HWL EBSWORTH
LAWYERS

CYBER BYTES

MARCH 2021

CYBER STATE OF PLAY: MARCH 2021

As cyber security risk continues to grow and evolve in 2021, we take stock of the current cyber state of play in Australia. What were the key developments in 2020, what have we already seen unfolding in 2021 and where is cyber law and regulation heading? Here is our snapshot.

THE THREAT LANDSCAPE

Ransomware grew exponentially in 2020 in frequency, severity and sophistication, with larger extortion demands and an increase in 'cybercrime-as-a-service'. The OAIC reported an increase of 150% in data breaches caused by ransomware in the first half of 2020, while the Australian Cyber Security Centre issued a number of ransomware alerts over the course of the year. In October, the US Office of Foreign Assets Control released an advisory warning against the sanctions risks of paying ransoms. As ransomware continues its upwards trajectory into 2021, it remains to be seen whether governments and regulators will crack down on ransom payments in response to growing calls for an outright ban on them.

Foreign states and the threat of cyber attacks were ever more on the radar, with the Prime Minister announcing on 19 June 2020 that Australia was under a series of attacks from a sophisticated state based cyber actor and the Defence Minister later suggesting that the line between "peace and war" had been blurred. Other nations also found themselves having to defend against foreign state cyber attacks and a number of the large incidents impacting the private sector were attributed to state sponsored actors.

Supply chain risk was a feature of numerous high profile and large scale incidents in 2020 and into 2021. These have included SolarWinds and Accellion and, closer to home, Law in Order, demonstrating the potential for a cyber attack on one company to affect multiple customers and stakeholders. In response to the growing risk, the ACSC has published a number of recent guides on identifying and managing cyber supply chain risk and managing security when engaging a managed service provider. The OAIC's latest Notifiable Data Breaches report also emphasised the risk of data breaches impacting managed service providers hosting data for one or more other entities.

COVID-19 wreaked havoc in 2020 and cyber security was not spared. The impact was felt with remote working risks, privacy concerns over contact tracing apps, COVID-19 themed scam emails and SMSes and, most alarmingly, cyber attacks on healthcare and other frontline sectors. As vaccines are rolled out, we are already starting to see a surge in further phishing emails and SMS scams with a vaccination theme.

Human error continues to be a major source of cyber risk. The OAIC reports human error as the second largest source of data breaches (38% of notified data breaches in the second half of 2020). Even amongst malicious or criminal breaches, which constituted 58% of notified data breaches, many were caused by social engineering or phishing emails which involve the human error of clicking on a malicious link or entering credentials. Thus, business email compromises continue as a major risk.

> *[T]he ACSC assesses ransomware as the highest threat. This assessment is based on the fact that ransomware requires minimal technical expertise, is low cost and can result in significant impact to an organisation, potentially crippling core business functions.*
>
> **Australian Cyber Security Centre,**
> **Annual Threat Report July 2019 - June 2020**

> *We know it's a sophisticated state-based cyber actor because of the scale and nature of the targeting and the tradecraft used.*
>
> **Prime Minister Scott Morrison**
> **19 June 2020**

> *All organisations should consider cyber supply chain risk management. If a supplier, manufacturer, distributor or retailer (i.e. businesses that constitute a cyber supply chain) are involved in products or services used by an organisation, there will be a cyber supply chain risk originating from those businesses.*
>
> **Australian Cyber Security Centre**
> **"Cyber Supply Chain Risk Management", January 2021**

THE NUMBERS

Australian Cyber Security Centre
Annual Threat Report July 2019 - June 2020

59,808
cybercrime reports to the ACSC from July 2019 to June 2020

2,266
cyber incidents responded to by the ACSC

27%
of ACSC cyber incidents involved "malicious emails"

OAIC Notifiable Data Breaches Report
July to December 2020

539
breaches notified to OAIC under NDB Scheme

58%
of data breaches from malicious or criminal attacks

68%
of malicious / criminal data breaches resulted from cyber incidents

$1.67BN
Government spend over next 10 years on Cyber Security Strategy 2020

17K
new cyber security jobs by 2026 as forecast by AustCyber

6,120
COVID-19 scams reported to Scamwatch up to March 2021

CYBER STATE OF PLAY: MARCH 2021

REGULATORS FLEX THEIR CYBER MUSCLES

Australia's regulators used their enforcement powers in 2020 more than ever before on matters of cyber security and data protection. These actions have come in a variety of forms:

