2024 at 8:58am, updated Wed 5 Jun 2024 at 2:53pm

Lawcover

Major data breaches 2024/25 - Australia

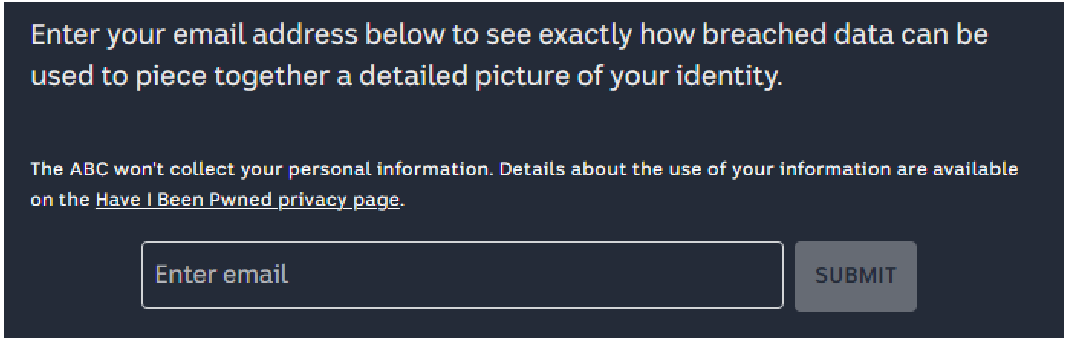
https://www.webberinsurance.com.au/data-breaches-list

';--have i been pwned?



See your identity pieced together from stolen data

Have you ever wondered how much of your personal information is available online? Here’s your chance to find out.

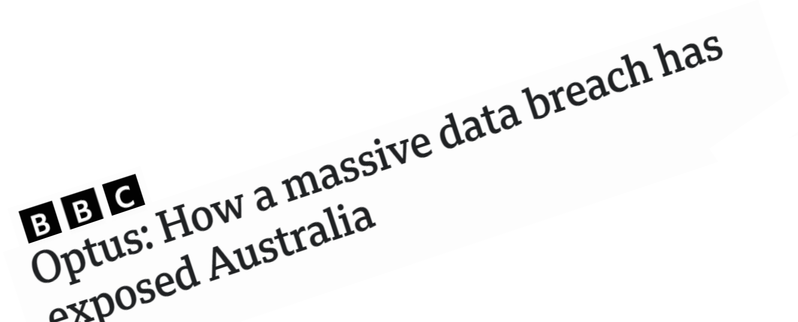


Enter your email address below to see exactly how breached data can be used to piece together a detailed picture of your identity.

The ABC won't collect your personal information. Details about the use of your information are available on the Have I Been Pwned privacy page.

https://www.abc.net.au/news/2023-05-18/data-breaches-your-identity-interactive/102175688

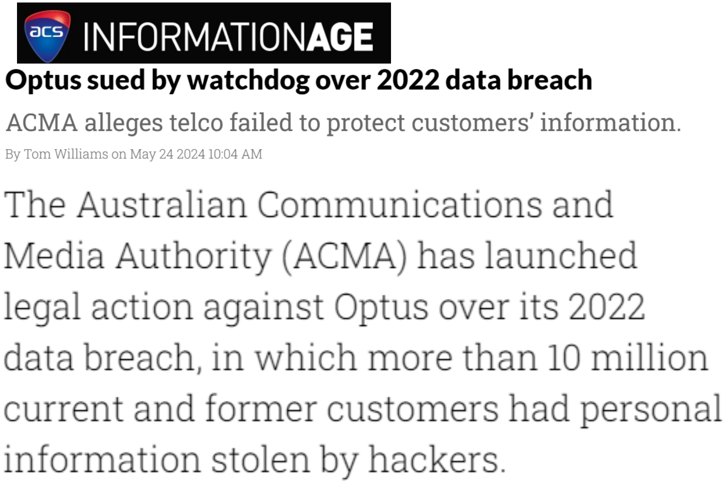
The alarm bells - Medibank Private & Optus



BBC

Optus: How a massive data breach has exposed Australia

29 September 2022



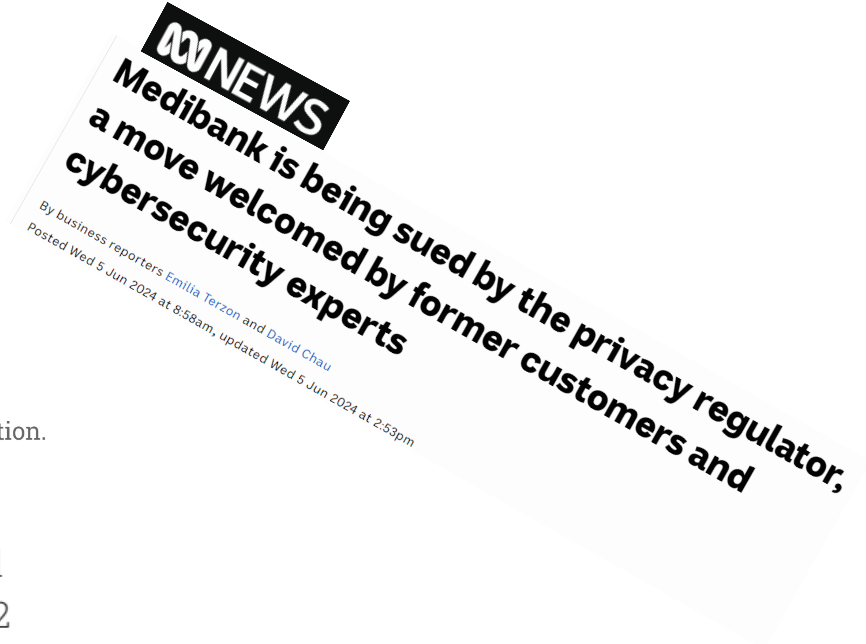
INFORMATIONAGE

Optus sued by watchdog over 2022 data breach

ACMA alleges telco failed to protect customers' information.

By Tom Williams on May 24 2024 10:04 AM

The Australian Communications and Media Authority (ACMA) has launched legal action against Optus over its 2022 data breach, in which more than 10 million current and former customers had personal information stolen by hackers.



ABC NEWS

Medibank is being sued by the privacy regulator, a move welcomed by former customers and cybersecurity experts

By business reporters Emilia Terzon and David Chau

Posted Wed 5 Jun 2024 at 8:58am, updated Wed 5 Jun 2024 at 2:53pm

Medibank Private & Optus – AIC Representative Complaints

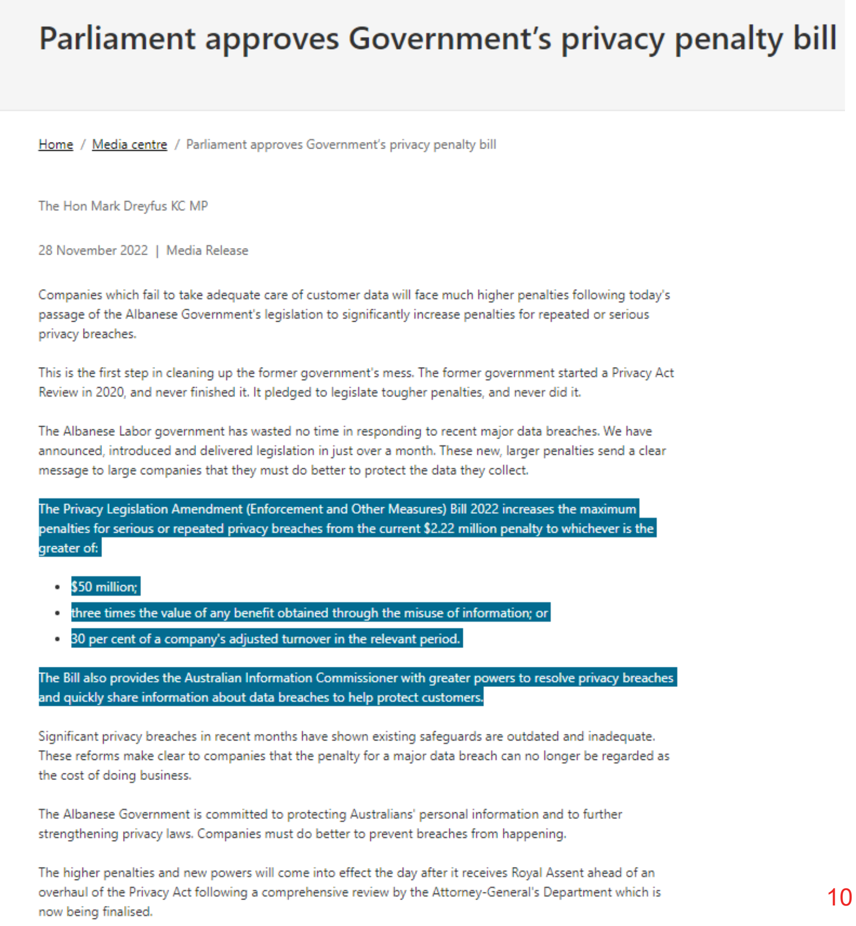
- A Representative Complaint is a complaint made by an individual under section 36 of the Privacy Act 1988 (Ch) (Privacy Act) on behalf of other individuals who have similar complaints about an act or practice that may be an interference with their privacy.
- The AIC has decided to investigate the Medibank and Optus representative complaints concurrently with the Commissioner-initiated investigations (CII) into the same respondent entities.

Ref: https://www.oaic.gov.au/newsroom/representative-complaints#what-is-a-representative-complaint

Increased penalties result

Whatever is the greater of:

- $50 million;
- Three times the value of any benefit obtained through the misuse of information; or
- 30% of a company's adjusted turnover in the relevant period.
- Greater powers to AIC



Parliament approves Government's privacy penalty bill

Home / Media centre / Parliament approves Government's privacy penalty bill

The Hon Mark Dreyfus KC MP

28 November 2022 | Media Release

Companies which fail to take adequate care of customer data will face much higher penalties following today's passage of the Albanese Government's legislation to significantly increase penalties for repeated or serious privacy breaches.

This is the first step in cleaning up the former government's mess. The former government started a Privacy Act Review in 2020, and never finished it. It pledged to legislate tougher penalties, and never did it.

The Albanese Labor government has wasted no time in responding to recent major data breaches. We have announced, introduced and delivered legislation in just over a month. These new, larger penalties send a clear message to large companies that they must do better to protect the data they collect.

The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 increases the maximum penalties for serious or repeated privacy breaches from the current $2.22 million penalty to whichever is the greater of:

- $50 million;
- three times the value of any benefit obtained through the misuse of information; or
- 30 per cent of a company's adjusted turnover in the relevant period.

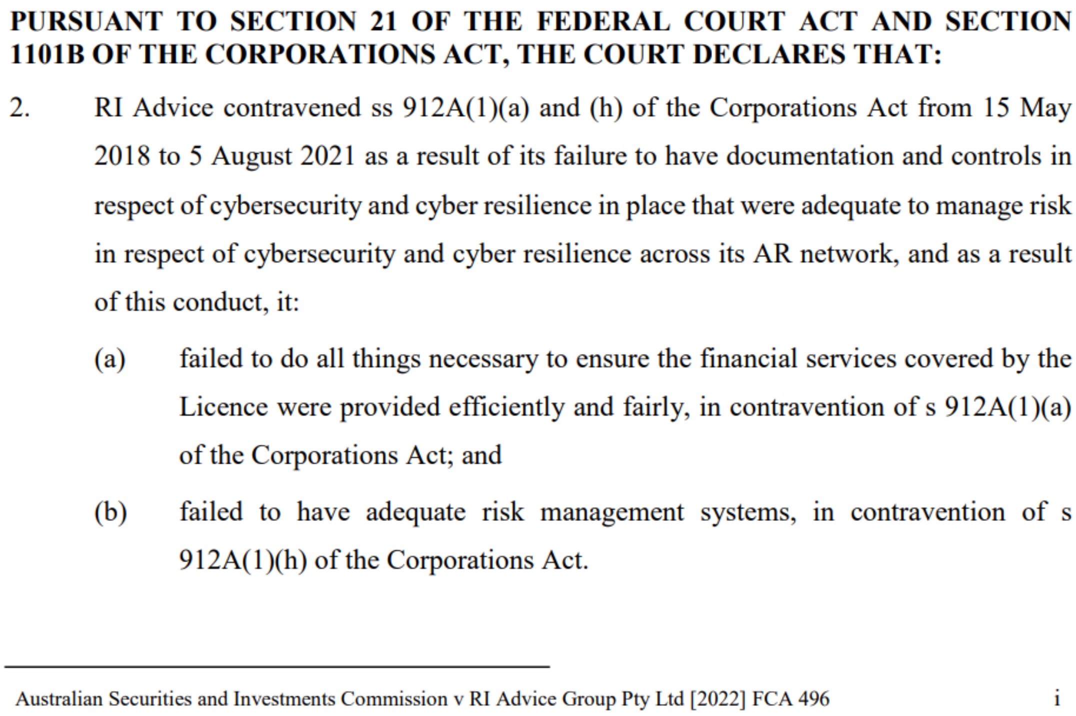
The Bill also provides the Australian Information Commissioner with greater powers to resolve privacy breaches and quickly share information about data breaches to help protect customers.

