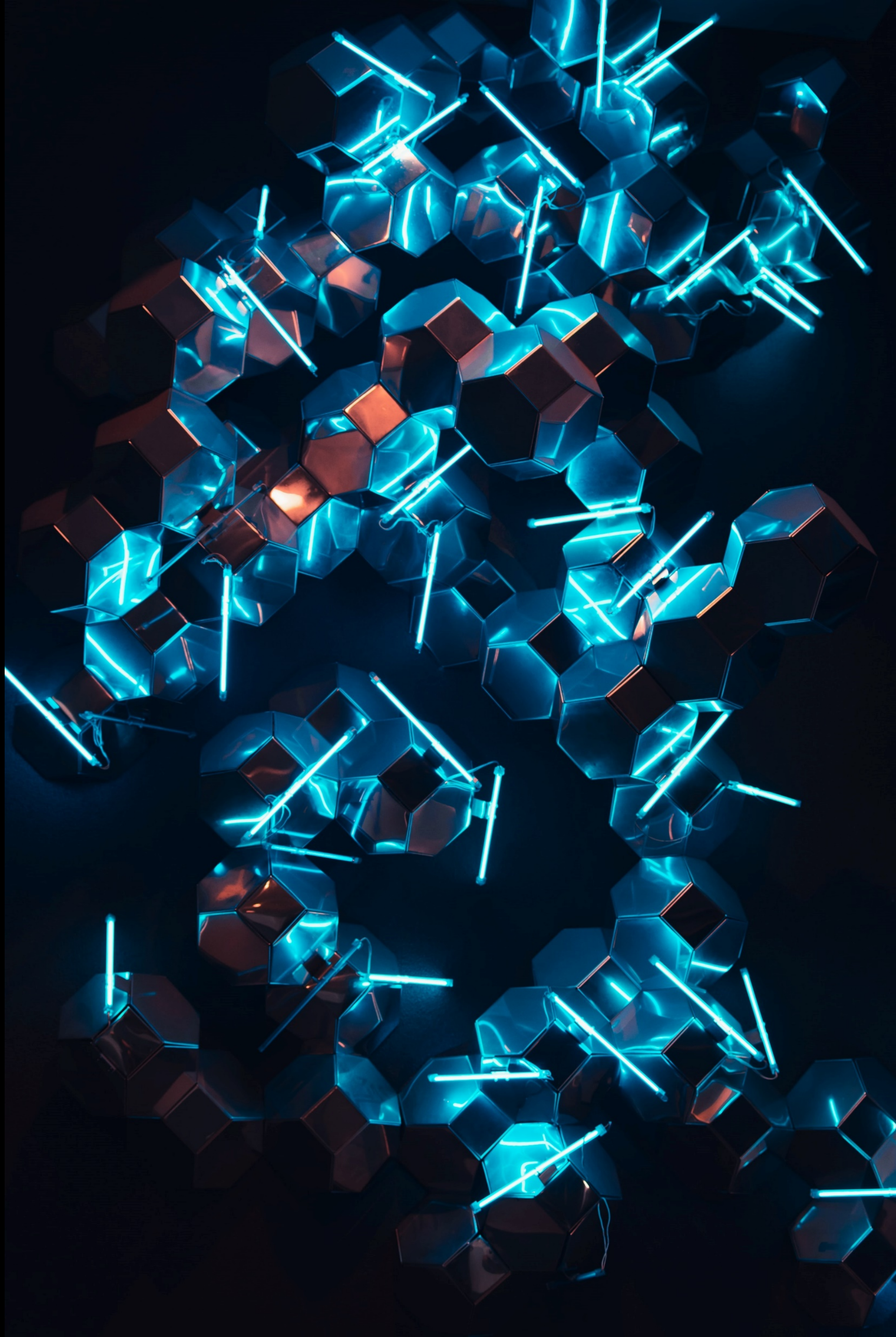
CYBER SECURITY

A year in review

December 2021

LANDER
& ROGERS



Foreword

As 2021 comes to a close and we step into 2022, we take this opportunity to reflect on how cyber threats have evolved both in Australia and globally, as well as the rapidly changing cyber regulatory landscape.

