Episode 16: Summary

Episode name: Managing Data Breaches and Cyber Incidents
Guest(s): Reece Corbett-Wilkins

What area(s) of law does this episode consider?

Cyber security and privacy laws.

Why is this topic relevant?

Our personal data is collected, stored, analysed and disclosed by corporations and government agencies everyday, sometimes passed on to external third parties, meaning this information can be exposed in the event of a cyber security attack. The effects of such an attack can not only mean loss of data, the cost to overcome such an attack, together with, in some instances, loss of reputation, which can be critical.

A study by global cybersecurity firm, Webroot, surveyed 600 SMEs in Australia, the UK and the US, as to the average cost to that business of a cyberattack. In Australia, the figure on average is approximately $1.89 million. Half of Australian respondents to that study indicated that their business would face costs of more than $1.3 million if critical client or business records were lost.

As our world increasingly moves to operate completely online with the rise of e-retail, e-commerce, cloud-based platforms and particularly working from home due to COVID19, it's therefore important to be aware of what best practice is to prevent a cyber attack from occurring, and how to manage the situation if one has taken place.

What legislation is considered in this episode?

Reece mentions the *Privacy Act 1988* (Cth) generally.

Regulators that oversee cyber incidents include:

- Office of the Australian Information Commissioner (OAIC);
- Australian Securities and Investments Commission (ASIC);
- the Australian Stock Exchange (ASX);
- Australian Competition and Consumer Commission (ACCC)
- Australian Cyber Security Centre (ACSC).

Foreign legislation and organisations mentioned in the episode include:

- European Union General Data Protection Regulation (GDPR); and
- Information Commissioner's Office (ICO) based in the UK.

What cases are considered in this episode?

1. '**Wannacry' ransomware attack in May 2017.**

    - Wannacry is an example of malicious software, or malware, used by cybercriminals to extort money. Ransomware is able to do this in one of 2 ways:

        - The ransomware locks you out of your computer so you are unable to use it; or

    - It encrypts valuable files so you are unable to read them. This is called crypto ransomware, and this is how Wannacry operates.

- The Wannacry attack of May 2017 attacked computers using Microsoft Windows as an operating system. It encrypted user data and demanded payment of a ransom in the cryptocurrency, Bitcoin, for its return.

- The attackers demanded $300 worth of Bitcoins, later increasing the ransom demand to $600. If victims did not pay the ransom within 3 days, they were told that their files would be permanently deleted.

- The advice when it comes to ransom payments is *not* to cave to the pressure, which of course, depending on the data you are unable to access might be easier said than done.

- This advice however, proved wise during the attack. It is said that the coding used in the attack was faulty – when victims actually paid their ransom, the attackers had no way of associating the payment with the victim's computer. To date, there are mixed reports as to whether users got their data back.

2. **Cambridge Analytica data breach in 2018**.

- Cambridge Analytica used data of 50 million Facebook users without their permission.

- The data was acquired via a third-party app, called 'thisisyourdigitallife', created by a researcher at Cambridge University's Psychometrics Centre, which was downloaded by 300,000 people.

- This gave the researcher, and by extension, Cambridge Analytica, access to not only their own data but that of their friends' as well.

- Cambridge Analytica worked on the 2016 Trump Campaign, which relied heavily on ad targeting.

- The user data obtained by Cambridge Analytica allowed the firm to build psychographic profiles of people and deliver pro-Trump material to them online.

What are the main points?

- A data breach is not simply an IT issue. It's reach extends far beyond that to a legal and ethical issue that requires expertise and advice to effectively manage.
- Cyber security firms can help contain the data leak, advise on negotiations with the threat actor, inform you on who to notify about the breach, and offer legal advice on the privacy impact.
- Organisations need to consider data protection within their own organisation as well as in relation to their service providers.

What are the practical takeaways?

- Businesses and employees should adopt best practice habits to avoid potential data risks, such as being able to identify phishing emails.
- Organisations should have an incident response plan in place and also consider the entire life cycle of data, not just focusing on obtaining data, but also making a plan for how to de-identify and delete data.

- Notifiable data breaches should be reported to the regulator, being the OAIC and the Australian Privacy Commissioner. Depending on the situation and leaked data, other institutions, such as the ASX, ASIC, GDPR etc., will need to be notified.
- Cyber insurance is becoming increasingly popular and is something that can prove useful in the event of a cyber attack.

Show notes

ACCC Scamwatch Website

OAIC Training Resources

OAIC Information Policy Resources

ACSC

A great explanation on the Cambridge Analytica scandal