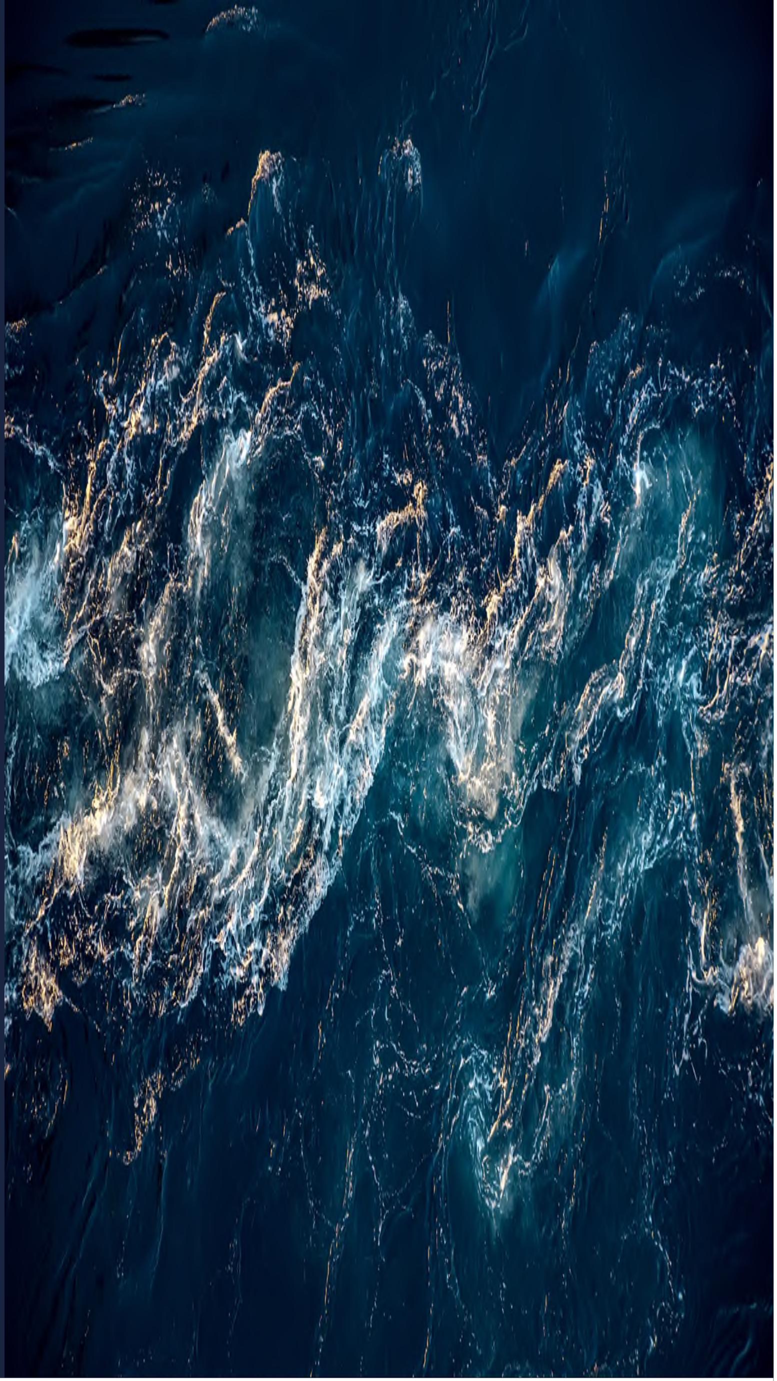
WIN In-House Counsel Week 2024

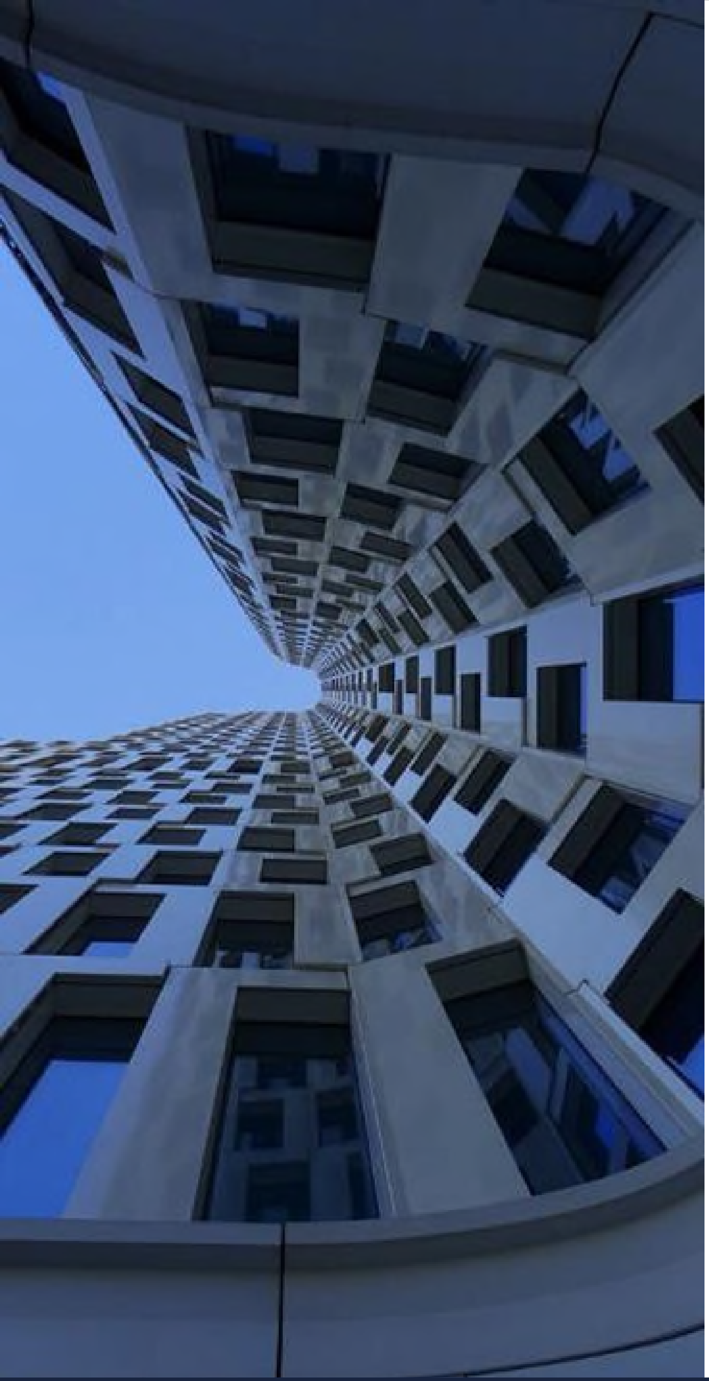
Insights from the trenches: top tips for managing (and avoiding) cyber incidents

Presenters: Sarah Birkett and William Kwan



DLA PIPER

WIN what in-house lawyers need



Introduction

- Cyber security is a key priority for Australian businesses and regulators in 2024
- The DLA Piper team has a wide breadth of experience managing cybersecurity incidents, collectively managing over 2,000 incidents worldwide across numerous industries
- In the course of our incident responses, we've gathered important insights for organisations' impacted by a data breach
- These lessons will help facilitate efficient and effective incident response from beginning to end, as well as provide useful tips for managing cyber resilience

Current threat levels

94,000 reports of cyber-crime

- Via Report-Cyber in FY 22-23
- Nearly 1 every 6 minutes
- Up 23% from the previous year