Significant privacy breaches in recent months have shown existing safeguards are outdated and inadequate. These reforms make clear to companies that the penalty for a major data breach can no longer be regarded as the cost of doing business.

The Albanese Government is committed to protecting Australians' personal information and to further strengthening privacy laws. Companies must do better to prevent breaches from happening.

The higher penalties and new powers will come into effect the day after it receives Royal Assent ahead of an overhaul of the Privacy Act following a comprehensive review by the Attorney-General's Department which is now being finalised.

Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496



PURSUANT TO SECTION 21 OF THE FEDERAL COURT ACT AND SECTION 1101B OF THE CORPORATIONS ACT, THE COURT DECLARES THAT:

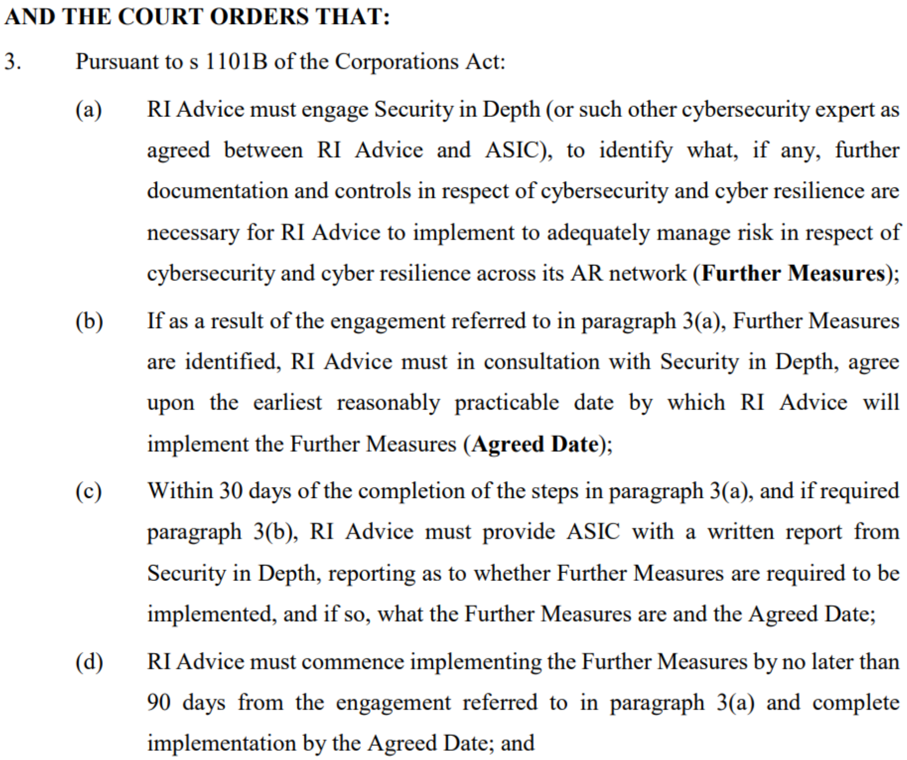
2. RI Advice contravened ss 912A(1)(a) and (h) of the Corporations Act from 15 May 2018 to 5 August 2021 as a result of its failure to have documentation and controls in respect of cybersecurity and cyber resilience in place that were adequate to manage risk in respect of cybersecurity and cyber resilience across its AR network, and as a result of this conduct, it:

   (a) failed to do all things necessary to ensure the financial services covered by the Licence were provided efficiently and fairly, in contravention of s 912A(1)(a) of the Corporations Act; and

   (b) failed to have adequate risk management systems, in contravention of s 912A(1)(h) of the Corporations Act.

Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496 i

Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496



AND THE COURT ORDERS THAT:

3. Pursuant to s 1101B of the Corporations Act:

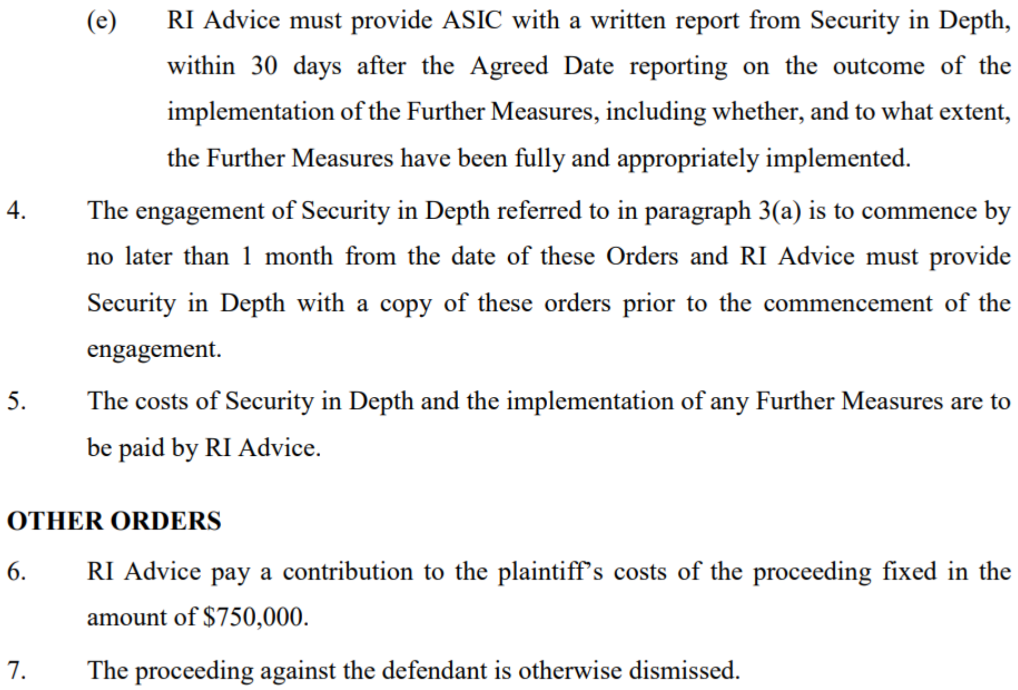
   (a) RI Advice must engage Security in Depth (or such other cybersecurity expert as agreed between RI Advice and ASIC), to identify what, if any, further documentation and controls in respect of cybersecurity and cyber resilience are necessary for RI Advice to implement to adequately manage risk in respect of cybersecurity and cyber resilience across its AR network (**Further Measures**);

   (b) If as a result of the engagement referred to in paragraph 3(a), Further Measures are identified, RI Advice must in consultation with Security in Depth, agree upon the earliest reasonably practicable date by which RI Advice will implement the Further Measures (**Agreed Date**);

   (c) Within 30 days of the completion of the steps in paragraph 3(a), and if required paragraph 3(b), RI Advice must provide ASIC with a written report from Security in Depth, reporting as to whether Further Measures are required to be implemented, and if so, what the Further Measures are and the Agreed Date;

   (d) RI Advice must commence implementing the Further Measures by no later than 90 days from the engagement referred to in paragraph 3(a) and complete implementation by the Agreed Date; and

Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496



(e) RI Advice must provide ASIC with a written report from Security in Depth, within 30 days after the Agreed Date reporting on the outcome of the implementation of the Further Measures, including whether, and to what extent, the Further Measures have been fully and appropriately implemented.

4. The engagement of Security in Depth referred to in paragraph 3(a) is to commence by no later than 1 month from the date of these Orders and RI Advice must provide Security in Depth with a copy of these orders prior to the commencement of the engagement.

5. The costs of Security in Depth and the implementation of any Further Measures are to be paid by RI Advice.

OTHER ORDERS

6. RI Advice pay a contribution to the plaintiff's costs of the proceeding fixed in the amount of $750,000.

7. The proceeding against the defendant is otherwise dismissed.

https://download.asic.gov.au/media/zhodijpp/22-104mr-2022-fca-496.pdf

Government Response Privacy Act Review Report

- Australians are seeking greater protection in the handling of their personal information
- 2023 ACAP survey - Three in five (62%) of Australians surveyed see the protection of their personal information as a major concern in their life
- 75% consider that data breaches are one of the biggest privacy risks they face today
- 84% want more control and choice over the collection and use of their personal information
- 89% would like the Government to provide more legislation in this area

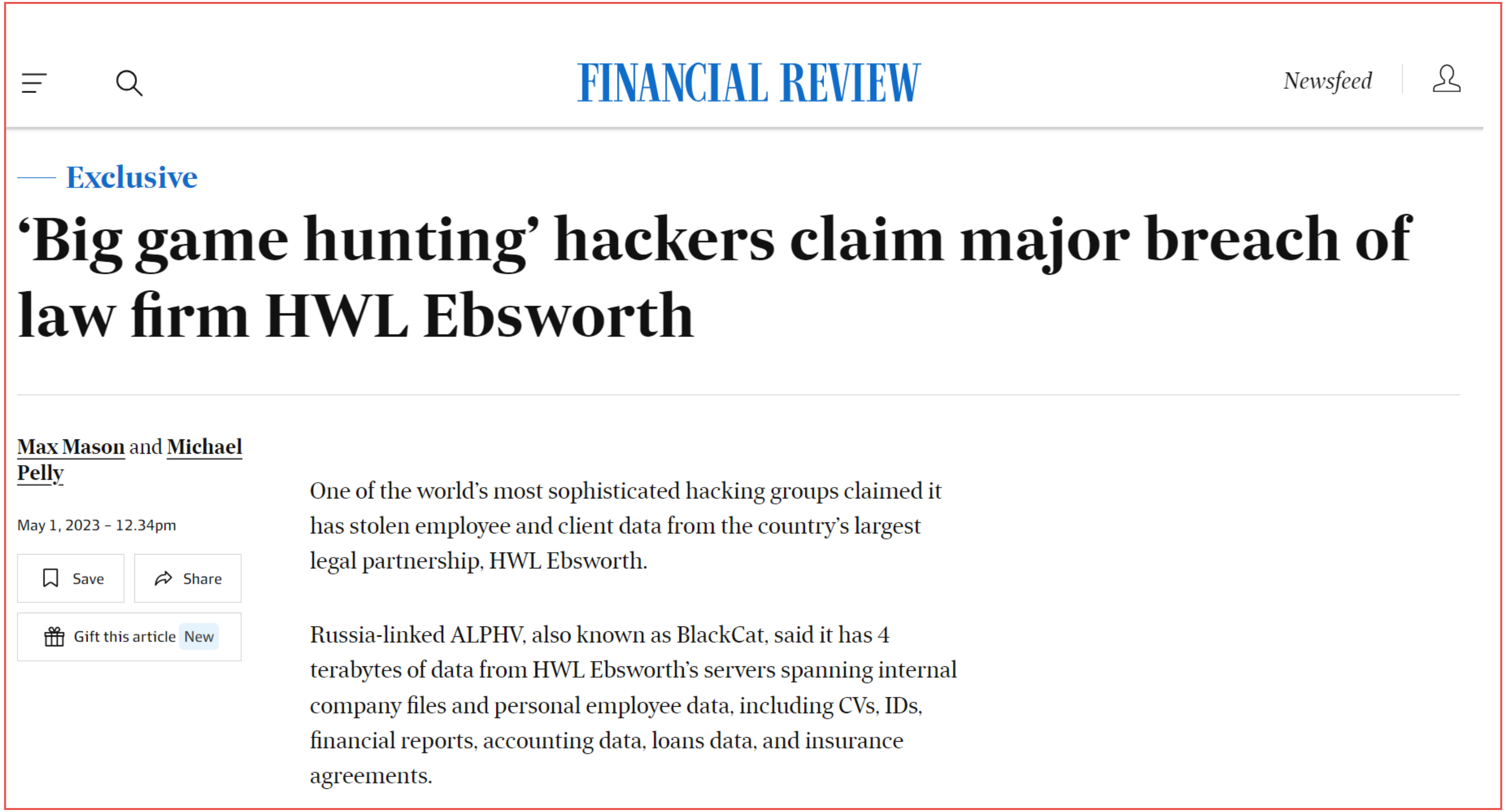
Australian Government

Government Response | Privacy Act Review Report

ACHIEVING A JUST AND SECURE SOCIETY | WWW.AG.GOV.AU

https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF

Nightmares for organisations



Exclusive

‘Big game hunting’ hackers claim major breach of law firm HWL Ebsworth

Max Mason and Michael Pelly

May 1, 2023 – 12.34pm

One of the world’s most sophisticated hacking groups claimed it has stolen employee and client data from the country’s largest legal partnership, HWL Ebsworth.

