



# Keeping Privacy Private in the Pacific



MARSH

Today's webinar is sponsored by:



MARSH





# Keeping Privacy Private in the Pacific

Visit [www.advisentd.com](http://www.advisentd.com) at the end of this webinar to download:

- Recording of today's webinar
- Copy of Slides

# ARE YOU A RISK MANAGER?

We have something just for you



Risk Managers and Insurance  
Buyers now get FPN Pro **FREE**

LEARN MORE

# Cyber OverVue

Adv|isen  
Transforming Insurance™



DATA DRIVEN SOLUTIONS  
TO EVALUATE CYBER RISK

LEARN MORE

Adv|isen  
Transforming Insurance™

# Today's Moderator



## Chad Hemenway

Managing Editor  
**Advisen**

Email at [chemenway@advisen.com](mailto:chemenway@advisen.com)

# Today's Panelists



**Kelly Butler**

Cyber Practice Leader - Pacific  
**Marsh**



**Lisa Fitzgerald**

Partner, Corporate  
**Lander & Rogers**



**Max Broodryk**

Product Leader – Cyber Risk  
International Financial Lines  
**AXA XL**

MARSH JLT SPECIALTY

LANDER  
& ROGERS



# Keeping Privacy Private in the Pacific



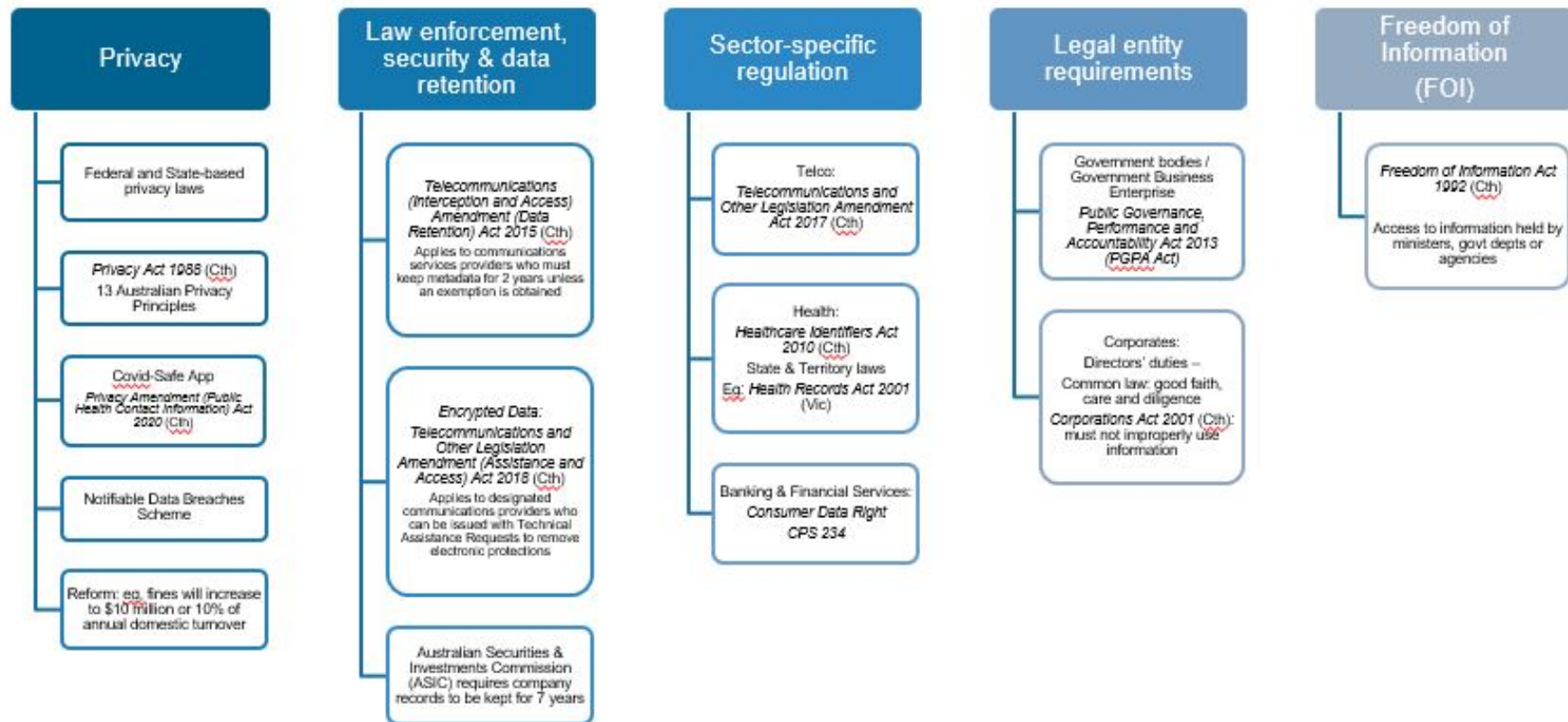
# Current Cyber Landscape

- **Targeted and more ambitious attacks:** New and emerging attack groups, refinement of tools and tactics used – Living off the Land attacks and shift towards “big game hunting”
- **New targets and access points:** Supply chain attacks up 78% in 2019, Internet of Things devices highly susceptible and targeted. Critical infrastructures will be plagued by more attacks and production downtimes
- **COVID 19:** has created substantial increase in remote working and overall internet user traffic, and rapid uptake of outsourced technology – increasing potential attack surface for many organisations. The ACSC has advised ongoing reports of COVID 19 related scams fraud and phishing campaigns as hackers seek to exploit uncertainty about the pandemic
- **Ransomware:** quickly reaching epidemic levels not just from frequency but more so the severity of demands:
  - The most frequently reported claim of the year – with several large Australian firms falling victims
  - New strains of ransomware – eg. Maze, which exfiltrates data as well as encrypting
  - Trends towards larger ransom demands
- **Increased focus from government and regulators:** Cyber Security Strategy released in August outlining \$1.79 billion in spending and additional regulatory measures. Released in the wake of PM’s announcement of targeting of Australian organisations by a “sophisticated state-based cyber actor”, and bolstering requirements with the Notifiable Data Breaches Scheme under the Privacy Act.

# Industry Headwinds

- The global cyber insurance market, including Australia, has experienced several large losses in 2019 and 2020 that have had a significant impact on the premium pool.
  - Ransomware is now driving large losses
  - Nation state attacks have increased
- Cyber insurance is inherently difficult to price, given that the frequency or severity of cyber-attacks cannot necessarily be predicted based on prior historical claims experience
- There is a concern within the insurance industry that insurers are not adequately pricing for the risk of aggregation (i.e. a single event affecting multiple policies):
  - Across different product lines
  - Across common vulnerabilities
  - Across common infrastructure