Source: *ASD Cyber Threat Report 2022-2023*

1 in 5 critical vulnerabilities exploited within 48 hours

- Despite patching or mitigation advice being available

Source: *ASD Cyber Threat Report 2022-2023*

Average cost of a data breach is USD 4.45m

- Global average
- 15% increase over 3 years

Source: *IBM Cost of a Data Breach Report, 2023*

469 notifiable data breaches

- In the six-month period from January – June 2023

Source: *OAIC's Notifiable Data Breaches Report: January to June 2023*

Health and finance are top reporting sectors

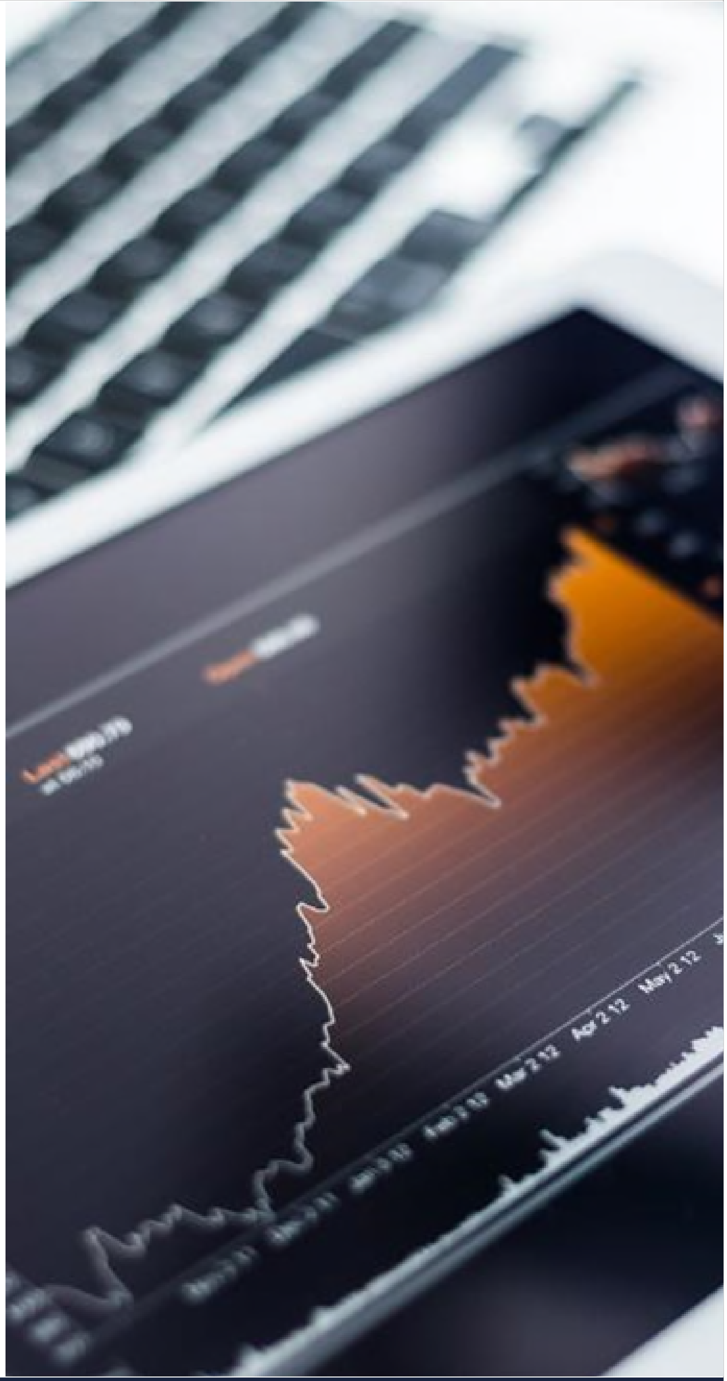
- For notifiable data breaches
- Followed by recruitment; legal, accounting and management, and insurance

Source: *OAIC's Notifiable Data Breaches Report: January to June 2023*

Average cyber maturity score of 1.66 (on a scale of 0 – 4)

- Weighted average of 697 participants in ASIC's cyber pulse survey
- Many organisations reactive, not proactive

Source: *ASIC Spotlight on Cyber: Findings and insights from the cyber pulse survey 2023, November 2023*



Lessons Learned

1. 80% of what you think in the first week probably isn't true

- Don't make bold assertions you might later need to walk back, and be candid about your ongoing commitment to finding out and sharing facts

- Be nimble about adjusting your playbook as facts change

- Where you have discretion, consider the timing of notifications (although that may not be possible following implementation of the Privacy Act Review)

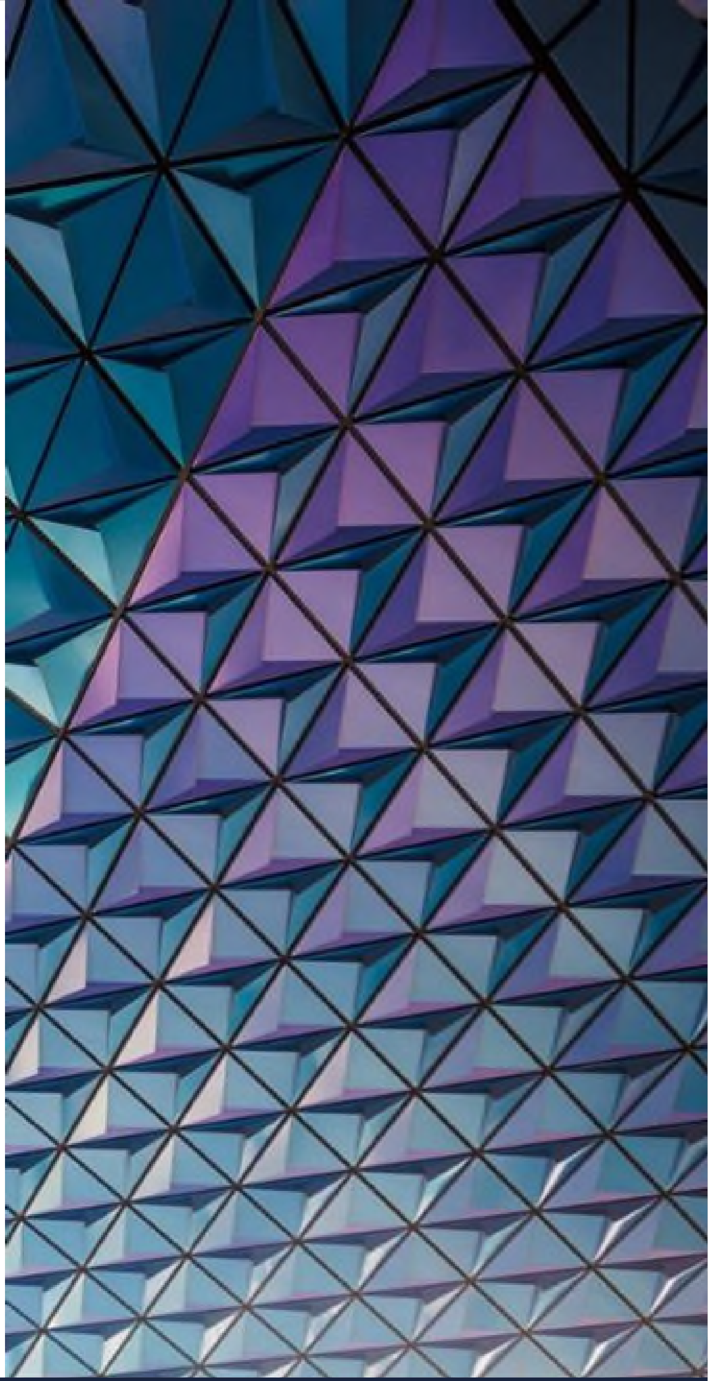
> *Only the wisest and stupidest of men never change*
>
> **-- Confucius**