This year we saw a dramatic increase in the frequency and severity of cyber attacks, with ransomware the predominant mode and COVID-19 continuing to pose risk for organisations shifting to remote working and cloud-based services. Most alarmingly, we saw that threat actors are increasingly taking aim at our critical infrastructure industries and favouring supply chain attacks due to their greater impact. We have also seen an increase in attacks carried out by state-sponsored actors, who are generally not motivated by profit.

These threats and the potentially devastating impact of cyber attacks on critical infrastructure have been recognised by governments around the world, including in Australia.

We have seen several key regulations and policies being introduced throughout the year aimed at improving the cyber resilience of Australian businesses, particularly in the critical infrastructure sectors, and enhancing data protection.

Similar steps have been taken in the US, UK, EU, Singapore and China. The OAIC has also taken active steps throughout the year to enforce privacy legislation after several global companies were involved in data breaches.

Changes to the risk environment and the regulatory landscape have a significant impact on organisations. More than ever, the Board and management of organisations, regardless of their size and online capabilities, need to be aware of cyber risks, understand their responsibilities and obligations around cybersecurity, and take proactive measures to enhance their organisation's cyber resilience.

With the hardening cyber insurance market, companies seeking insurance cover are also facing increased scrutiny from cyber insurers.

Cyber insurers increasingly play an important part in educating clients and improving their cyber security.

We foresee that the role of cyber insurers in risk mitigation and increasing the cyber resilience of their corporate clients will continue well into 2022.

It seems generally accepted that cyber threats will evolve and become increasingly sophisticated. In particular, we expect that Australia will continue to face significant cyber threats in the next 12 months, with new ransomware models, supply chain attacks and exploitation of zero-day vulnerabilities already proving problematic.

Cyber threats cannot be eliminated, but organisations can make it more difficult for attacks to succeed. This will require strong will from all sides: Australian businesses (including their Boards and management), the cyber insurance industry and governments.

The enactment and enforcement of cyber security regulations introduced this year by the Australian Government will play an important role in shaping how Australia responds to cyber threats and improves its cyber resilience.

We trust that this inaugural *Cyber security year in review* will provide a useful guide to the nature of current cyber threats and Australia's rapidly evolving regulatory landscape.

Key contacts

Technology, privacy and cyber

Robert Neely *Partner*
Corporate

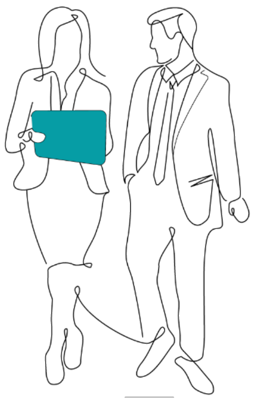
Lisa Fitzgerald *Partner*
Corporate

Keely O'Dowd *Senior Associate*
Corporate

Cyber insurance

Melissa Tan *Special Counsel and*
Head of Cyber Insurance,
Insurance Law & Litigation

Louisa Henderson *Lawyer*
Insurance Law & Litigation



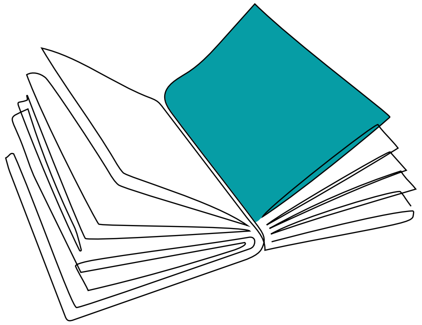
CASE NOTES

Notable cyber attacks

There was a dramatic increase in the frequency and severity of cyber attacks in 2021, with ransomware the predominant mode and COVID-19 continuing to prove difficult for organisations shifting to remote working and cloud-based services.

Learn more about each case study.

