CYBER UPDATE

New Zealand Cyber – What is Happening ?

OCTOBER 2025

LOCKTON®

Discussion Points

What bring us here & some topical issues

Brief evolution of cyber and insurance risk in New Zealand

Unusual market trends

Key takeaways

What brings us here?

Another day, another cyber issue

Insurance News · China-linked cyber campaign targeting law firms, warns Google

China-linked cyber campaign targeting law firms, warns Google

Have you legal clients? They may already be compromised

Home / New Zealand

Wellington law firm warns clients of potential for leak after cyberattack

Business News · Microsoft server software comes under widespread cyberattack

Microsoft server software comes under widespread cyberattack

Analysts warn of widespread breaches around the globe

Auckland accounting firm named in ransomware group data leak

Emerging cybercrime group claims breach of business and client records

Lawyers urged to check IT systems as scammers target clients and trust accounts

CRIMINAL NEWS

Home / New Zealand

Wellington law firms fall prey to offshore scammers posing as ANZ bank, over $2m stolen

What is going on?

Increase in cyber incidents reported.

Social engineering, phishing and business email compromises remain common.

Recent phone scam example.

Increase in regulatory pressure and obligations.

(more prevalent outside of NZ)

Data Driven

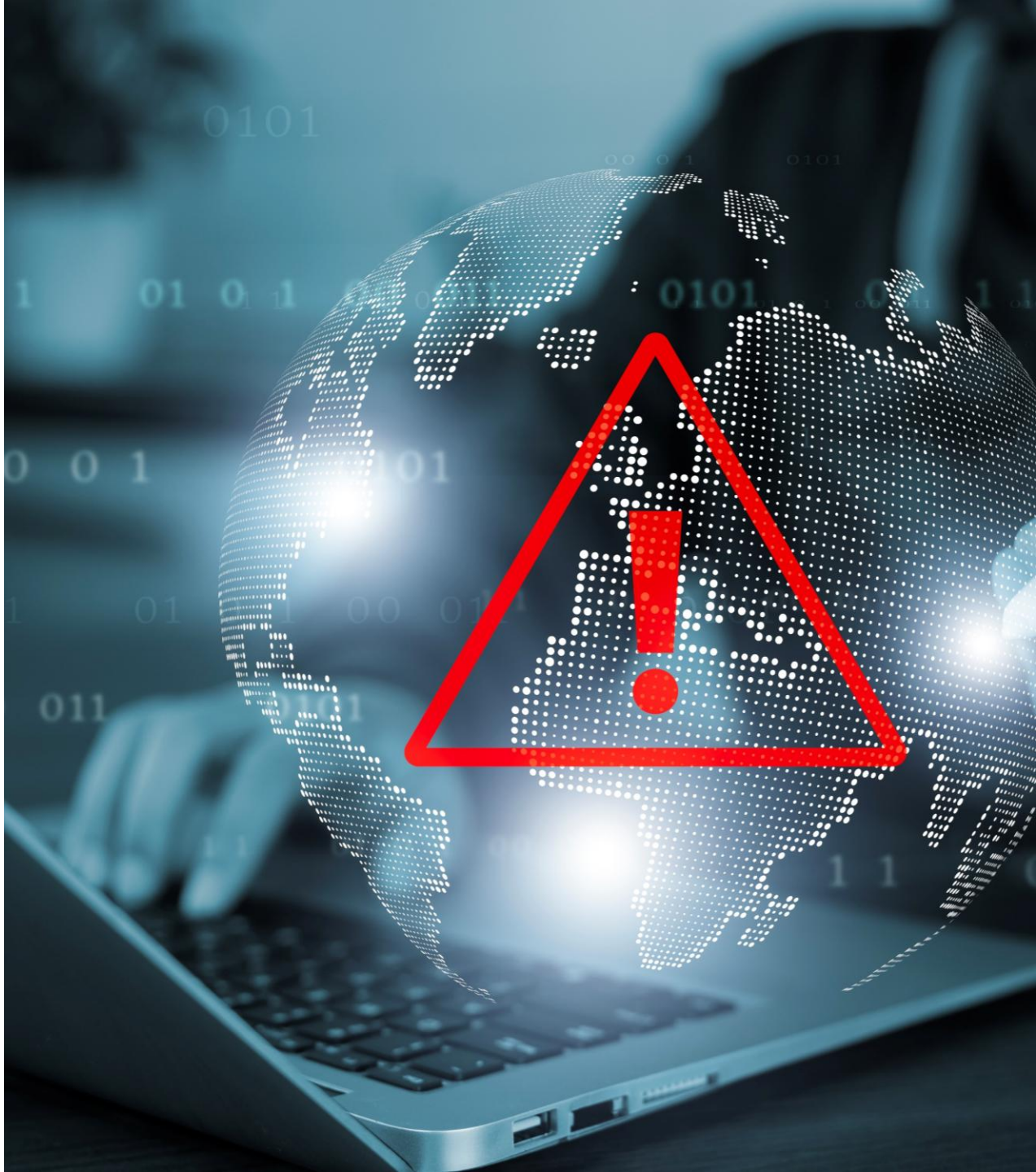
Over 50% of NZ SMEs faced a cyber threat in the past 6 months
National Cyber Security Centre, Sept 2025

Cyber incidents ranked #1 global business risk for last 4 years.
Allianz Global Risk Barometer, 2025

30% of NZ executives say cyber is their biggest concern
Insurance Business News Survey, 2025

NZ still has a very relaxed view of cyber exposure.

‘It won’t happen to me’ is alive and well !!!!



Brief Evolution of Cyber Insurance in New Zealand

ESurance

The original Cyber Insurance – Click for Cover (CFC)

Evolution of Cyber Underwriting

Declarations to Proposals to Nothing……

Risk Areas in Focus

- Multi Factor Authentication for remote access
- Firewalls / Endpoint Protections
- Data Storage / Privacy Management
- Staff Awareness/Training

Cyber Insurance Market Trends

- Something is not quite right.
- Over supply of cyber insurers and capacity with coverage expanding and premiums reducing.
- Cyber Incidents are increasing and quantum and frequency of claims increasing also so how can this be.
- What comes next ?

Not all Cyber policies respond the same way

With such a range of markets, insurers and solutions available what do we need to think about ?

Social Engineering (Phishing): - Sub limits will often apply to this cover.

Business Interruption : If your service provider is interrupted, are you covered.

Conditions Precedent to Indemnity : Hidden in the wording or endorsements.

What about a non malicious Cyber event – think CrowdStrike ?

Contingent / Non-Contingent Business Interruption – what is the difference.

We are currently working with the NZLS so watch this space.

KEY TAKEAWAYS

01

Pause and consider these key points.

- Is the message creating an unnecessary sense of urgency.
- Is it sending you to a website that doesn't look correct.
- Is it making an offer that's too good to be true?

02

Do the basics right.

Don't just rely on your managed service provider and have a strong layered approach to cyber security.

Incident Response Plan. Know who to call and what to do if things go sideways.

03

Make sure you have a fit for purpose insurance solution.

There are a range of options available.

04

No substitute for proactive staff training – awareness is the key

Organisations that regularly test their cyber incident response plans are significantly less likely to face breach-related cyber issues.

THANK YOU !