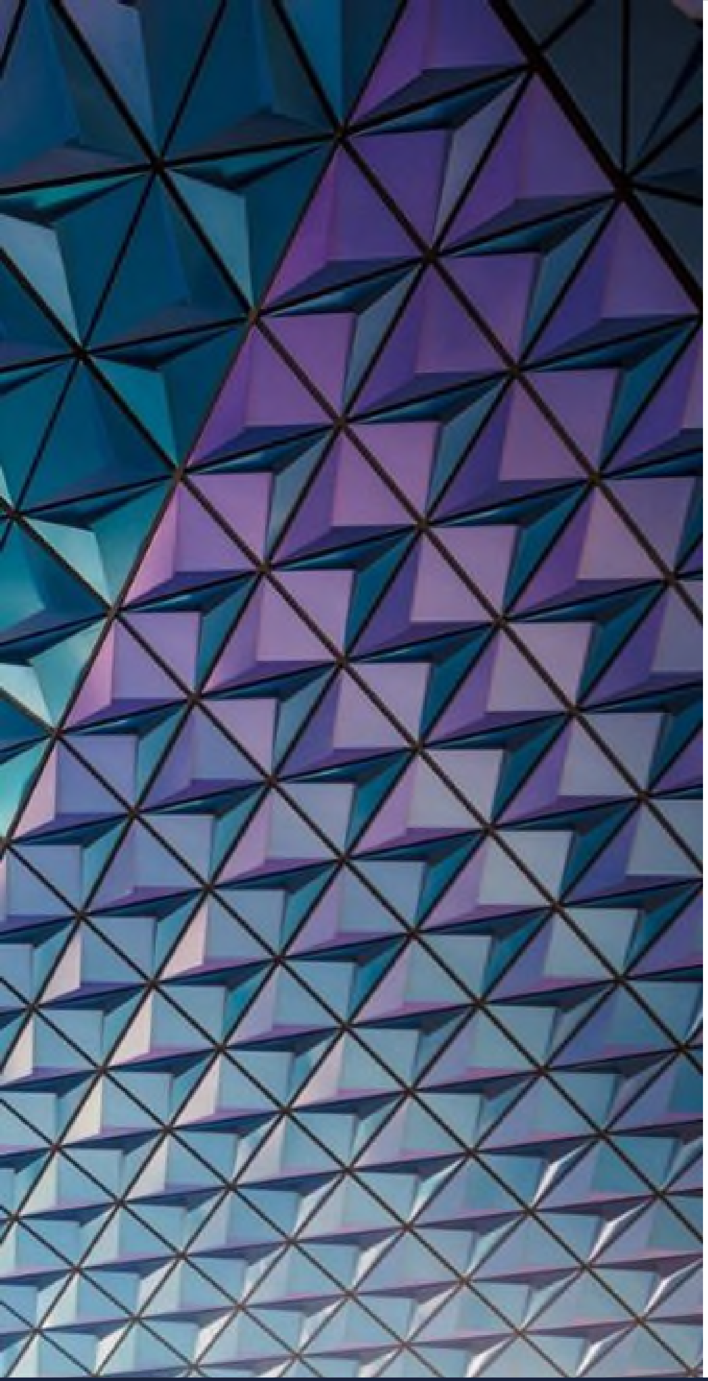
2. You must make the facts stand still

- Getting factual clarity about what happened is critical to good decision making, communications, and managing legal and regulatory risk

- Maintain a single source of truth

- Make it happen as quickly as you can





3. A rock and a hard place

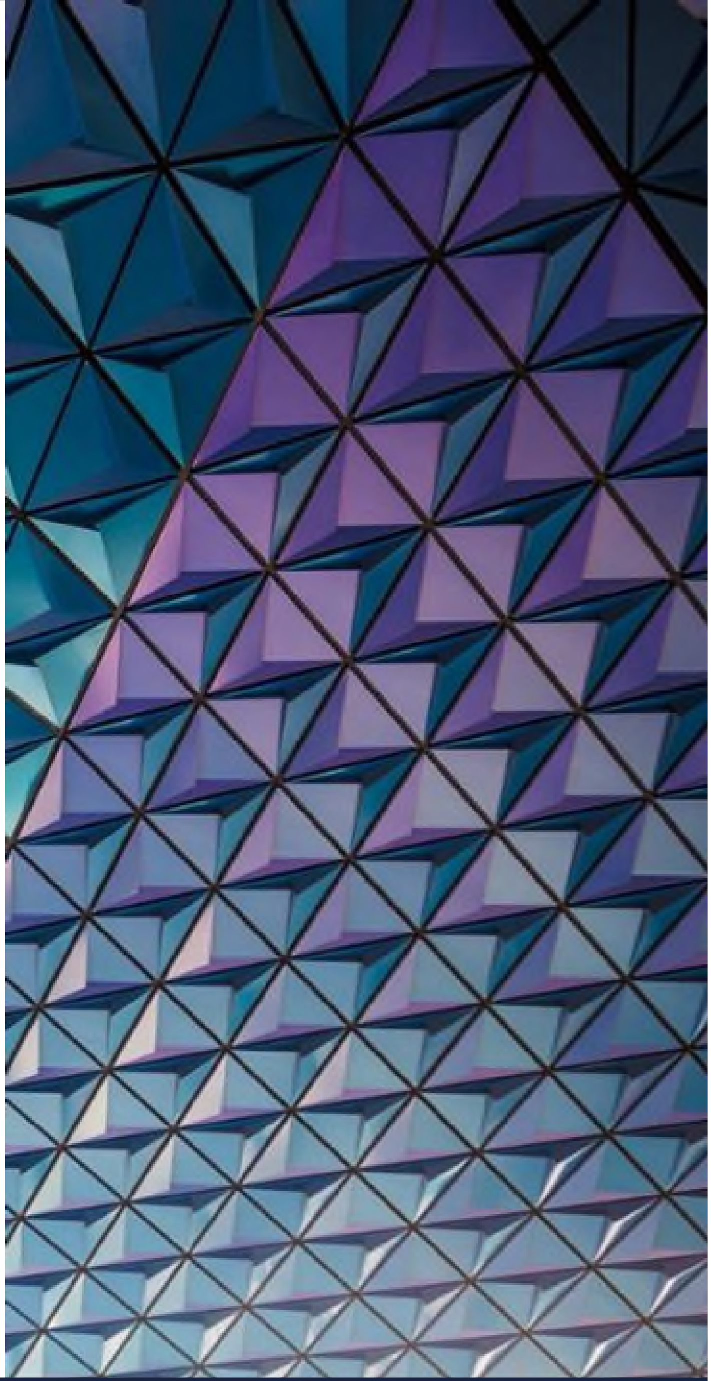
- A lot of choices are between two bad options, and the aim is to choose the "least bad" option

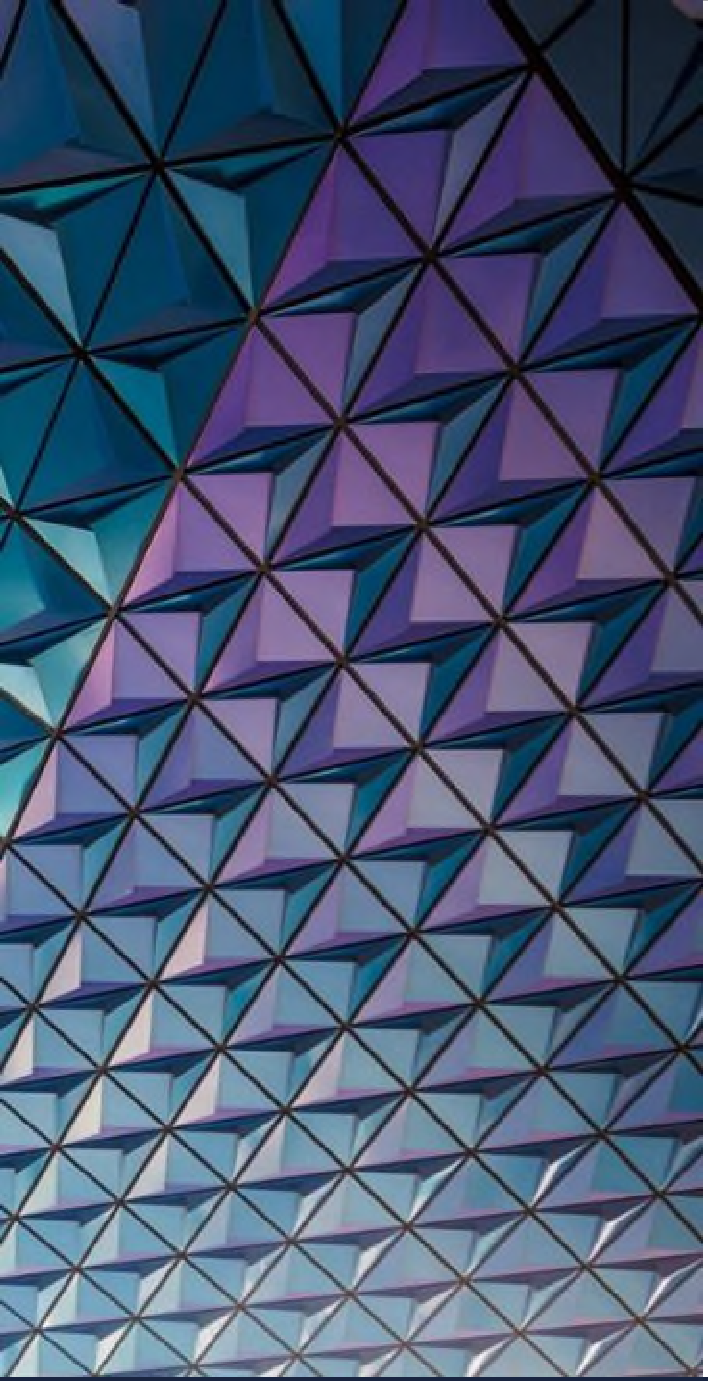
- There isn't always a right answer – and this can be frustrating (especially for lawyers)