Russia-linked ALPHV, also known as BlackCat, said it has 4 terabytes of data from HWL Ebsworth’s servers spanning internal company files and personal employee data, including CVs, IDs, financial reports, accounting data, loans data, and insurance agreements.

Businesses working with government

- Lessons Learned
  - What worked well?
  - What was challenging?
  - What was interesting?
- Applying the lessons learned

Official TLP: Clear

Australian Government
National Office of Cyber Security

HWL Ebsworth Cyber Security Incident

National Office of Cyber Security | Lessons Learned Review

February 2024

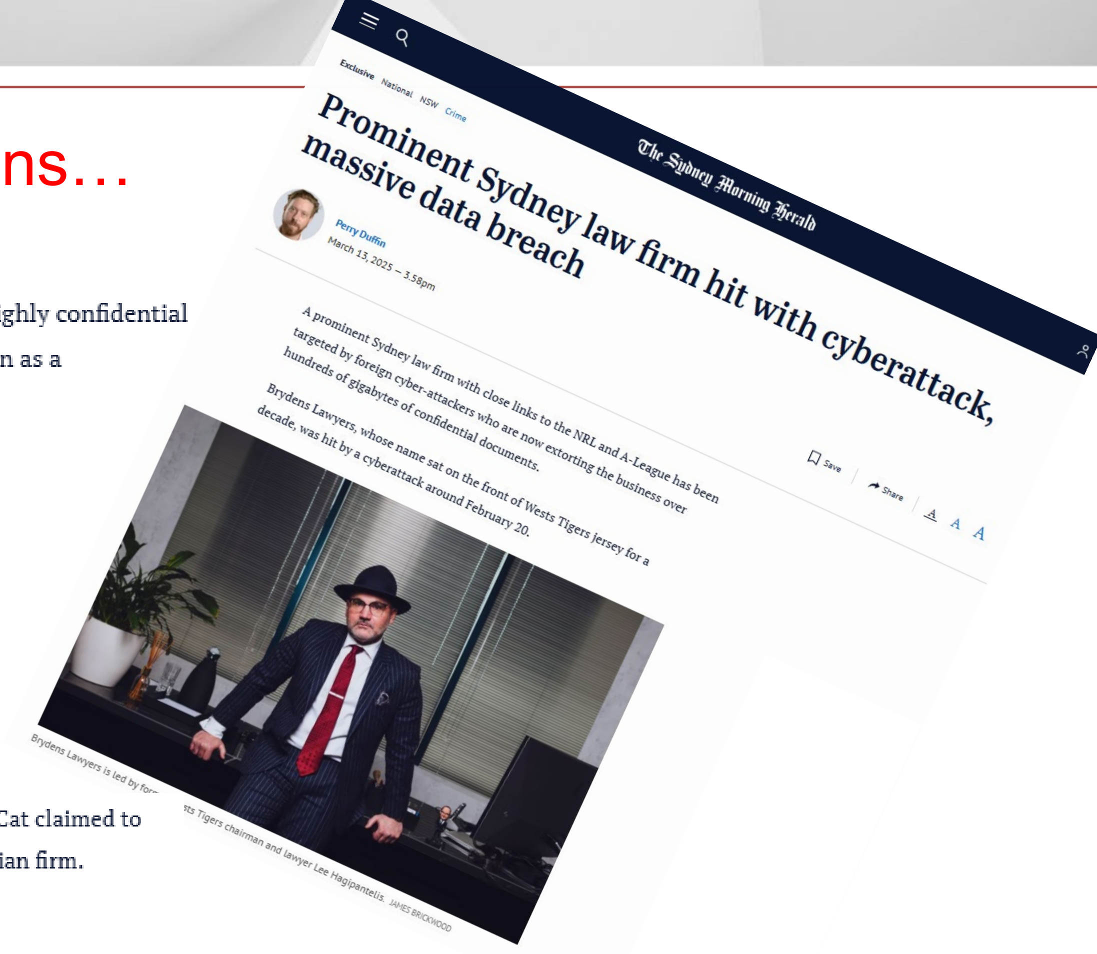
Ref: https://NOCS HWL Ebsworth Lessons Learned Report (homeaffairs.gov.au)

Nightmares for organisations…

> “ As legal offices are entrusted with reams of highly sensitive, highly confidential documents, Brydens is not the first firm to suffer what is known as a “ransomware” attack.

> “ Just one month earlier, in mid-January, staff of New Zealand firm Bell and Graham returned from their Christmas break to find their server had been breached.

> “ Two years ago, a Russian-linked group calling itself ALPHV/BlackCat claimed to have “exfiltrated data” from HWL Ebsworth, another large Australian firm.



The Sydney Morning Herald

Exclusive National NSW Crime

Prominent Sydney law firm hit with cyberattack, massive data breach

Perry Duffin
March 13, 2025 — 3.58pm

A prominent Sydney law firm with close links to the NRL and A-League has been targeted by foreign cyber-attackers who are now extorting the business over hundreds of gigabytes of confidential documents.

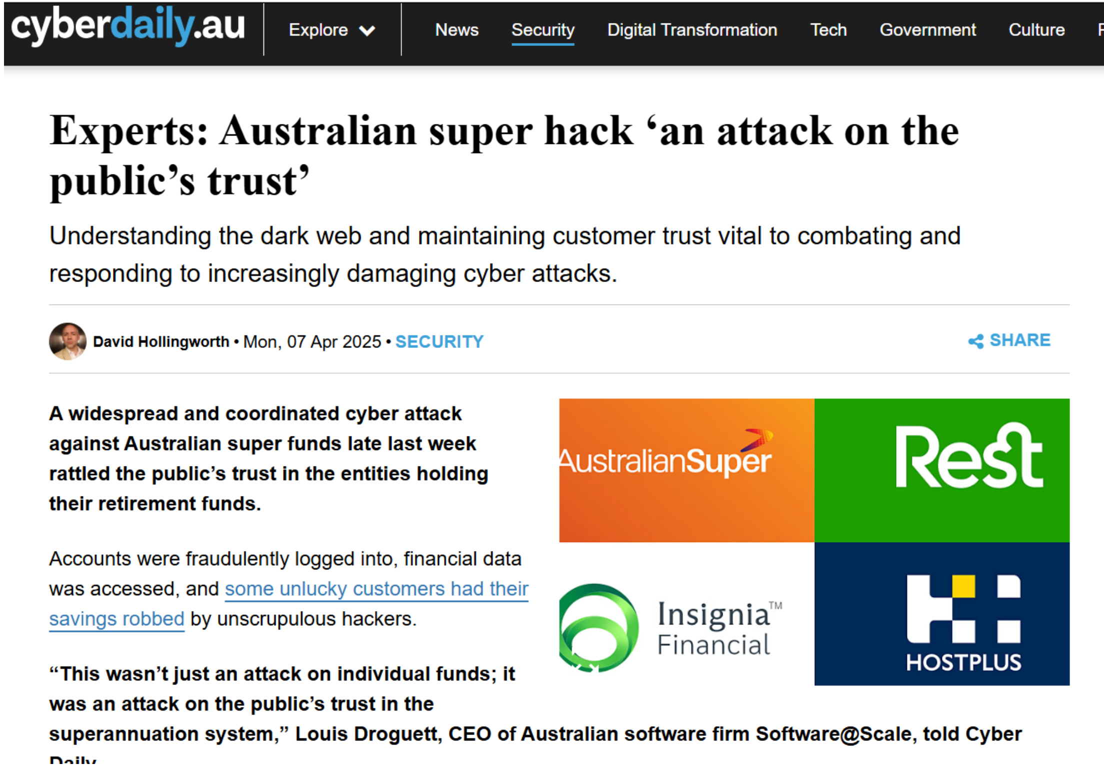
Brydens Lawyers, whose name sat on the front of Wests Tigers jersey for a decade, was hit by a cyberattack around February 20.

Brydens Lawyers is led by for sts Tigers chairman and lawyer Lee Hagipantelis. JAMES BRICKWOOD

https://www.smh.com.au/national/nsw/prominent-sydney-law-firm-hit-with-cyberattack-massive-data-breach-20250313-p5ljd8.html

Nightmares for the public

- Impacts public trust



Experts: Australian super hack 'an attack on the public's trust'

Understanding the dark web and maintaining customer trust vital to combating and responding to increasingly damaging cyber attacks.

David Hollingworth • Mon, 07 Apr 2025 • SECURITY

A widespread and coordinated cyber attack against Australian super funds late last week rattled the public's trust in the entities holding their retirement funds.

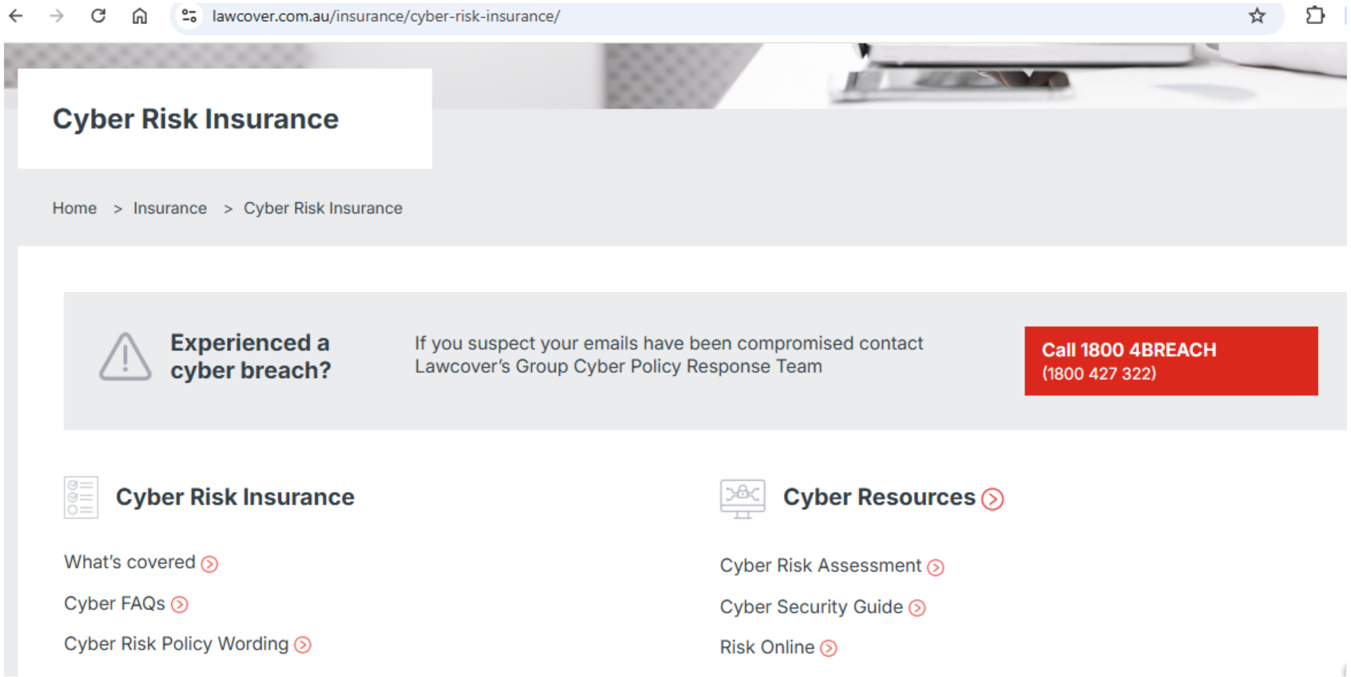
Accounts were fraudulently logged into, financial data was accessed, and some unlucky customers had their savings robbed by unscrupulous hackers.

"This wasn't just an attack on individual funds; it was an attack on the public's trust in the superannuation system," Louis Droguett, CEO of Australian software firm Software@Scale, told Cyber Daily

https://www.cyberdaily.au/security/11945-experts-australian-super-hack-an-attack-on-the-publics-trust?utm_source=CyberDaily&utm_campaign=08_04_2025&utm_medium=email&utm_content=Daily&utm_emailID=202bc2d492b8fb36486e9d49154dbbb3656c87dccaa940a87873b84dbcd4eeb3

PII - Cyber assisted fraud claims

Cyber Risk Insurance



lawcover.com.au/insurance/cyber-risk-insurance/

Cyber Risk Insurance

Home > Insurance > Cyber Risk Insurance

Experienced a cyber breach?