Learn more



Accellion

Dec 2020

- Supply chain attack
- Zero-day vulnerabilities
- Perpetrator: UNC2546 and UNC2582

Acer (Taiwan & India)

Mar 2021, Oct 2021

- Leveraging MS Exchange Server "zero-day" vulnerabilities
- Large ransom demanded
- Exposed poor cybersecurity practices and vulnerable servers
- Perpetrators: REvil and Desorden Group

Kaseya (US)

Jul 2021

- Supply chain attack
- Ransomware with malicious Sodinokibi / REvil code deployed
- US$70m demanded. Kaseya didn’t negotiate or pay
- Perpetrator: REvil, Yaroslav Vasinskyi

SolarWinds (US)

Dec 2020

- Supply chain attack
- Breach went undetected for months and could have exposed sensitive data in the highest reaches of US government
- Third-party claim led to shareholder class action
- Suspected: SVR

Nine Network (Aus)

Mar 2021

- Media network
- Malware attack with no ransom demanded
- Valuable sensitive data, disruption of services
- Perpetrator: unknown

Log4j2

Dec 2021

- Zero-day vulnerability
- Ransomware
- State-sponsored attacks

Microsoft Exchange Server (US)

Jan-Mar 2021

- MS Exchange Server zero-day vulnerabilities and patching
- Exploited by threat actors to launch cyber attacks
- Suspected: Hafnium and 9+ others

Facebook (US)

Apr 2021

- Social media platform
- Personal information exfiltrated
- Perpetrators unknown

Frontier Software / SA Government

Dec 2021

- Ransomware and supply chain attack
- State government impacted and employee data exfiltrated
- Suspected: Russian hackers

Florida water supply (US)

Feb 2021

- Critical infrastructure: water supply
- Hacker's attempt to poison water supply
- Perpetrator: unknown

Colonial Pipeline (US)

May 2021

- Critical infrastructure: oil and gas
- Ransomware attack
- Perpetrator: DarkSide, a RaaS provider
- US$4.4 million ransom paid (more than half was recovered)

CNA Financial (US)

Mar 2021

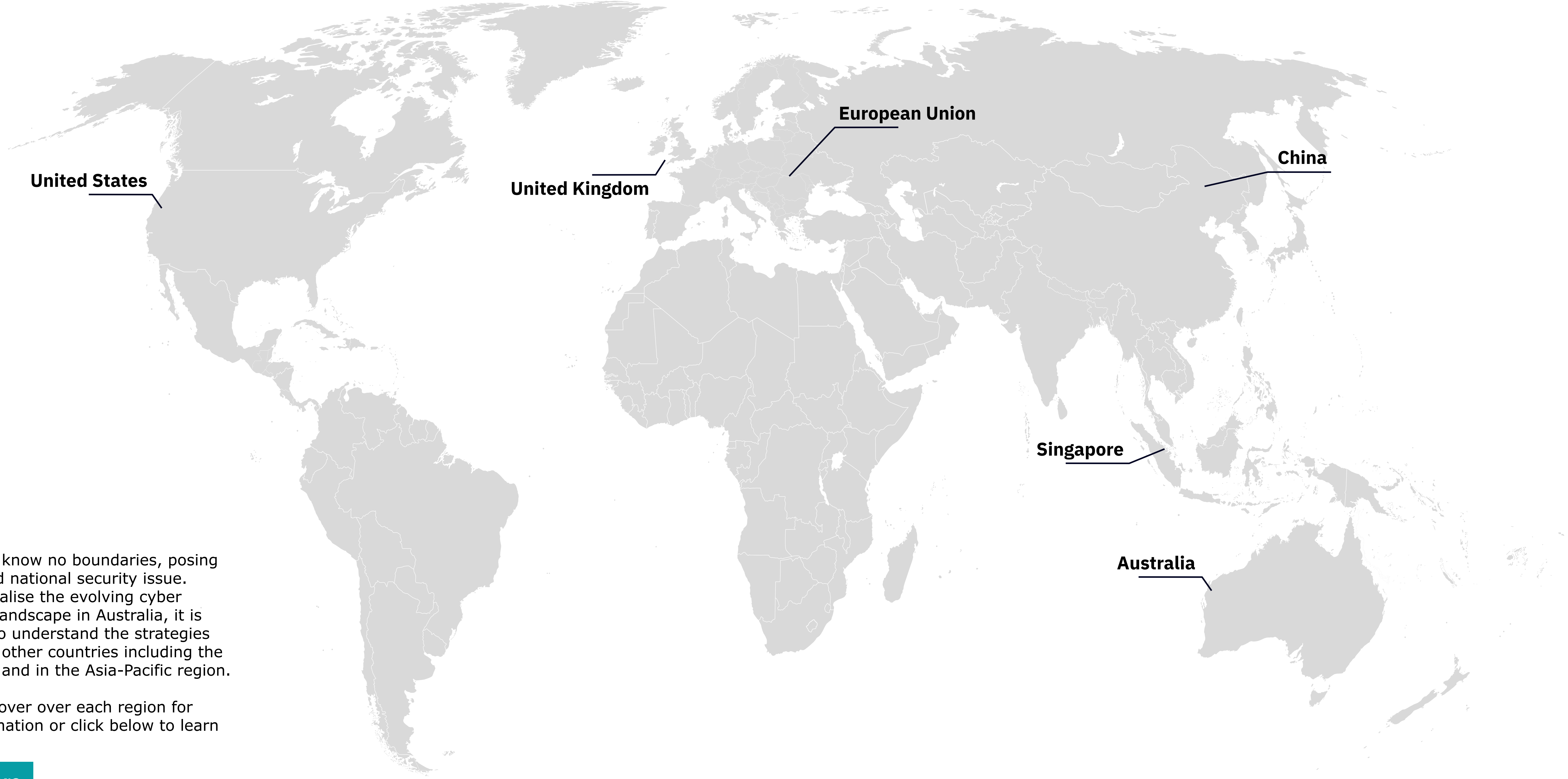
- Largest ransomware payout at US$40m
- One of the biggest US insurance companies
- Ransomware attack: Phoenix CryptoLocker encrypted remote workers' devices logged into VPN
- Suspected: Evil Corp