- Remote working as a result of the Covid-19 pandemic has increased the vulnerability of entities to cyber-attacks
- The regulatory risk of data breaches is increasing.

# Australian Data Regulation



# Ransomware Trend Summary

- ➔ Trend of increased frequency and severity of ransomware attacks continues in 2020
  - ➔ Resulting in a direct increase in ransomware claims and cyber industry loss ratios
  - ➔ Partially offset by trend of reduction in other types of data breach events
- ➔ Rise of the 'Big game hunting' movement has resulted in increased ransom demands
  - ➔ Targeted, sophisticated attacks against major companies
- ➔ Dual extortion techniques, which blend ransomware requests and data breach
  - ➔ This will impact the claims evolution and requires a blended response to both detection and incident response
- ➔ COVID-19 related attacks
  - ➔ Mass agile working and exploitation of remote access

# Australian Privacy Law v GDPR

Requirement	Australia	GDPR
Reasonable steps to ensure privacy compliance and transparency	APP 1	Article 5, Principle 2
Privacy policy	APPs 1.3 and 1.4	Articles 7, 12-14
<b>Consent</b> to use personal information	Not always required if 'reasonably expected' and may be implied or express	There must be a legal basis or explicit consent
Permissible collection of information	APP 3 PI may only be collected where reasonably necessary or directly related to functions or activities, and by lawful and fair means	Article 5 PI may only be collected for specified, explicit and legitimate purposes
Notification of collection	APP 5 Collection notice is required	Articles 13-14 Privacy statement is required
Permissible use or disclosure of personal information	APP 6 Use for a primary purpose does not always need consent  Use for a secondary purpose may need consent  Exceptions Health, safety and law enforcement may require disclosure outside the secondary purpose	Article 6 Data processing may only occur where the data subject has consented to one or more specific purposes  Exception Where processing is necessary to perform a contract or comply with a legal obligation
Cross-border disclosure in compliance with certain conditions	APP 8 Requires reasonable steps to ensure the overseas recipient does not breach the APPs and recipient must be subject to similar laws	Chapter 5 Permitted only where the jurisdiction is 'adequate' in terms of data protection laws and rules
<b>Government-related identifiers</b> must not be used to identify persons	APP 9 Government related identifiers may not be used to identify individuals: eg TFN, Medicare #	No equivalent
Ensure data quality and integrity	APP 10	Article 5
Reasonable steps to keep personal information secure	APP 11	Article 5
<b>Access requests</b>	APP 12 (exceptions, eg employee records)	Article 15 (additional rights)
Correction of personal information	APP 13 (reasonable steps to correct)	Article 16 (absolute right to obtain without delay)
Penalties	Now: \$2.1 for serious or repeated breaches Future: greater of \$10million, 3x the value of the benefit obtained from the data misuse or 10% of annual domestic turnover	Greater of 20million euros or 4% of global annual turnover, for infringements (maximum)
<b>Application</b>	Government agency, company with an annual turnover of \$3million	All entities