If you suspect your emails have been compromised contact Lawcover's Group Cyber Policy Response Team

Call 1800 4BREACH
(1800 427 322)

Cyber Risk Insurance

What's covered

Cyber FAQs

Cyber Risk Policy Wording

Cyber Resources

Cyber Risk Assessment

Cyber Security Guide

Risk Online

Lawcover Group Cyber Risk Insurance Policy

Lawcover's group cyber risk insurance policy

- Automatic cover for law practices that purchase Lawcover's PII
- Up to $50K limit
- No premium payable by law practices
- Crisis and claims assistance
- Subject to terms, conditions & exclusions of the policy wording
- A per-claim excess applies
- > 90% are caused by Business Email Compromise

Cyber claims – Lawcover Group Cyber Risk Insurance Policy

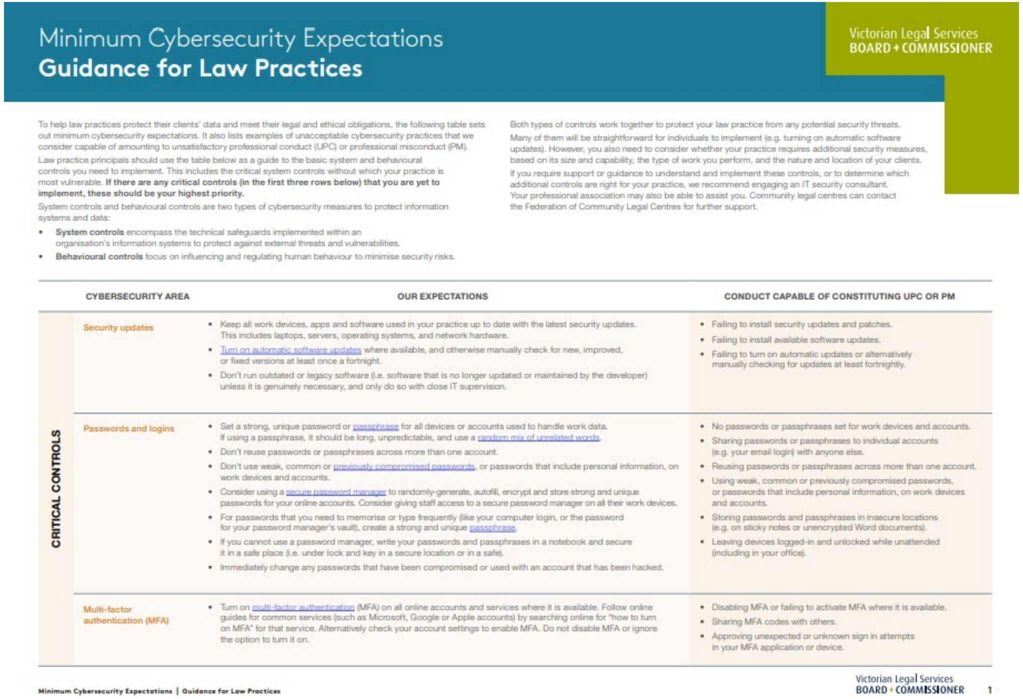
How to avoid a double excess

2024/25 Professional Indemnity Insurance Schedule

Excess:

- EXCEPT THAT **excess** means twice that amount for **claims** arising from any payment or electronic funds transfer made on an instruction or authorisation that the **law practice** did not take reasonable steps to verify.

Victorian Legal Services Board + Commissioner



Minimum Cybersecurity Expectations

Guidance for Law Practices

Victorian Legal Services
BOARD + COMMISSIONER

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

Law practice principals should use the table below as a guide to the basic system and behavioural controls you need to implement. This includes the critical system controls without which your practice is most vulnerable. **If there are any critical controls (in the first three rows below) that you are yet to implement, these should be your highest priority.**

System controls and behavioural controls are two types of cybersecurity measures to protect information systems and data:

- **System controls** encompass the technical safeguards implemented within an organisation's information systems to protect against external threats and vulnerabilities.
- **Behavioural controls** focus on influencing and regulating human behaviour to minimise security risks.

Both types of controls work together to protect your law practice from any potential security threats.

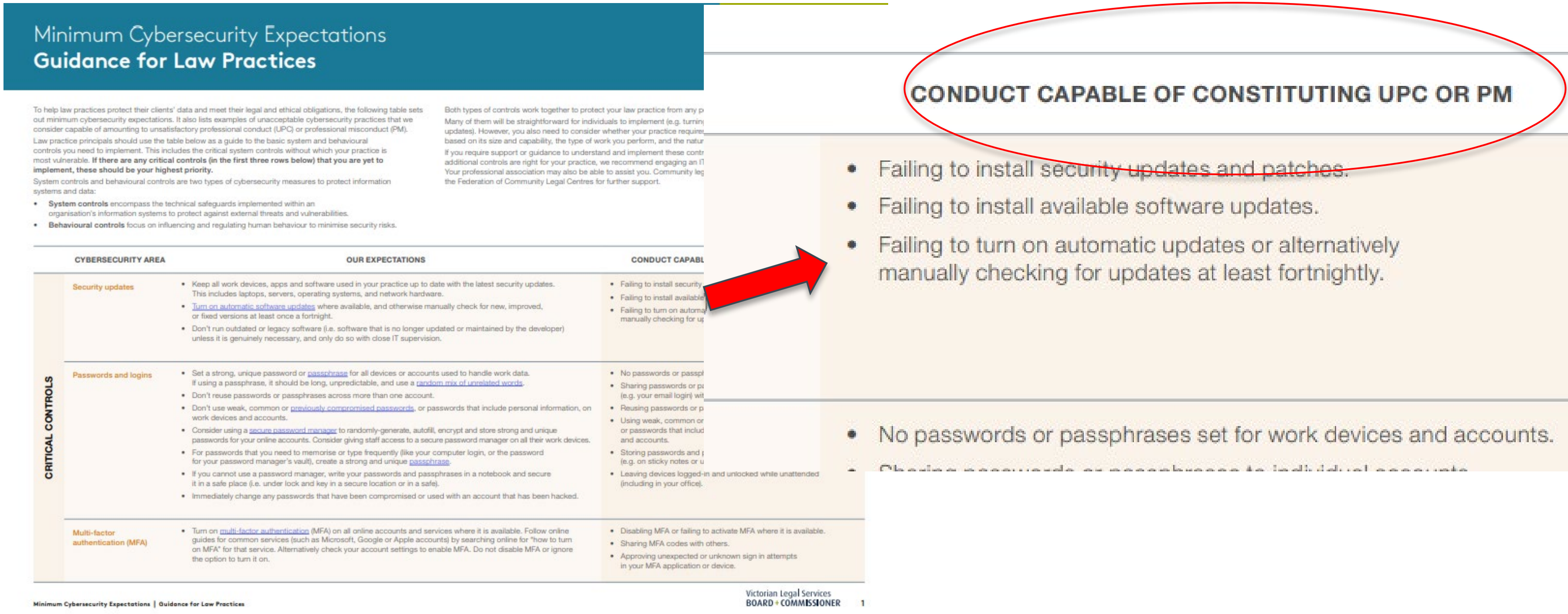
Many of them will be straightforward for individuals to implement (e.g. turning on automatic software updates). However, you also need to consider whether your practice requires additional security measures, based on its size and capability, the type of work you perform, and the nature and location of your clients.

If you require support or guidance to understand and implement these controls, or to determine which additional controls are right for your practice, we recommend engaging an IT security consultant. Your professional association may also be able to assist you. Community legal centres can contact the Federation of Community Legal Centres for further support.

	CYBERSECURITY AREA	OUR EXPECTATIONS	CONDUCT CAPABLE OF CONSTITUTING UPC OR PM
CRITICAL CONTROLS	Security updates	• 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.
	Passwords and logins	• Set a strong, unique password or passphrase for all devices or accounts used to handle work data. If using a passphrase, it should be long, unpredictable, and use a random mix of unrelated words. • Don't reuse passwords or passphrases across more than one account. • Don't use weak, common or previously compromised passwords, or passwords that include personal information, on work devices and accounts. • Consider using a secure password manager to randomly-generate, autofill, encrypt and store strong and unique passwords for your online accounts. Consider giving staff access to a secure password manager on all their work devices. • For passwords that you need to memorise or type frequently (like your computer login, or the password for your password manager's vault), create a strong and unique passphrase. • If you cannot use a password manager, write your passwords and passphrases in a notebook and secure it in a safe place (i.e. under lock and key in a secure location or in a safe). • Immediately change any passwords that have been compromised or used with an account that has been hacked.	• No passwords or passphrases set for work devices and accounts. • Sharing passwords or passphrases to individual accounts (e.g. your email login) with anyone else. • Reusing passwords or passphrases across more than one account. • Using weak, common or previously compromised passwords, or passwords that include personal information, on work devices and accounts. • Storing passwords and passphrases in insecure locations (e.g. on sticky notes or unencrypted Word documents). • Leaving devices logged-in and unlocked while unattended (including in your office).
	Multi-factor authentication (MFA)	• Turn on multi-factor authentication (MFA) on all online accounts and services where it is available. Follow online guides for common services (such as Microsoft, Google or Apple accounts) by searching online for "how to turn on MFA" for that service. Alternatively check your account settings to enable MFA. Do not disable MFA or ignore the option to turn it on.	• 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.

https://lsbc.vic.gov.au/sites/default/files/2024-02/VLSB%2BC_Minimum_Cybersecurity_Expectations.pdf

Victorian Legal Services Board + Commissioner



Minimum Cybersecurity Expectations

Guidance for Law Practices

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

Law practice principals should use the table below as a guide to the basic system and behavioural controls you need to implement. This includes the critical system controls without which your practice is most vulnerable. **If there are any critical controls (in the first three rows below) that you are yet to implement, these should be your highest priority.**

System controls and behavioural controls are two types of cybersecurity measures to protect information systems and data:

- **System controls** encompass the technical safeguards implemented within an organisation's information systems to protect against external threats and vulnerabilities.
- **Behavioural controls** focus on influencing and regulating human behaviour to minimise security risks.

Both types of controls work together to protect your law practice from any p

Many of them will be straightforward for individuals to implement (e.g. turnin updates). However, you also need to consider whether your practice require based on its size and capability, the type of work you perform, and the natur

If you require support or guidance to understand and implement these contr additional controls are right for your practice, we recommend engaging an IT Your professional association may also be able to assist you. Community leg the Federation of Community Legal Centres for further support.

	CYBERSECURITY AREA	OUR EXPECTATIONS	CONDUCT CAPABL
CRITICAL CONTROLS	Security updates	• 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 • Failing to install available • Failing to turn on automa manually checking for u
	Passwords and logins	• Set a strong, unique password or passphrase for all devices or accounts used to handle work data. If using a passphrase, it should be long, unpredictable, and use a random mix of unrelated words. • Don't reuse passwords or passphrases across more than one account. • Don't use weak, common or previously compromised passwords, or passwords that include personal information, on work devices and accounts. • Consider using a secure password manager to randomly-generate, autofill, encrypt and store strong and unique passwords for your online accounts. Consider giving staff access to a secure password manager on all their work devices. • For passwords that you need to memorise or type frequently (like your computer login, or the password for your password manager's vault), create a strong and unique passphrase. • If you cannot use a password manager, write your passwords and passphrases in a notebook and secure it in a safe place (i.e. under lock and key in a secure location or in a safe). • Immediately change any passwords that have been compromised or used with an account that has been hacked.	• No passwords or passp • Sharing passwords or p (e.g. your email login) wi • Reusing passwords or p • Using weak, common or or passwords that includ and accounts. • Storing passwords and (e.g. on sticky notes or u • Leaving devices logged-in and unlocked while unattended (including in your office).
	Multi-factor authentication (MFA)	• Turn on multi-factor authentication (MFA) on all online accounts and services where it is available. Follow online guides for common services (such as Microsoft, Google or Apple accounts) by searching online for "how to turn on MFA" for that service. Alternatively check your account settings to enable MFA. Do not disable MFA or ignore the option to turn it on.	• 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.