- The **OAIC**, in the first use of its civil penalty powers, commenced Federal Court proceedings in April against Facebook alleging privacy breaches in the disclosure of 311,127 Australian users' personal information in the Cambridge Analytica scandal.
- The **ACCC**, with much higher penalties in its arsenal, continued to weigh into the data protection space, using consumer protection laws to allege misleading conduct in the use of personal data in a second action commenced against Google in July and obtaining a $2.7 million penalty against HealthEngine in the Federal Court in August.
- **ASIC** used the financial services licensee provisions of the Corporations Act 2001 (Cth) to bring a Federal Court civil penalty proceeding, commenced in August, against a financial planning company for alleged failure to have adequate cyber security systems.
- **APRA** released its 2020-2024 Cyber Security Strategy in November, flagging its intention to "take a much more targeted approach" in holding boards and management accountable where Prudential Standard CPS 234 Information Security is not complied with.

CLASS ACTIONS

In recent years, the prospect of privacy related class actions has been a gradually awakening 'sleeping giant', with the first litigation funded representative complaint to the OAIC filed in 2018 (against Facebook) and the first settlement of a common law privacy class action in the NSW Supreme Court in late 2019. In 2020, the sleeping giant was roused further, with an OAIC representative complaint brought against Optus in relation to an October 2019 data breach concerning the accidental online publication of 50,000 customers' names, addresses and phone numbers. This is the first OAIC representative complaint to be made off the back of a data breach notification under the NDB Scheme.

> *"Cyber threats and cyber security will be an area of focus for ASIC in 2021. ASIC's goal is to improve the cyber resilience of all entities operating in Australia's financial markets. ... We are assisting our regulated population in their efforts to improve cyber resilience. And we've shown that we will litigate when necessary."*
>
> **ASIC Commissioner, Sean Hughes, February 2021**

This edition of Cyber Bytes was written by Andrew Miers, Partner, Zoe Tishler, Associate, Claudia George, Lawyer, Max Henshaw, Lawyer, Luke Roper, Lawyer and James Fyfe, Lawyer.

HWL EBSWORTH
LAWYERS

NEW CYBER SECURITY OBLIGATIONS

We have seen a recent increase in new legislation, regulations, codes and guides prescribing new cyber security obligations. The Federal Government's Cyber Security Strategy 2020 flagged an intention to introduce further legislative changes to set a minimum cyber security baseline across the economy. Here are some of the cyber security obligations recently introduced, or currently in progress:

Consumer Data Right (CDR): The CDR commenced in the banking sector from 1 July 2020. Among the obligations imposed on 'Accredited Data Recipients' are detailed minimum information security controls (including multi-factor authentication, restriction of administrator privileges, password authentication, encryption and more) and a requirement to report security incidents to the Australian Cyber Security Centre.

The Internet of Things (IoT): On 3 September 2020, the Federal Government released a voluntary code of practice on securing the IoT with 13 principles for device manufacturers, IoT service providers, mobile app developers and retailers, dealing with matters such as passwords, a vulnerability disclosure policy and updated software security.

Medical devices: On 25 February 2021, changes to medical devices regulations came into effect for manufacturers and sponsors of software-based medical devices, with updated 'Essential Principles' which include new requirements for cyber security and management of data and information.

Critical infrastructure: The Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth) is currently before Parliament. It will impose new cyber security obligations on existing critical infrastructure sectors (electricity, gas, water and ports) and new sectors (including communications, financial services, higher education, energy, food and health), with higher level obligations for 'systems of national significance'. The Government will have power to intervene in significant cyber attacks.

Privacy: A review of the Privacy Act 1988 (Cth) kicked off in late 2020 and will continue throughout 2021, with the effectiveness of privacy enforcement and the Notifiable Data Breaches scheme amongst the issues being considered. The government has also committed to increased penalties for serious or repeated privacy breaches.

Standards: The Cyber Security Standards Harmonisation Taskforce (led by the NSW Government, Standards Australia and AustCyber) released its initial recommendations in January 2021 and is continuing to work on the adoption and implementation of cyber focussed standards (new, existing and revised).

Directors' duties: The Cyber Security Strategy 2020 suggested cyber security duties for company directors and other business entities as one potential reform option. This would be consistent with ASIC's recent cyber resilience focus which has relied on existing corporations law and directors' duties, but would presumably introduce more explicit cyber security obligations.