- As with all complex decisions, best approach is to be armed with as much information as possible (and that's where having clarity over the facts can help)

4. You can’t properly investigate or assess risk until you contain

- Develop clear workstreams – containment, remediation, investigation etc
- Fix before you get too caught up in extent of damage, or the “who done it,” which you just don't and can't know immediately
- Workstreams operate in parallel, but focus will change as incident progresses





5. Frontload resiliency and continuity issues – but don’t shoot yourselves in the foot

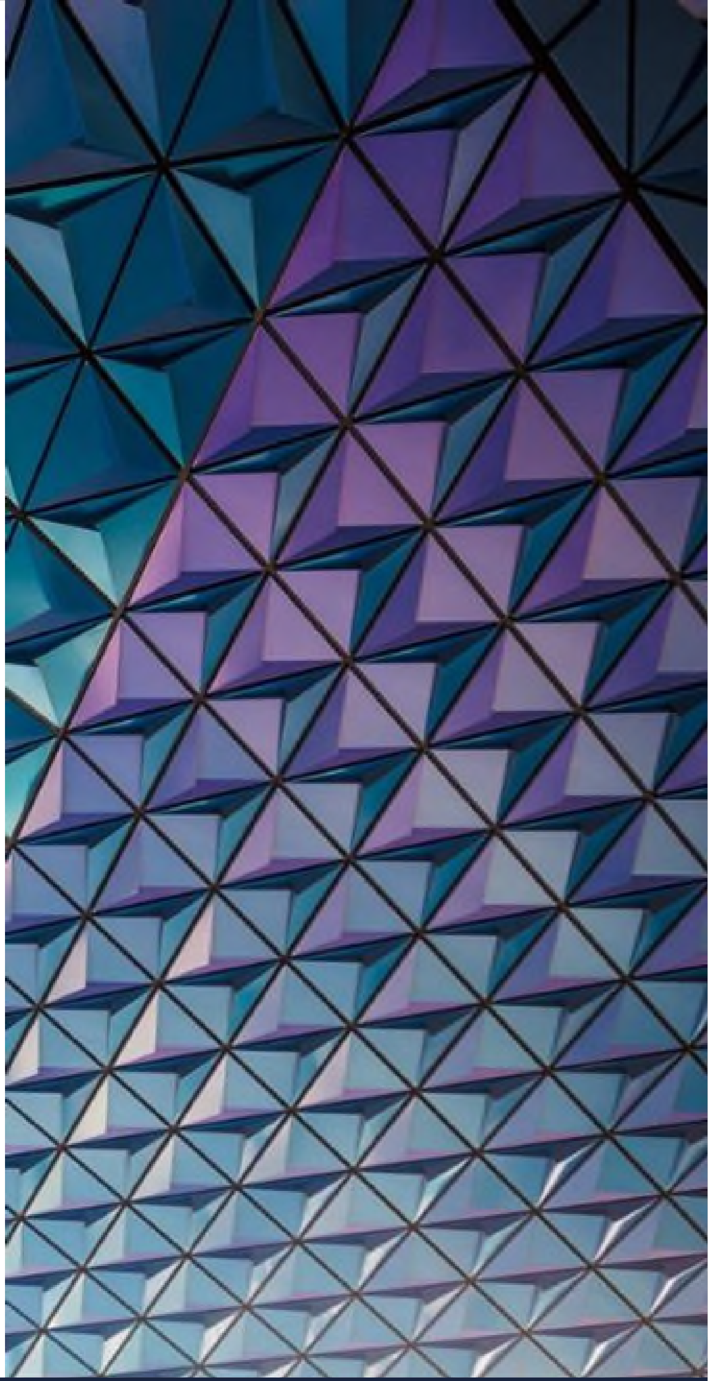
- While focus is on remediation and containment, legal issues are usually backloaded – but should not be forgotten

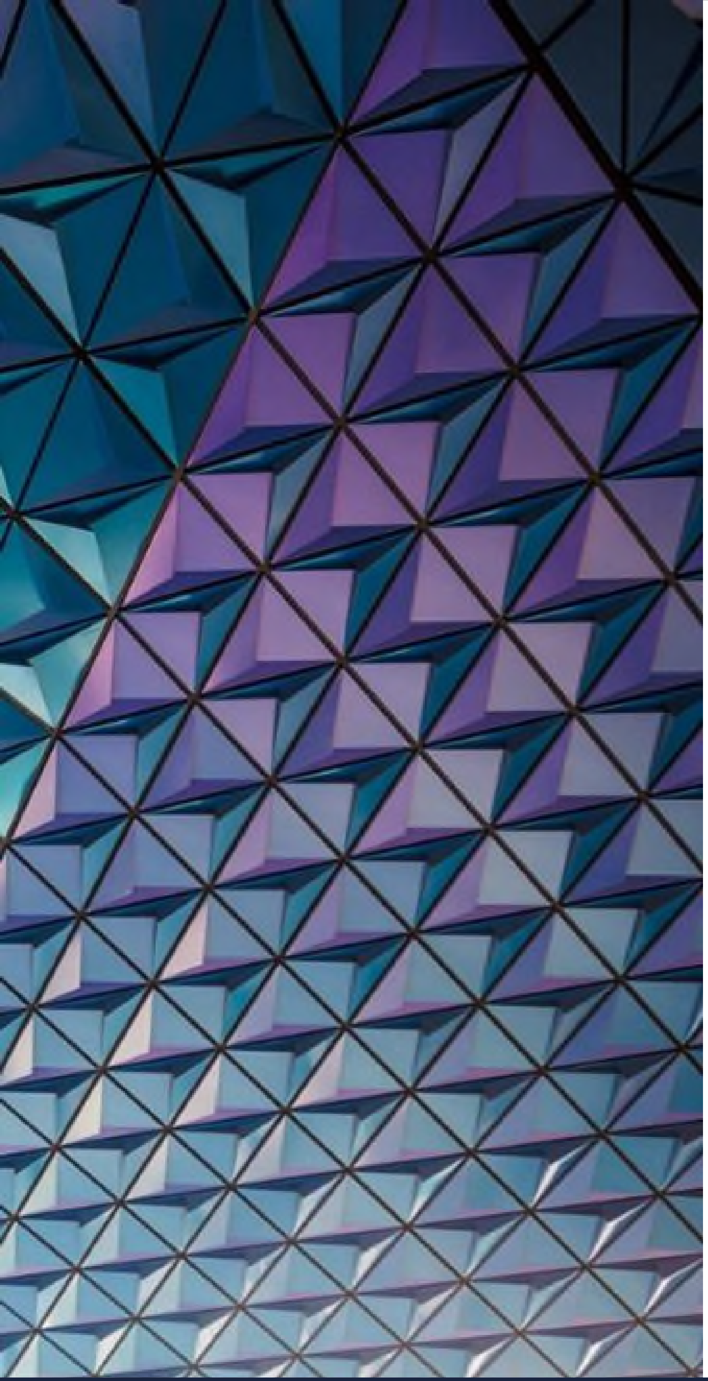
- Fixing the problem is paramount, but do so knowing regulators and potential claimants are lurking

- Ensure key requirements are adhered to from day one – including privilege

6. Communicating about events has risk – silence is riskier

- Timing is key
- Be transparent to the extent you have certainty, and sometimes all that's certain is there's an issue you are addressing
- Consider both internal and external comms, including media, customers, shareholders and regulators
- Internal communications may be used against the company, particularly if they conflict with (or suggest a potential conflict with) public statements
- Being precise and thoughtful, while truthful and candid, will help minimise the risk that communications are subsequently used against the company
- Obtain external expertise





7. Having clear operational authority and escalation criteria is critical

- Decide this in advance
- Planning in advance is key – develop appropriate policies
- Test and refresh regularly
- Who is responsible for key decisions?