Minimum Cybersecurity Expectations | Guidance for Law Practices

Victorian Legal Services
BOARD + COMMISSIONER 1

CONDUCT CAPABLE OF CONSTITUTING UPC OR PM

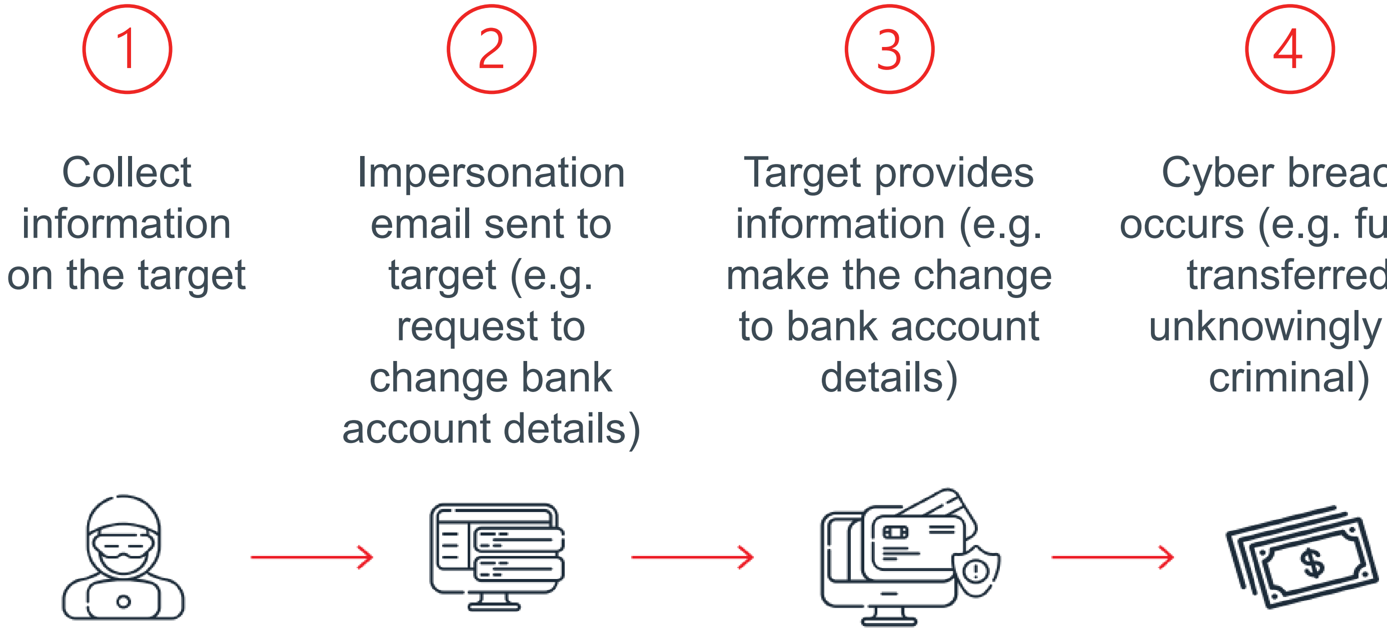
- Failing to install security updates and patches.
- Failing to install available software updates.
- Failing to turn on automatic updates or alternatively manually checking for updates at least fortnightly.

- No passwords or passphrases set for work devices and accounts.
- Sharing passwords or passphrases to individual accounts

https://lsbc.vic.gov.au/sites/default/files/2024-02/VLSB%2BC_Minimum_Cybersecurity_Expectations.pdf

Business Email Compromise

What is it and how does it work?



1. Collect information on the target

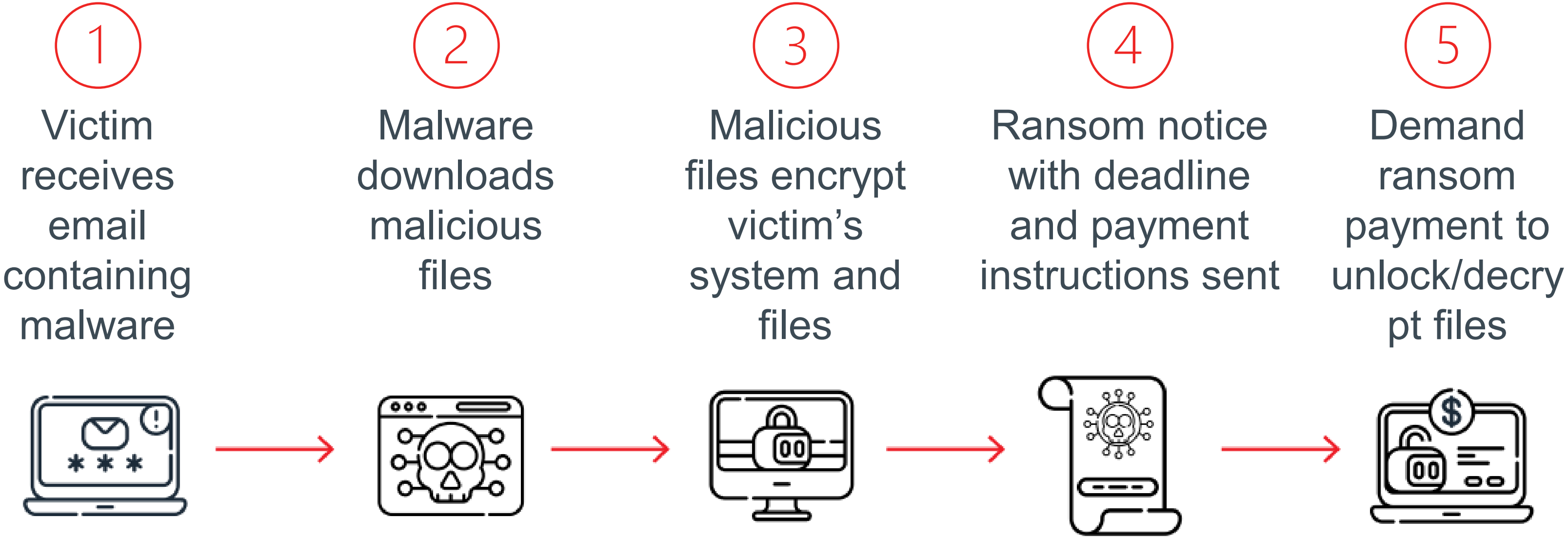
2. Impersonation email sent to target (e.g. request to change bank account details)

3. Target provides information (e.g. make the change to bank account details)

4. Cyber breach occurs (e.g. funds transferred unknowingly to criminal)

Ransomware

What is it and how does it work?



1. Victim receives email containing malware
2. Malware downloads malicious files
3. Malicious files encrypt victim’s system and files
4. Ransom notice with deadline and payment instructions sent
5. Demand ransom payment to unlock/decrypt files

Business Email Compromise and Ransomware - Causes

1 Weak passwords

- Use of the same password for different accounts
- Use of a password that is easily guessed (e.g. birth dates)
- Passwords recorded in a notebook
- Use of a variation of the same password for different accounts

2 Malicious links and attachments

- Decision and skill-based errors, (e.g. opening malicious email or attachments or clicking a malicious link)
- Lack of or inadequate protective software to block malicious emails
- Lack of staff training and awareness of cyber security and threats

Business Email Compromise and Ransomware - Causes

3

Risks with WiFi and USB drives

- Use of WiFi available in public places
- Use of portable storage devices that are not your own or are unprotected
- Failure to protect your own portable storage devices

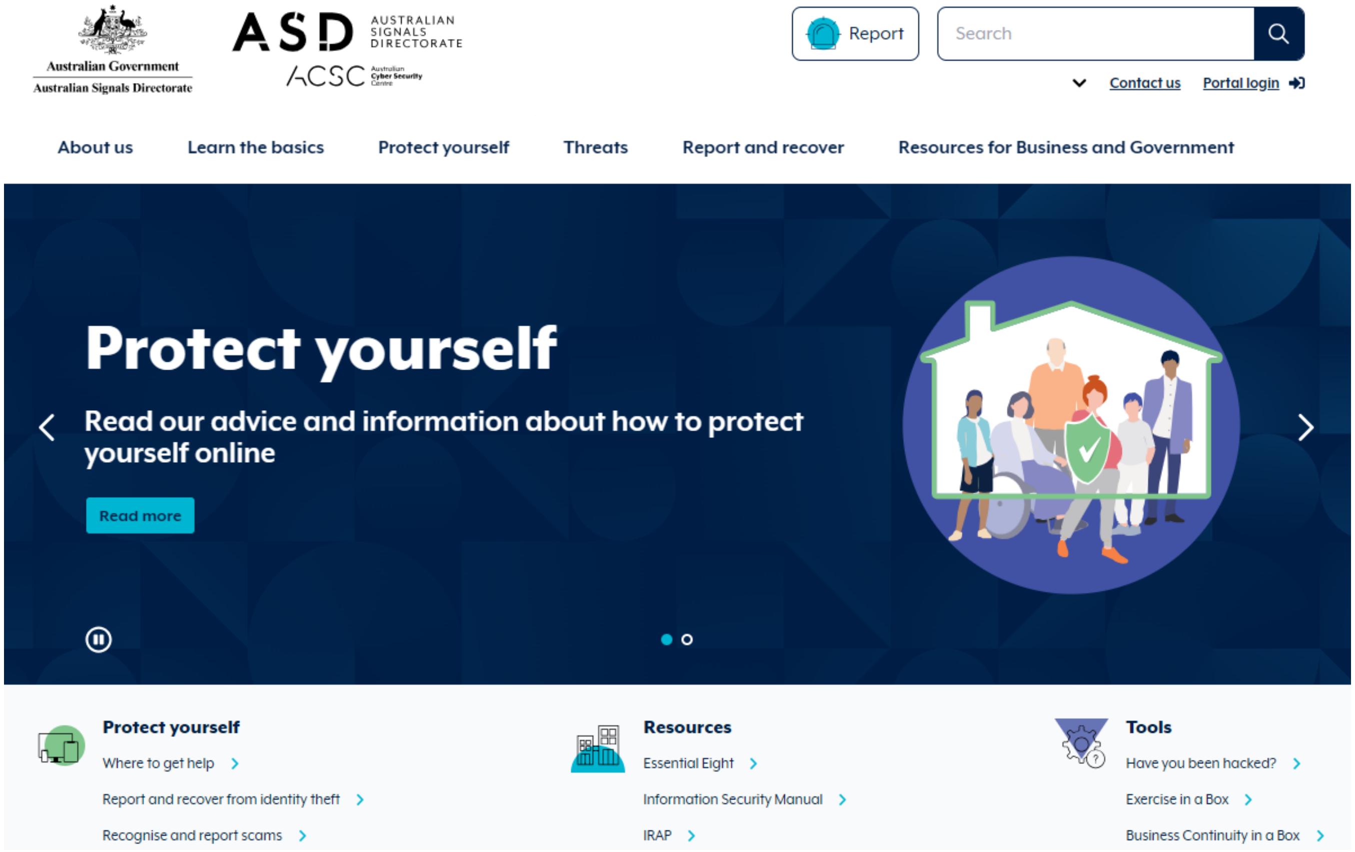
4

Poor protection software and data backups

- Little or no protection software to safeguard your system
- Disabled software protection alerts
- Failure to perform updates when alerted
- Failure to perform frequent data backups
- Failure to check efficacy of data backups

Lawcover

cyber.gov.au



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

Report

Search

Contact us Portal login

About us · Learn the basics · Protect yourself · Threats · Report and recover · Resources for Business and Government

Protect yourself

Read our advice and information about how to protect yourself online

Read more

Protect yourself

- Where to get help
- Report and recover from identity theft
- Recognise and report scams

