Australian Insurance Law Association (AILA) National Conference 2019 – Questions from the Event App.

1. Should there be a minimum standard of security signed off by boards/management? What should that standard be?

There is no set minimum standard for unregulated entities and organisations should look to industry best practices. Most organisations that do business on the internet, hold potentially sensitive data and/or have a highly digital supply chain should be running regular independent vulnerability assessments of all systems and penetration testing of internet-facing systems like VPN/remote access and web sites. They should also have a cyber security strategy, policies and procedures and run cyber risk awareness training for all staff. Organisations should also review all 3rd party service provider agreements and have an incident response plan.

In terms of regulation: On July 1 2019, APRA's CPS 234 came into effect for APRA regulated entities, that requires certain minimum standards be adhered to by July 1 2019. For 3rd party service providers to regulated entities, contracts need to be in check with the regulation on renewal, or by July 1 2020. There are also mandatory data breach reporting requirements under The Federal Privacy Act (1988) for all organisations with turnover >AUD 3 million or hold highly sensitive information like healthcare.

Whilst CPS 234 compliance specifically requires board involvement, there is currently no requirement for other organisations. From the CPS234 Prudential Practice Guide:

"Under CPS 234, the Board of an APRA-regulated entity is ultimately responsible for the information security of the entity." [1]

The boards and leadership teams I have spoken to all understand they should have a better understanding and take more responsibility, however there is still a concerning gap for most organisations between the IT teams' cyber risk management knowledge and that of leaders outside of IT. Assisting organisations to close this gap is one of the key functions of the Cyber Advisory Practice.

Ideally the Federal Government's 2020 Cyber Security strategy will provide more guidance for all Australian organisations and the tools to help them improve, and be able to better articulate, their cyber risk management capabilities. There is a groundswell in the cyber industry for increased regulation of all ASIC registered businesses, but we'll see. I like to use CPS 234 compliance methods, where relevant, as an aspirational goal for organisations I work with.

2. Ransomware attacks aimed at businesses tend to seek ransoms equivalent to the probable limits of liability under the victim's cyber security policy. Where do we go to deal with this?

As I mentioned in the presentation, organisations must ensure that their limits of liability are kept totally confidential. If cyber criminals think that an organisation with a ransomware insurance buffer is a softer target, then they will do what they can to find out the limits and set extortion demands accordingly.

Unfortunately, with ransomware, if an organisation does not have the ability to revert to backup or will suffer too much in terms of business interruption, then a tough decision must be made in the case of an incident. It is important to keep in mind that often paying the ransom doesn't provide the solution and can lead to further demands.

[1] https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_1.pdf

An organisation's cyber incident response strategy should have a pre-defined policy for ransomware, and even better, has includes scenario testing.

3. Does the AICD have cyber risk included in its training and updates to directors?

The AICD offers a "Cyber for Directors" [2] one-day short course, which I have heard from attendees is well worthwhile. There is also much discussion around cyber risk in the Company Directors Course and that Directors must be providing more effective governance in this area.

4. Passwords - why don't we use fingerprint and facial recognition technology in our work environment and how secure is it?

This is an interesting question. Computers, tablets and phones all support biometric authentication – mostly passwords and fingerprints, however many organisations do not switch it on for company-owned assets or support it for "Bring Your Own Device" connections to corporate resources. There are a few reasons for this:

- Biometric authentication is still considered relatively new technology to be enforced for all users
- Older devices may not support the functionality
- IT support teams have seen a sharp increase in support calls from users when adopting the tech
- Use of facial recognition can lead to privacy concerns, however it is becoming more commonplace

Most highly sensitive commercial cyber environments like data centres use biometrics for physical access, we will see this expand to more full-scale adoption in the coming years.

In terms of its security, using biometrics instead of passwords should be more secure as there are more complexities in a biometric signature and are therefore much harder to hack. Use of such technology must be well-planned and have clear policies and procedures, especially around system administration.

5. From a cyber terrorist perspective, can individual flying aircraft be hacked?

As I mentioned in the presentation, anything that is "smart" can potentially be hacked. Modern aircraft can use networks to communicate with airport support systems and airlines are very careful if they use this technology. Many do not use it for security reasons, and if used are "closed-loop" with no connection to the Internet. Internal wi-fi systems on planes for travellers are not connected to any of the airplane systems (that I know of!)

IT security is only as strong as its weakest links, that's what hackers look for. Unfortunately, the weakest links have often proven to be the people who use and manage IT systems. This is one of the reasons that effective security awareness training around use and administration of systems, along with the existence of clear policies and risk management strategies, is critical.

Please feel free to get in touch with any further questions.

[2] https://aicd.companydirectors.com.au/education/courses-for-the-director/short-courses/cyber-for-directors