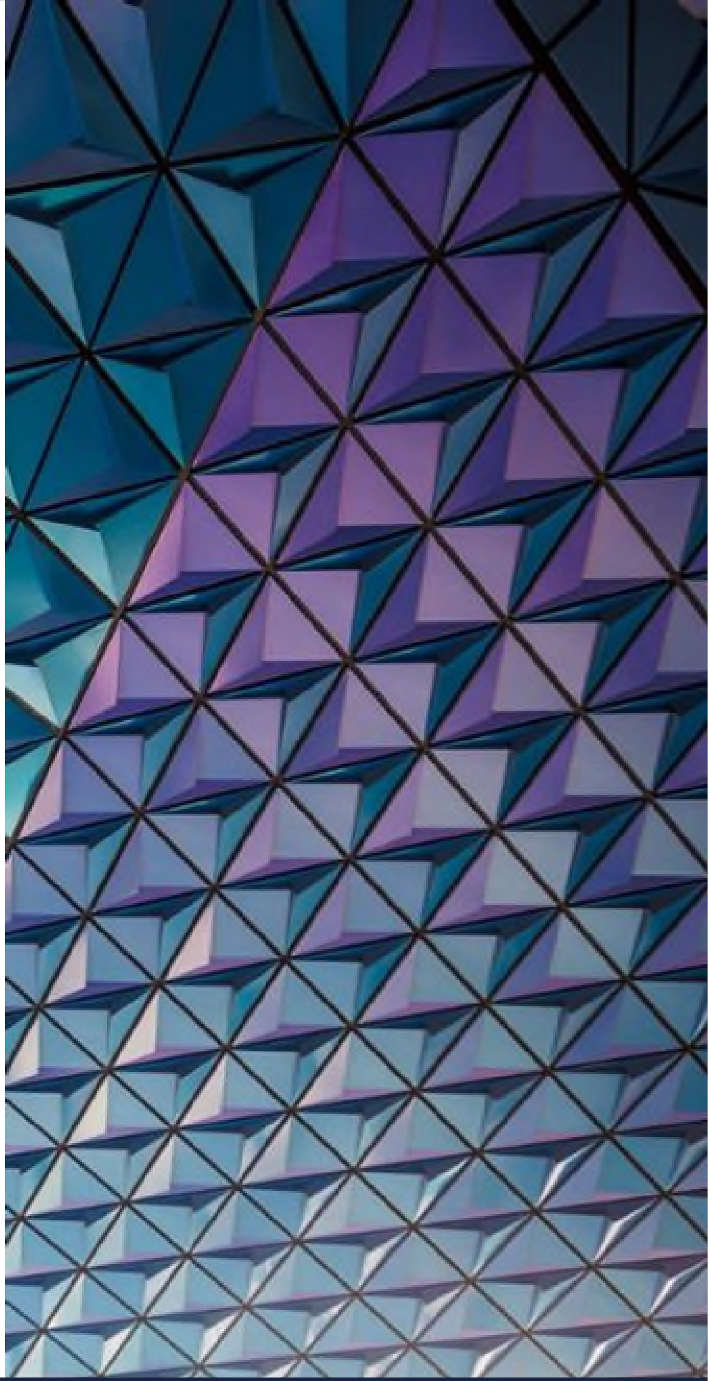
8. Understand your business processes and data flows ahead of time

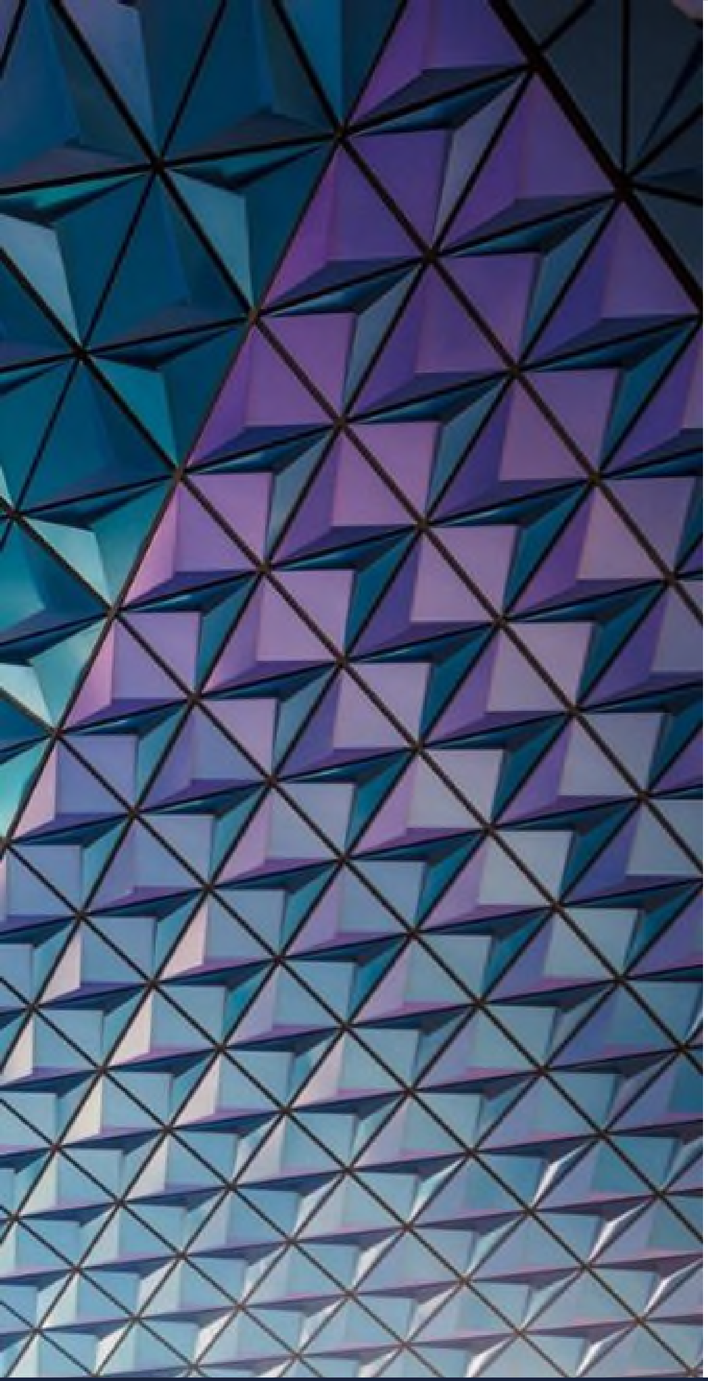
- Don't wait for a problem to understand how your systems work or what data you hold

- Having clarity will help you understand and mitigate the impact

- Activities such as data mapping are beneficial (including supply chain)