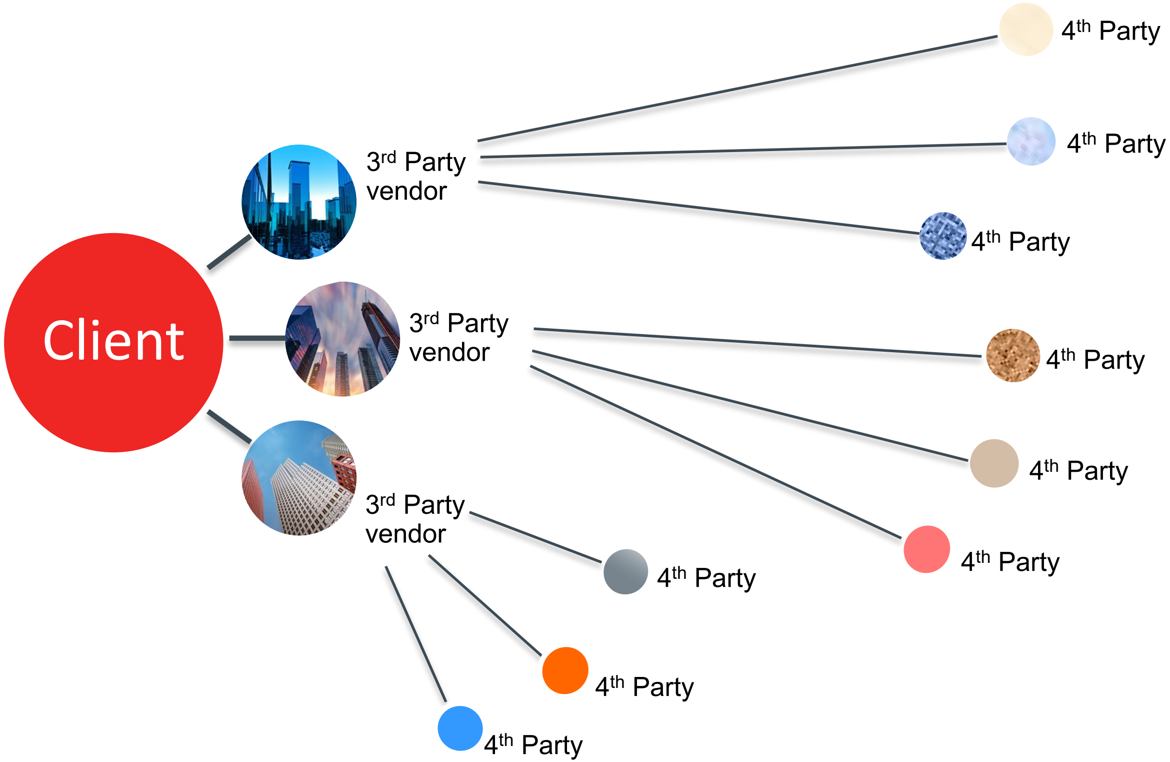
Resources

- Essential Eight
- Information Security Manual
- IRAP

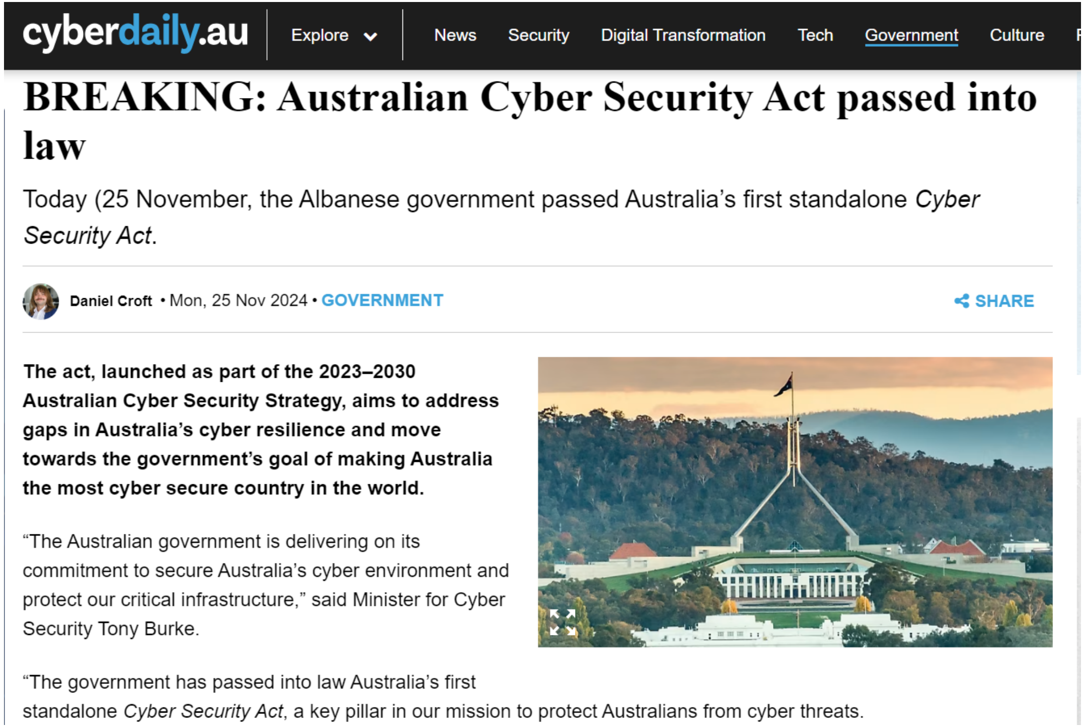
Tools

- Have you been hacked?
- Exercise in a Box
- Business Continuity in a Box

Supply chain risk – fourth party risk



Australian Cyber Security Act



BREAKING: Australian Cyber Security Act passed into law

Today (25 November, the Albanese government passed Australia's first standalone *Cyber Security Act*.

Daniel Croft • Mon, 25 Nov 2024 • GOVERNMENT

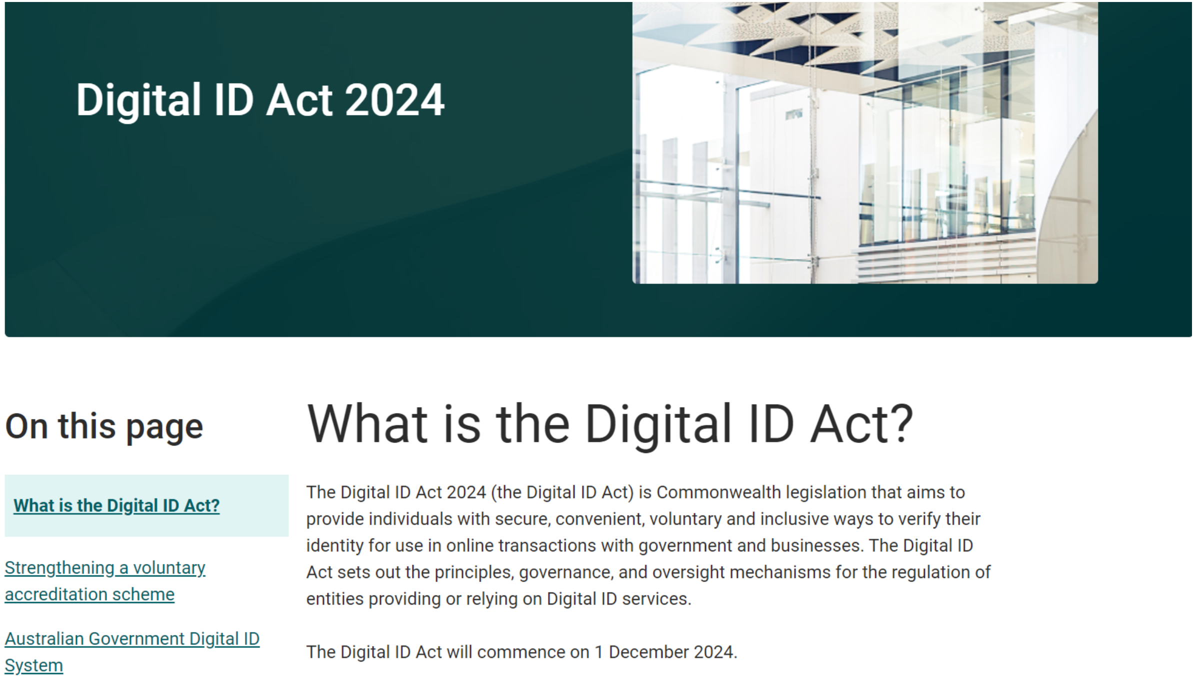
The act, launched as part of the 2023–2030 Australian Cyber Security Strategy, aims to address gaps in Australia's cyber resilience and move towards the government's goal of making Australia the most cyber secure country in the world.

"The Australian government is delivering on its commitment to secure Australia's cyber environment and protect our critical infrastructure," said Minister for Cyber Security Tony Burke.

"The government has passed into law Australia's first standalone *Cyber Security Act*, a key pillar in our mission to protect Australians from cyber threats.

BREAKING: Australian Cyber Security Act passed into law - Cyber Daily

Digital ID Act 2024



Digital ID Act 2024

On this page

- [What is the Digital ID Act?]
- Strengthening a voluntary accreditation scheme
- Australian Government Digital ID System

What is the Digital ID Act?

The Digital ID Act 2024 (the Digital ID Act) is Commonwealth legislation that aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses. The Digital ID Act sets out the principles, governance, and oversight mechanisms for the regulation of entities providing or relying on Digital ID services.

The Digital ID Act will commence on 1 December 2024.

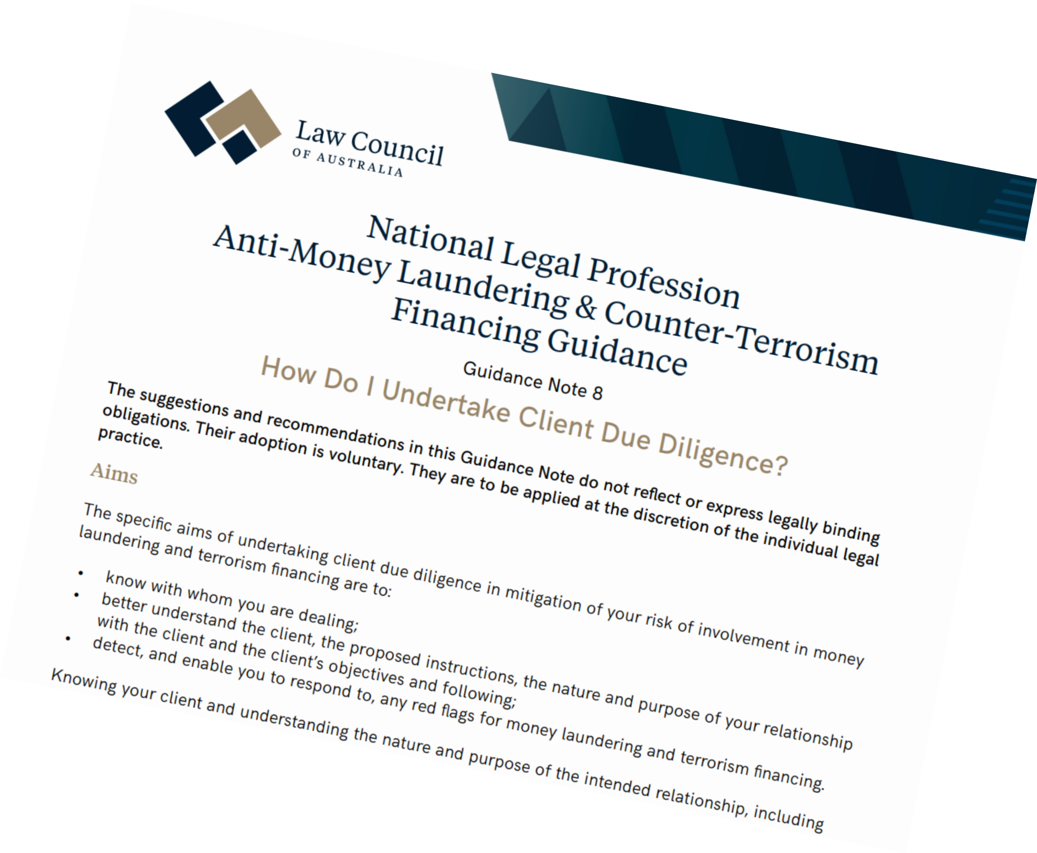
https://www.Digital ID Act 2024 | Digital ID System

AML/CTF changes

Extract from The Law Council of Australia

National Legal Profession Anti-Money Laundering & Counter-Terrorism Financing Guidance

28 June 2024



Law Council OF AUSTRALIA

National Legal Profession Anti-Money Laundering & Counter-Terrorism Financing Guidance

Guidance Note 8

How Do I Undertake Client Due Diligence?

The suggestions and recommendations in this Guidance Note do not reflect or express legally binding obligations. Their adoption is voluntary. They are to be applied at the discretion of the individual legal practice.