# Who is responsible for cyber risk?

## Managing cyber risk

- generally accepted to fall under the risk management umbrella of boards of directors (express under CPS 234 for financial services companies)
- all directors and officers have a key responsibility (and personal liability) to ensure adequate risk management strategies exist to protect the company and shareholders
- cyber incidents likely assessable in the context of overall duties to company, shareholders and risk management function

## Directors' duties

- directors and officers have a fundamental, non-delegable duty to exercise reasonable care and diligence, both under s 180 of the Corporations Act 2001 (Cth) & common law
- scope of this duty untested for cyber risk but courts imposing increasingly high standards of care on directors and officers and intimate understanding and active management of all risks

## Listed companies

All publicly listed companies on the Australian Securities Exchange (ASX) also have:

- continuous disclosure obligations to inform the ASX of any information that materially affect price or value of the company's securities
- a potential obligation to notify the ASX of a cyber incident
- **industry-specific** obligations should a cyber incident occur, requiring notification to **regulators** and affected individuals of cyber incidents

## Enforcement

The corporate regulator, Australian Securities and Investments Commission (ASIC), empowered to bring actions against directors/officers for a breach of their duties. Consequences:

- a declaration of contravention
- pecuniary penalties
- compensation orders
- disqualification of the director or officer from managing a corporation

Failures by directors and officers to take reasonable steps to prevent, or respond appropriately to, a cyber incident may also give rise to:

- civil proceedings by affected individuals
- derivative actions brought by shareholders

# Thank You!

**Marsh JLT Specialty** is a trade name of **Marsh LLC**. Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position. **Marsh.com**



@Marshglobal

@Marsh

---

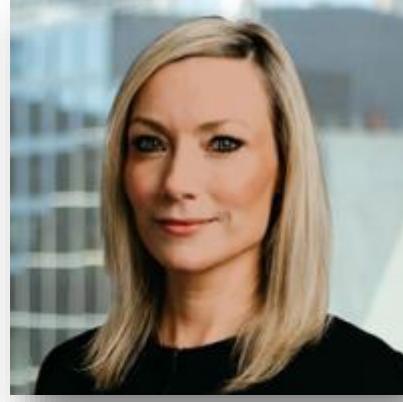
# Keeping Privacy Private in the Pacific



**Chad Hemenway**  
Advisen  
[Moderator]



**Kelly Butler**  
Marsh



**Lisa Fitzgerald**  
Lander & Rogers



**Max Broodryk**  
AXA XL



# Thank You Panelists



**Kelly Butler**

Cyber Practice Leader - Pacific  
**Marsh**



**Lisa Fitzgerald**

Partner, Corporate  
**Lander & Rogers**



**Max Broodryk**

Product Leader – Cyber Risk  
International Financial Lines  
**AXA XL**



# Keeping Privacy Private in the Pacific

Visit [www.advisentd.com](http://www.advisentd.com) at the end of this webinar to download:


- Recording of today's webinar
- Copy of Slides

For more on Advisen, visit at  
[www.advisentd.com](http://www.advisentd.com) or email us at  
[webinars@advisen.com](mailto:webinars@advisen.com)



MARSH





Leading the way to **smarter**  
and more **efficient**  
risk and insurance **communities.**

*Advisen delivers:*  
the **right information** into  
the **right hands** at  
the **right time**  
to **power performance.**

#### **About Advisen Ltd.**

Advisen is the leading provider of data, media, and technology solutions for the commercial property and casualty insurance market. Advisen's proprietary data sets and applications focus on large, specialty risks. Through Web Connectivity Ltd., Advisen provides messaging services, business consulting, and technical solutions to streamline and automate insurance transactions. Advisen connects a community of more than 200,000 professionals through daily newsletters, conferences, and webinars. The company was founded in 2000 and is headquartered in New York City, with offices in the US and the UK.

+1 (212) 897-4800 | [info@advisen.com](mailto:info@advisen.com) | [www.advisenltd.com](http://www.advisenltd.com)