- Also consider approach to retention



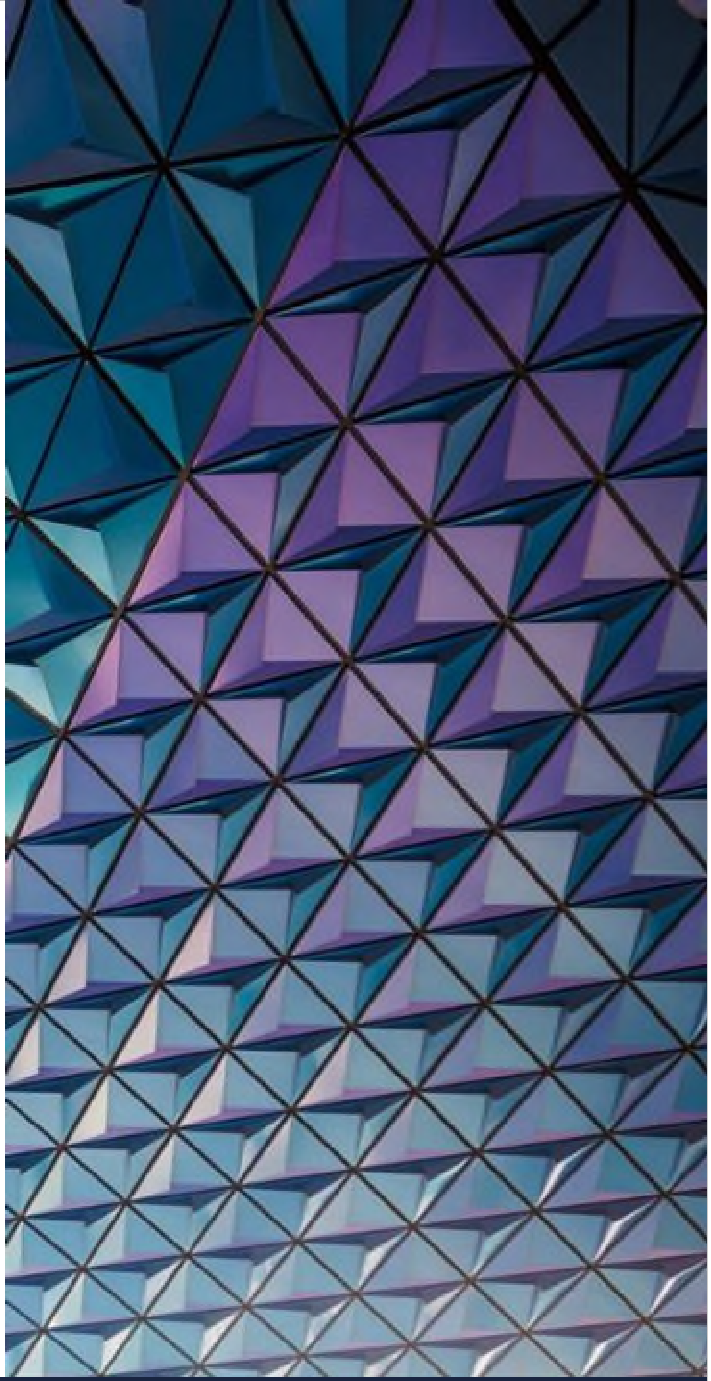


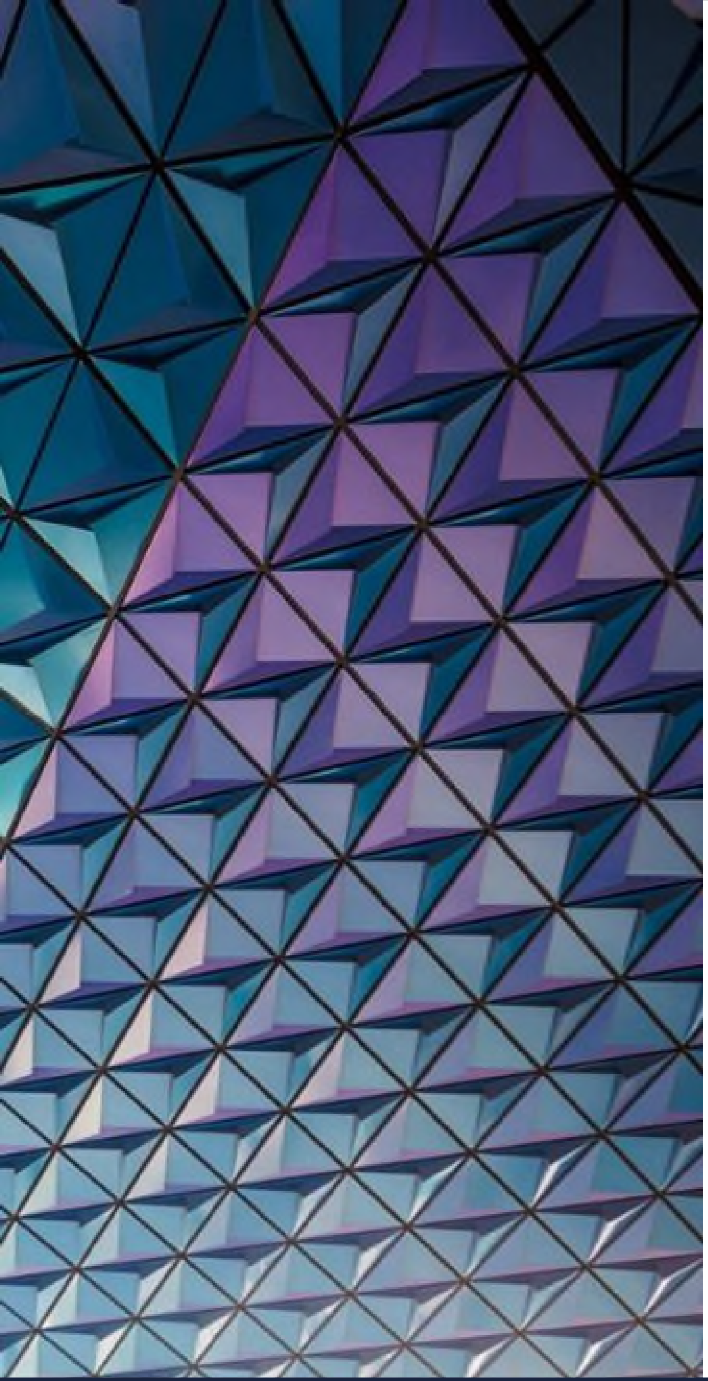
9. Recovery will take longer than you think

- There is no magic switch to recover your business after an attack - it will take a lot of time and effort
- Be realistic with internal and external assessments – avoid the pressure to “sugar-coat”

10. You can’t fight physics

- Certain parts of the process are dependent upon the speed of getting and processing large amounts of information, and you can’t make that go faster than physics will allow
- There are other ways to speed up incident response – for example, pre-engagement of key external vendors





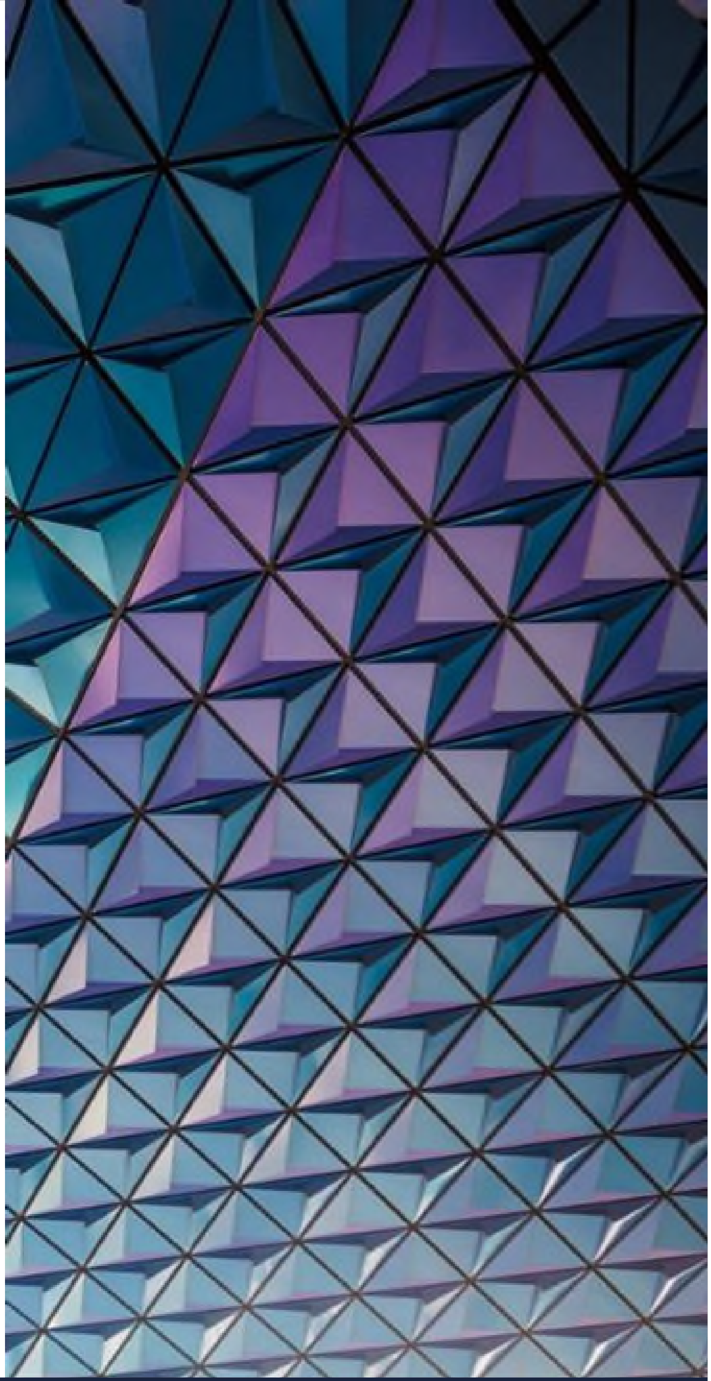
11. Internal IT/IS teams are a key bottleneck

- There will be a core group of internal IT/IS professionals that external expertise cannot replicate, and this will be one of your main choke points
- Rely on your key people, knowing there's only so much they can do
- Move quickly to bring in outside help
- Present a united front

12. Cyber isn’t the problem, resiliency is

- Having robust backups and contingency plans is the key to minimising business disruption