Aims

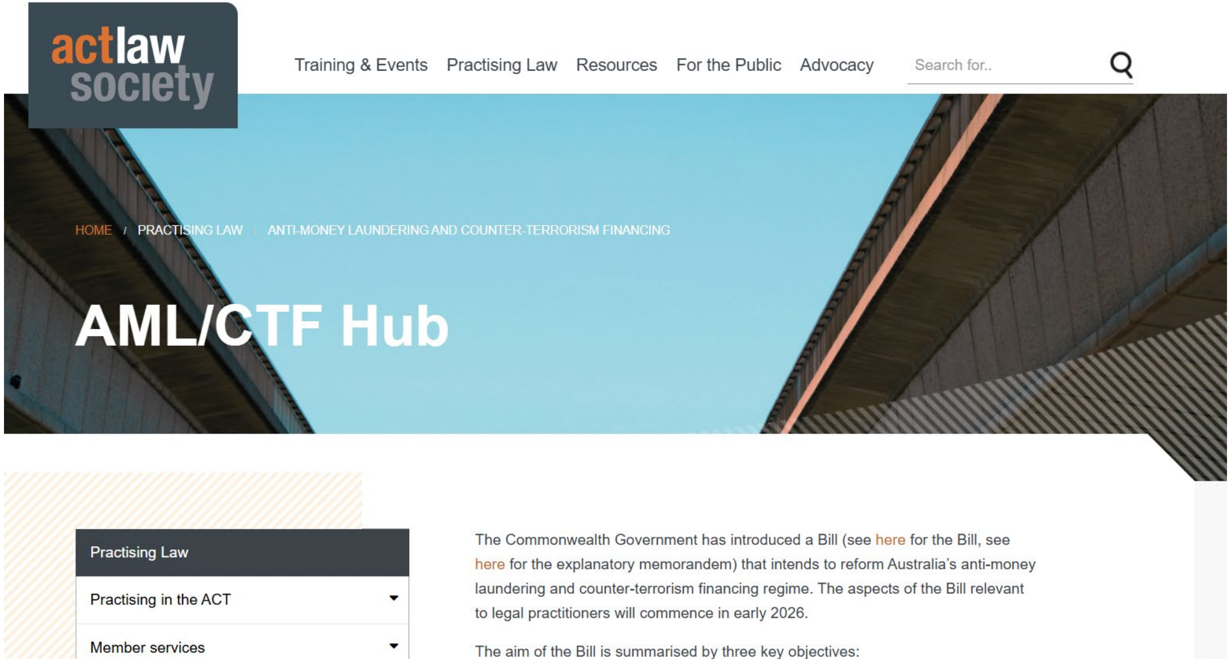
The specific aims of undertaking client due diligence in mitigation of your risk of involvement in money laundering and terrorism financing are to:

- know with whom you are dealing;
- better understand the client, the proposed instructions, the nature and purpose of your relationship with the client and the client's objectives and following;
- detect, and enable you to respond to, any red flags for money laundering and terrorism financing.

Knowing your client and understanding the nature and purpose of the intended relationship, including

https://lawcouncil.au/resources/policies-and-guidelines/national-legal-profession-anti-money-laundering---counter-terrorism-financing-guidance

ACT Law Society - AML/CTF HUB



HOME / PRACTISING LAW / ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING

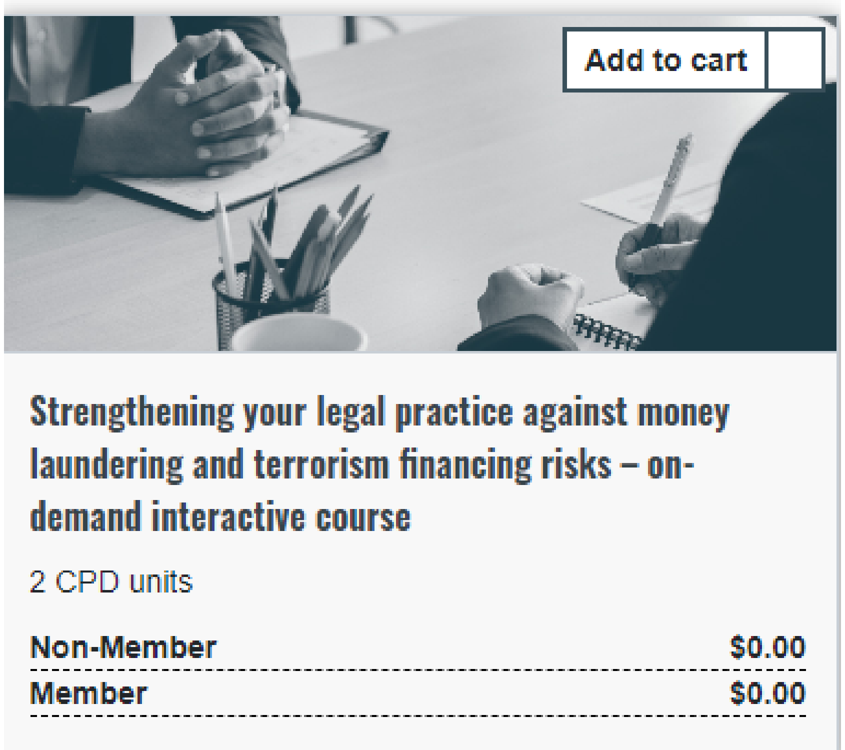
AML/CTF Hub

The Commonwealth Government has introduced a Bill (see here for the Bill, see here for the explanatory memorandem) that intends to reform Australia's anti-money laundering and counter-terrorism financing regime. The aspects of the Bill relevant to legal practitioners will commence in early 2026.

The aim of the Bill is summarised by three key objectives:

https://actlawsociety.asn.au/practising-law/aml-ctf

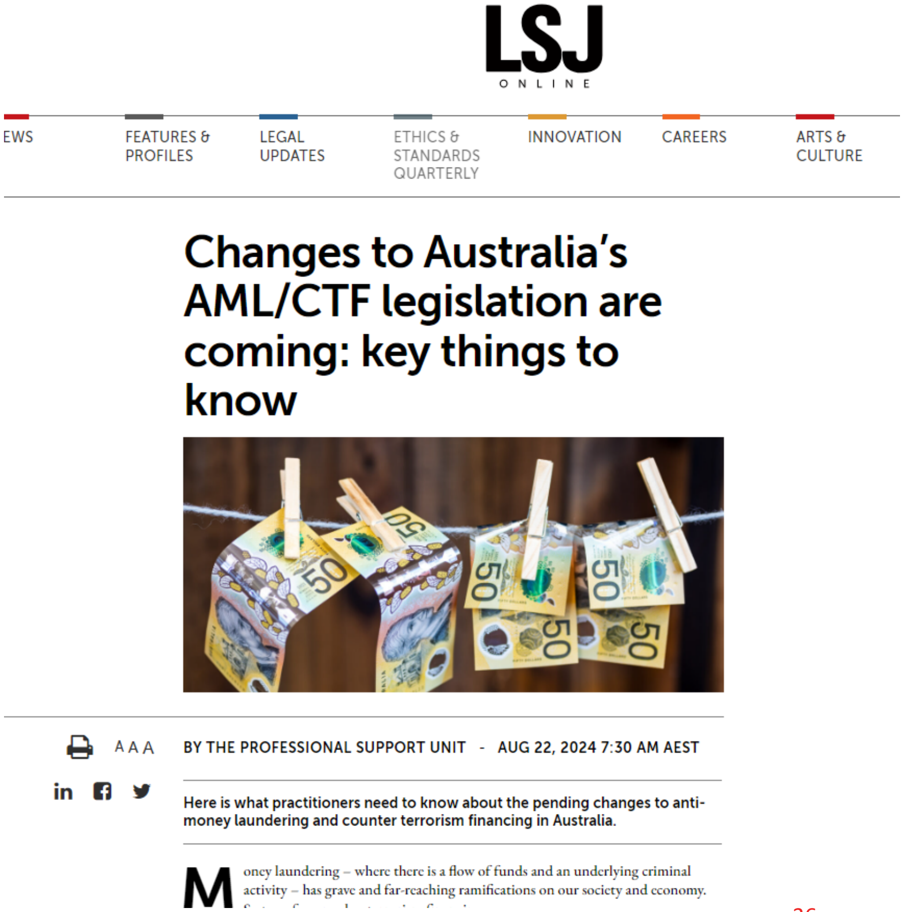
LSNSW Resources



Strengthening your legal practice against money laundering and terrorism financing risks – on-demand interactive course

2 CPD units

Non-Member	$0.00
Member	$0.00



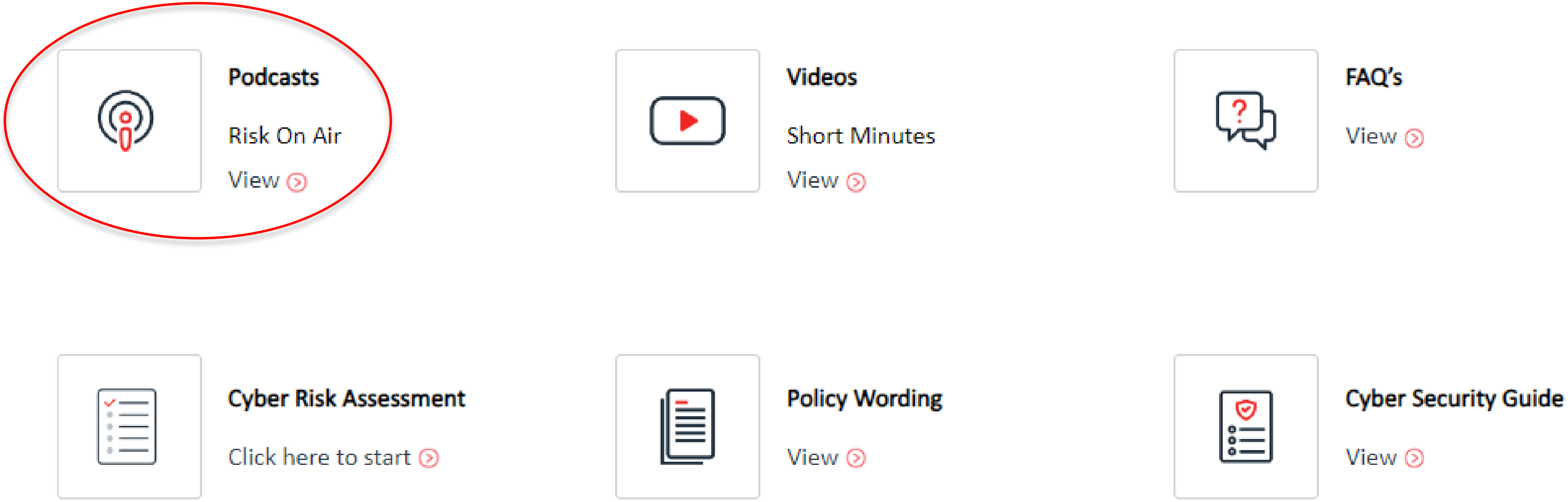
Changes to Australia's AML/CTF legislation are coming: key things to know

BY THE PROFESSIONAL SUPPORT UNIT - AUG 22, 2024 7:30 AM AEST

Here is what practitioners need to know about the pending changes to anti-money laundering and counter terrorism financing in Australia.

Money laundering – where there is a flow of funds and an underlying criminal activity – has grave and far-reaching ramifications on our society and economy.