JBS Foods (Brazil, US, Aus)

May 2021

- Critical infrastructure: food and supply chain
- Ransomware attack
- Perpetrator unknown: REvil suspected
- US$11 million ransom paid

GLOBAL VIEW OF CYBER LANDSCAPE



Cyber risks know no boundaries, posing a global and national security issue.
To contextualise the evolving cyber regulatory landscape in Australia, it is important to understand the strategies adopted by other countries including the US, UK, EU and in the Asia-Pacific region.

Tool tip: Hover over each region for more information or click below to learn more.

Learn more

For added functionality, view this document with a PDF viewer like Adobe Acrobat.

TIMELINE

Legislation and policies

May 2021

Digital Economy Strategy
Sets out measures of success including enhanced security of critical services and infrastructure; high levels of cyber security across government; e-commerce and cyber security tool use for 95% of SMEs.

NSW Cybersecurity Strategy
Government to lead by example in cyber resilience.

Jun 2021

WA Govt Digital Strategy 2021-2025
Outlines focuses for improving cyber resilience, expanding secure service delivery, enhanced transparency and accountability in managing data.

NT Govt Darwin Joint Cyber Security Service
Collaborative hub between state and federal government.

Jul 2021

HGIT Initiative
Three Cyber Hub pilots established to provide cyber services for government agencies needing additional skills.

Aug 2021

Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth)
New law enforcement powers for Australian Federal Police and Australian Criminal Intelligence Commission to combat serious online crime.

Sep 2021

Vic Govt Cyber Strategy 2021
Sets out state's cyber security strategy for next five years.

Oct 2021

Ransomware Action Plan
Strategic government approach to tackling threat posed by ransomware.

Australian privacy law reform
Attorney-General's Department releases Privacy Act 1988 Discussion Paper and the Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021.

Strengthening Australia's cyber security regulations and incentives
143 submissions received to government consultation.

Cyber Security Skills Partnership Innovation Fund
Government announces additional $43.8 million in funding to grow cyber security workforce.

Dec 2021

Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Bill 2021 (Cth)
Bill receives royal assent. Government may issue sanctions directly against cyber hackers that ban them from visiting Australia or investing their criminal gains in Australia.

Security Legislation Amendment (Critical Infrastructure) Bill 2021
Bill receives royal assent. Aims to enhance security and resilience of critical infrastructure assets and systems of national significance.

Present

Jan 2022

Online Safety Act 2021 (Cth)
Act commences 23 January. First-of-its kind cyber scheme for adults; enhanced protections for children; greater transparency in tech.

HOT TOPIC

Insights from the Information Commissioner's investigations into Uber, 7-Eleven and Clearview AI

In 2021, the Office of the Australian Information Commissioner (OAIC) released three determinations in respect of its investigations into the privacy practices of Uber, 7-Eleven and Clearview AI.