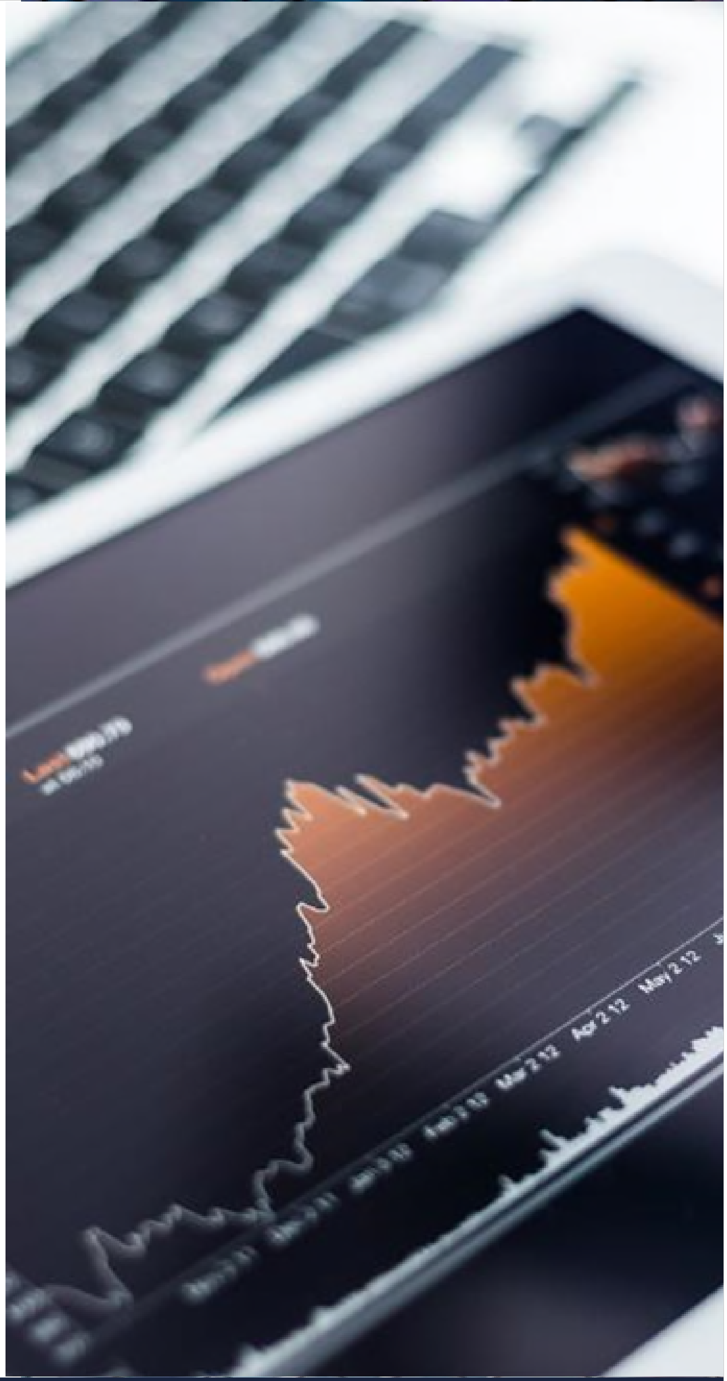
- Consider redundancy – buy two of what you really need



Key take-aways

- Incorporating these insights into your incident response program may help streamline and strengthen the process from start to finish

- The best time to prepare for an incident is before it happens, so all organisations should be focused on key areas including:
  - Developing / testing /maintaining plans
  - Understanding their environment (including data maps and role of supply chain)
  - Pre-engaging key vendors



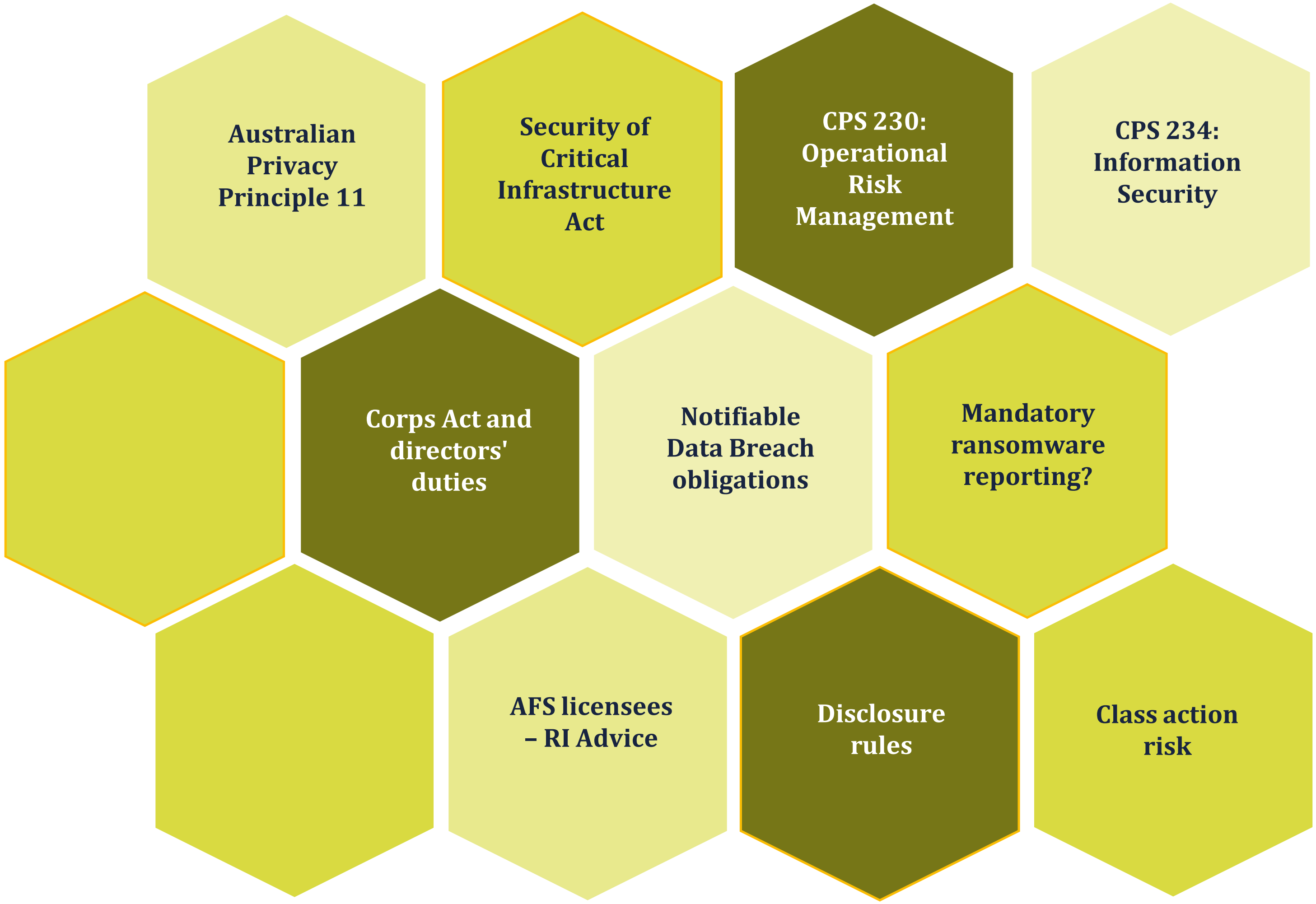
Practical tips

- Routinely evaluate cybersecurity risks, such as by developing a remediation plan for material cybersecurity risks, to help reduce exposure by preventing nascent risks from materialising into incidents
- Create internal protocols that encourage connecting the dots for even seemingly unrelated cyber events, as those events could share a common root cause or nexus
- Be mindful of mitigating risks resulting from unmanaged technology (i.e., “Shadow IT”) and information systems assets to prevent network activity that is inconsistent with security policies
- Evaluate internal process for reviewing and validating public statements about cybersecurity, incidents, and development practices
- Consider performing gap and maturity assessments as part of a broader privileged review
- Examine the organisation’s culture, staffing, and resourcing - foster a culture of compliance and active dedication to mitigating risk, instead of passive acceptance