Lawcover's Cyber Resources



Podcasts

Risk On Air

View

Videos

Short Minutes

View

FAQ's

View

Cyber Risk Assessment

Click here to start

Policy Wording

View

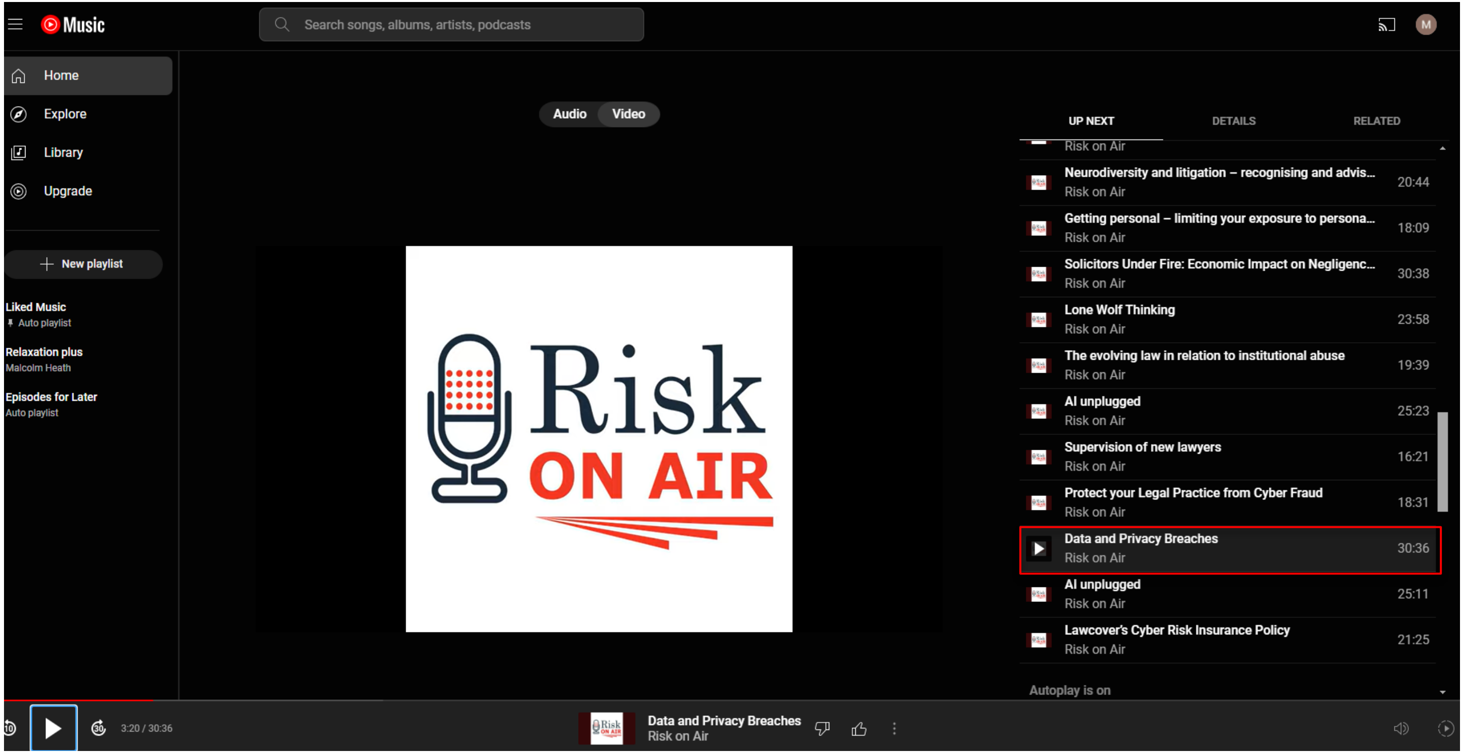
Cyber Security Guide

View

Lawcover

lawcover.com.au/cyber-resources/

Lawcover’s Cyber Resources



	Risk on Air	
Neurodiversity and litigation – recognising and advis...	Risk on Air	20:44
Getting personal – limiting your exposure to persona...	Risk on Air	18:09
Solicitors Under Fire: Economic Impact on Negligenc...	Risk on Air	30:38
Lone Wolf Thinking	Risk on Air	23:58
The evolving law in relation to institutional abuse	Risk on Air	19:39
AI unplugged	Risk on Air	25:23
Supervision of new lawyers	Risk on Air	16:21
Protect your Legal Practice from Cyber Fraud	Risk on Air	18:31
Data and Privacy Breaches	Risk on Air	30:36
AI unplugged	Risk on Air	25:11
Lawcover's Cyber Risk Insurance Policy	Risk on Air	21:25

Autoplay is on

Data and Privacy Breaches
Risk on Air

lawcover.com.au/cyber-resources/

Lawcover’s Guide to Cyber Security

Designed to help legal practices navigate the world of cyber security; identify and prioritise their security needs and implement effective defense systems, ongoing protection and appropriate response plans in their own practice.

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.

lawcover.com.au

lawcover.com.au/cyber-security-guide

Lawcover's Guide to Cyber Security

Supplementary materials with step-by-step instructions to help protect critical aspects of your practice.

Data

Passwords

Email and messaging

Mobile device

Hardware

lawcover.com.au/cyber-security-guide

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

CYBER SECURITY SNAPSHOTS

Useful reminders and tips for the whole practice.

Protect your DATA

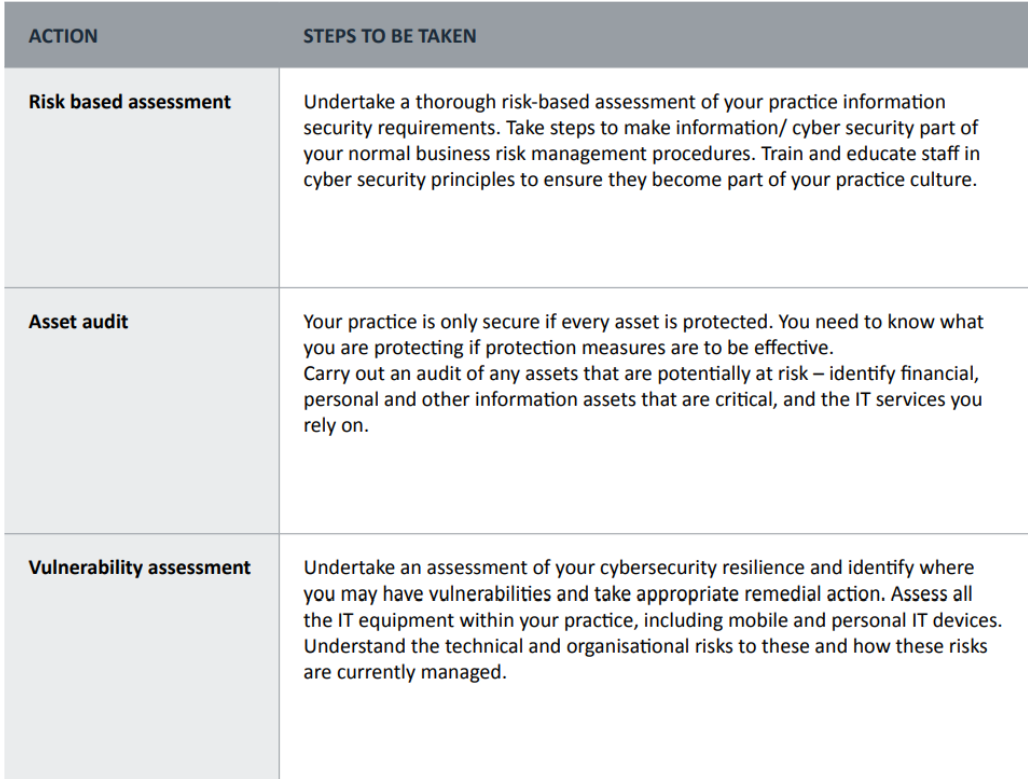
Protect your HARDWARE

Protect your PASSWORDS

Protect your EMAIL, CHAT APPS, MESSAGING AND SOCIAL MEDIA

Protect your MOBILE DEVICE

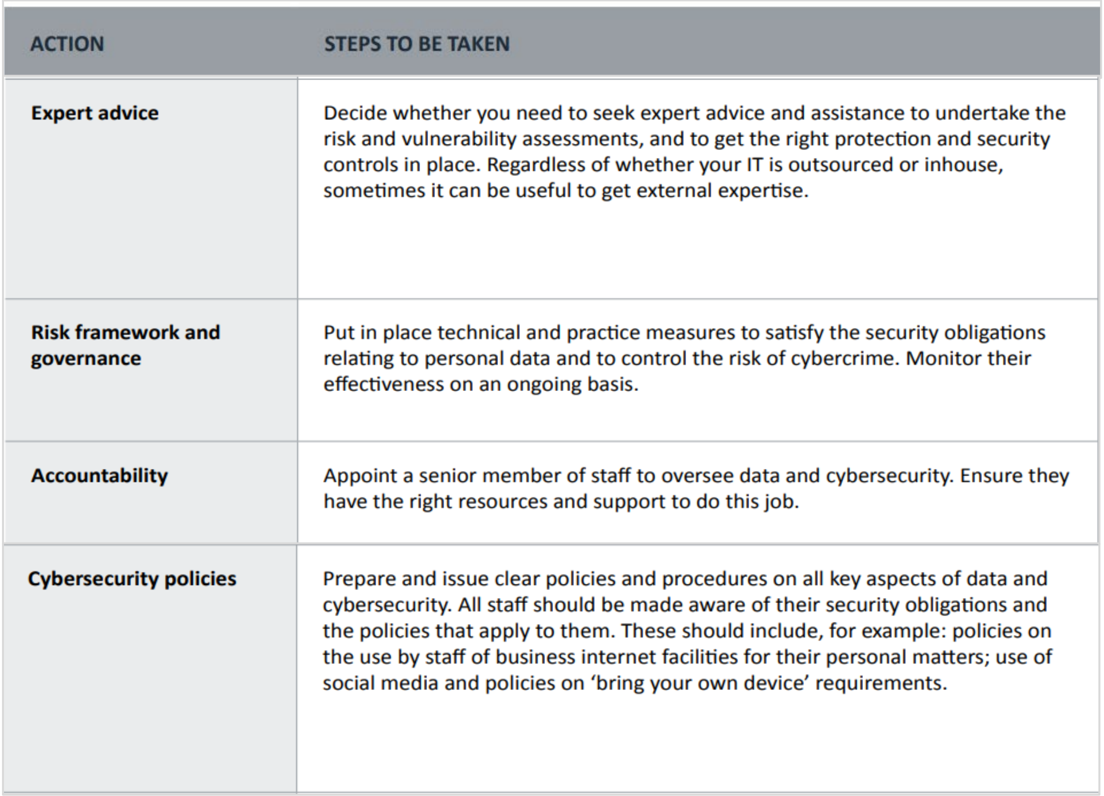
Cyber security response plan and tips



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 cybersecurity 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.

https://www.lawcover.com.au/wp-content/uploads/2022/09/Guide-to-Cyber-Security.pdf

Cyber security response plan and tips

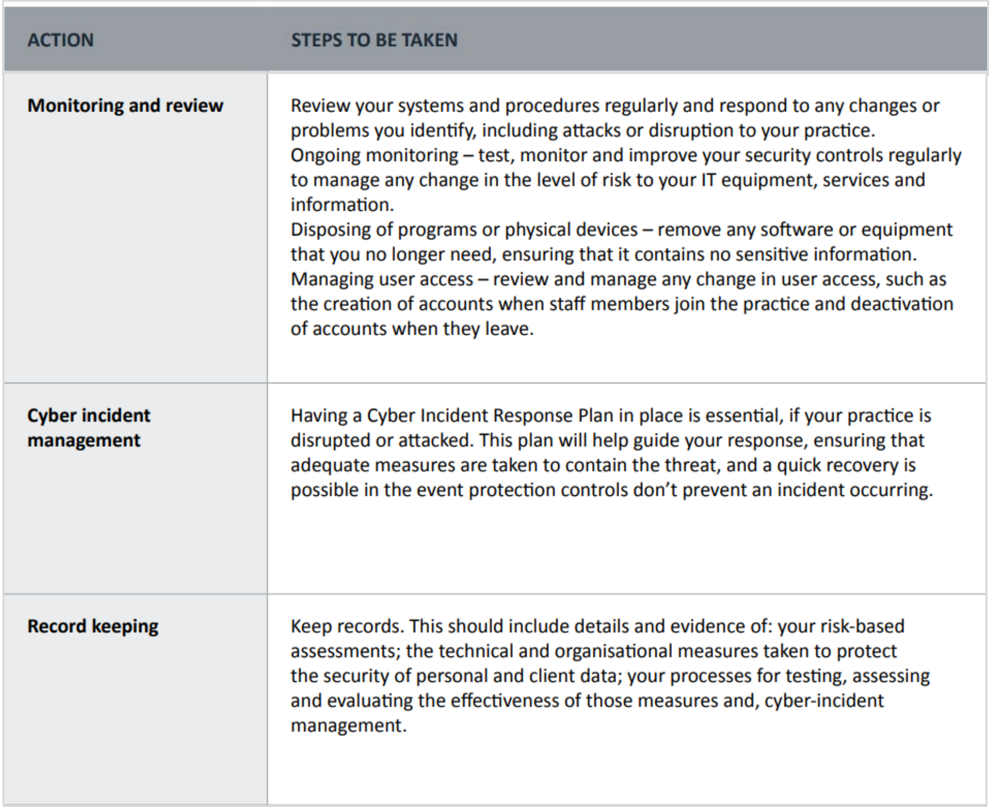


ACTION	STEPS TO BE TAKEN
Expert advice	Decide whether you need to seek expert advice and assistance to undertake the risk and vulnerability assessments, and to get the right protection and security controls in place. Regardless of whether your IT is outsourced or inhouse, sometimes it can be useful to 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 cybersecurity. Ensure they have the right resources and support to do this job.
Cybersecurity policies	Prepare and issue clear policies and procedures on all key aspects of data and cybersecurity. All staff should be made aware of their security obligations and the policies that apply to them. These should include, for example: policies on the use by staff of business internet facilities for their personal matters; use of social media and policies on 'bring your own device' requirements.

Lawcover

https://www.lawcover.com.au/wp-content/uploads/2022/09/Guide-to-Cyber-Security.pdf

Cyber security response plan and tips



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.

Lawcover

https://www.lawcover.com.au/wp-content/uploads/2022/09/Guide-to-Cyber-Security.pdf

Cyber Security

Malcolm Heath, Practice Risk Manager

Lawcover™