Case study

Uber Technologies, Inc. & Uber B.V.

In Australia, Uber B.V. (UBV) is a ride hailing service delivered through a mobile application for Australian users. UBV has been operating in Australia and collecting customers' and drivers' personal information since September 2012. UBER Technologies Inc (UTI) was contracted by UBV to process information in accordance with UBV's instructions under a processing agreement.

In 2016 the personal data of drivers and customers was accessed by an unauthorised third party.

Learn more

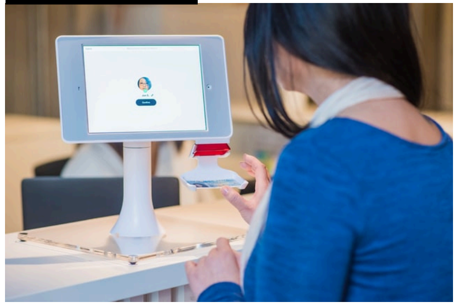
Case study

7-Eleven

7-Eleven is a private company with over 700 convenience stores across Australia. Between 15 June 2020 and 24 August 2021, 7-Eleven deployed a technology-enabled customer feedback mechanism in its stores. The mechanism used third-party facial recognition technology to collect facial images and faceprints of customers who completed a feedback survey using an instore tablet device. The facial images were retained for seven days and the faceprints were retained for an indefinite period.

Learn more

Case study



Clearview AI

American facial recognition company Clearview AI provides a facial recognition search tool for mobile and web users. The tool allows users to upload an image of an individual's face and search Clearview AI's database for likely matches, to enable identification of the individual.

Clearview AI's userbase comprises government and law enforcement entities who use the tool for law enforcement and national security purposes.

Learn more

TRENDS

Top four cyber security trends for 2022

Hover over the word cloud for more information or click here.

Breach Internet Password Data
Hacker Network Ransomware
Virus Online Cyber Malware Phishing
Training Attack security Privacy
Deep fake Software Cloud Information Detection
Firewall Legal Security Spyware
Insurance Crypto crime

BUILDING CYBER RESILIENCE

Lessons from 2021

There are four key cyber security lessons from 2021 to inform 2022 and beyond.

Learn more

1

The human factor

Work on reducing the cost of the human factor.

2

Cyber insurance

Cyber insurers and brokers can play an important role in building cyber resilience.

3

Collaboration

Information sharing is key.

4

Ecosystem

A collective approach is needed for cyber ecosystem strength.

KEY CONTACTS

Cyber security legal specialists

Technology, privacy and cyber

Lisa Fitzgerald
Partner
Corporate

D +61 3 9269 9103
E lfitzgerald@landers.com.au

Robert Neely
Partner
Corporate

D +61 2 8020 7704
E rneely@landers.com.au

Keely O'Dowd
Senior Associate
Corporate

D +61 3 9269 9526
E kodowd@landers.com.au

Cyber insurance

Melissa Tan
Special Counsel and
Head of Cyber Insurance,
Insurance Law & Litigation

D +61 2 8020 7889
E mtan@landers.com.au

Louisa Henderson
Lawyer
Insurance Law & Litigation

D +61 2 8020 7897
E lhenderson@landers.com.au

ABOUT US

Founded in 1946, Lander & Rogers is one of the few remaining truly independent Australian law firms and a leader in legal tech innovation.

With offices across the eastern seaboard of Australia, Lander & Rogers has grown organically resulting in a unified firm with a strong focus on client and staff care.

We believe legal services involve more than just the law – practical, commercial advice and exceptional client experience are equally important to our clients and to us.

Lander & Rogers advises corporate, government, not-for-profit and private clients in insurance law and litigation, family law, workplace relations & safety, real estate, corporate transactions, digital & technology and commercial disputes.

The firm is global in approach, working closely with a network of leading firms to provide advice to clients, both domestically and abroad. Lander & Rogers is also the exclusive Australian member of the world's leading independent network of law firms, TerraLex.

Melbourne	**Sydney**	**Brisbane**
T +61 3 9269 9000	**T** +61 2 8020 7700	**T** +61 7 3456 5000
F +61 3 9269 9001	**F** +61 2 8020 7701	**F** +61 7 3456 5001