Legal and enforcement landscape and best practice

Current legal landscape

No comprehensive cyber security law, but overlapping obligations



Australian Privacy Principle 11

Security of Critical Infrastructure Act

CPS 230: Operational Risk Management

CPS 234: Information Security

Corps Act and directors' duties

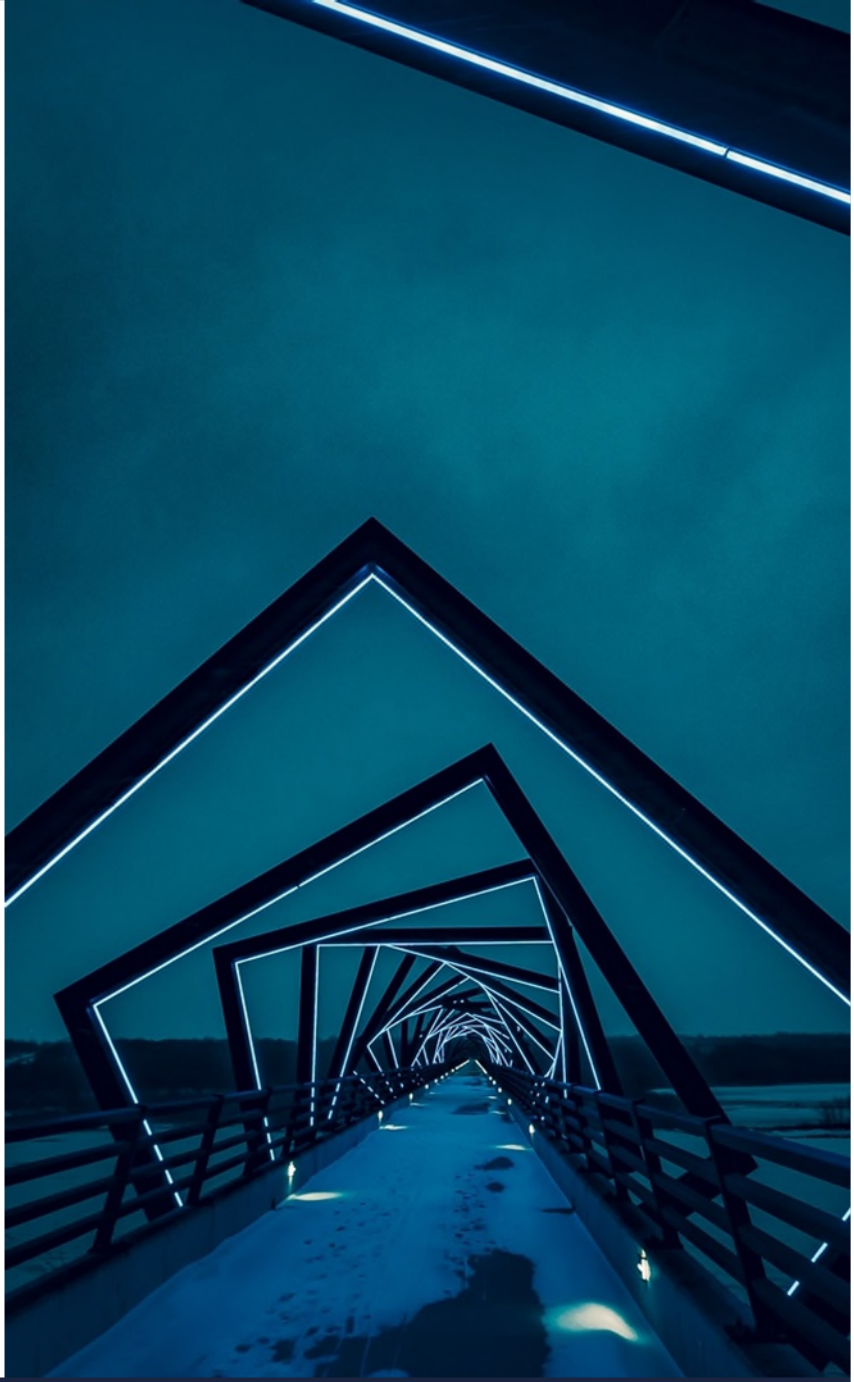
Notifiable Data Breach obligations

Mandatory ransomware reporting?

AFS licensees – RI Advice

Disclosure rules

Class action risk



Best practice approaches

Essential 8

- Home grown – developed by the Australian Cyber Security Centre
- Eight core mitigation strategies, with four different maturity levels, plus guidance
- Should be viewed as a baseline

Information Security Manual

- Developed by Australian Signals Directorate
- Cyber security principles and guidelines (more detailed than the Essential 8)
- Widely used by Federal Government (and its supply chain)

ISO 27001 – Information Security Management Systems

- Globally recognised standard
- Can be organisational wide, or for specific systems
- Requires external accreditation
- Can be time-consuming and costly

PCI DSS – Payment Card Indutry Data Security Standards

- Applicable to the storage, transmission and processing of payment card data

SOC 2 – System and Organization Contol Report

- Independent audit of information security controls
- Used to audit SaaS providers

NIST Cybersecurity Framework

- Mandatory for US federal government agencies

WIN In-House Counsel Week

Thank you for joining our webinar: Insights from the trenches - top tips for managing (and avoiding) cyber incidents

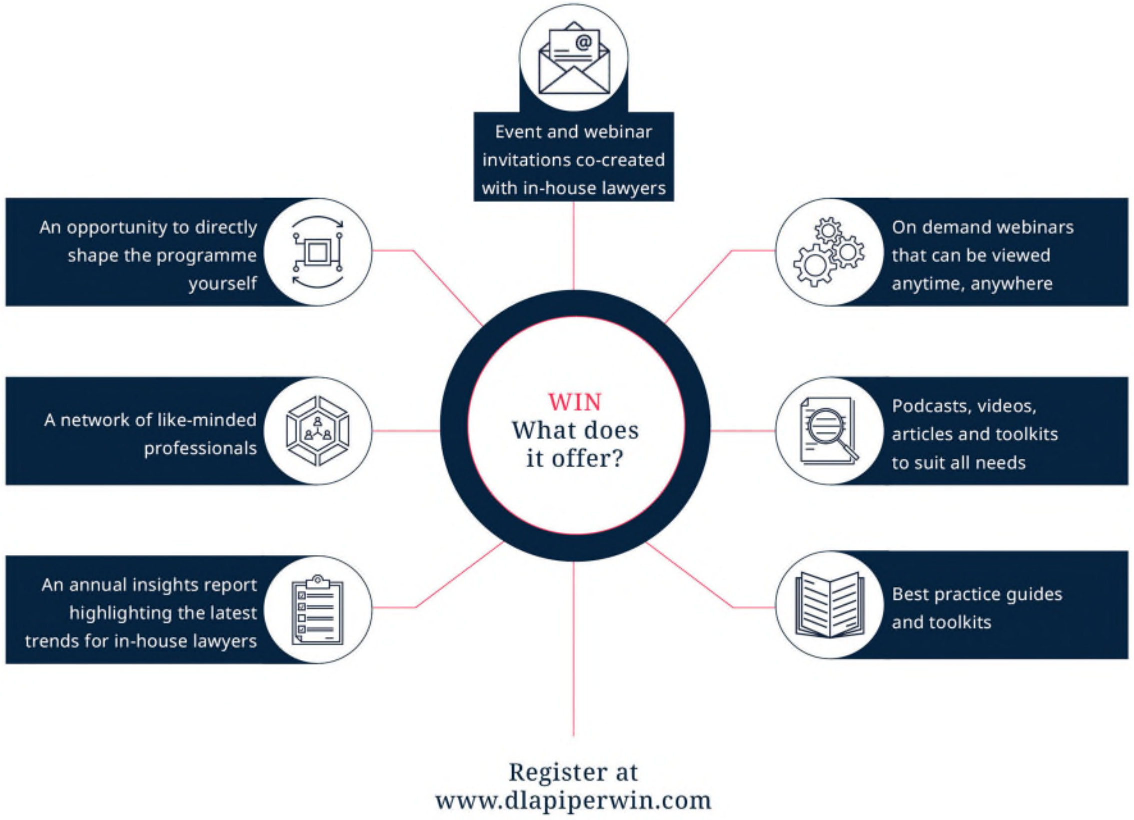
Session presenters:

Sarah Birkett
Special Counsel
T: +61 3 9274 5464
sarah.birkett@dlapiper.com

William Kwan
Senior Information, Security & Compliance Manager
+61 3 9274 5151
william.kwan@dlapiper.com

Join our WIN program today

Register at
www.dlapiperwin.com



WIN
What does it offer?

Event and webinar invitations co-created with in-house lawyers

An opportunity to directly shape the programme yourself

On demand webinars that can be viewed anytime, anywhere

A network of like-minded professionals

Podcasts, videos, articles and toolkits to suit all needs

An annual insights report highlighting the latest trends for in-house lawyers

Best practice guides and toolkits

Register at
www.dlapiperwin.com