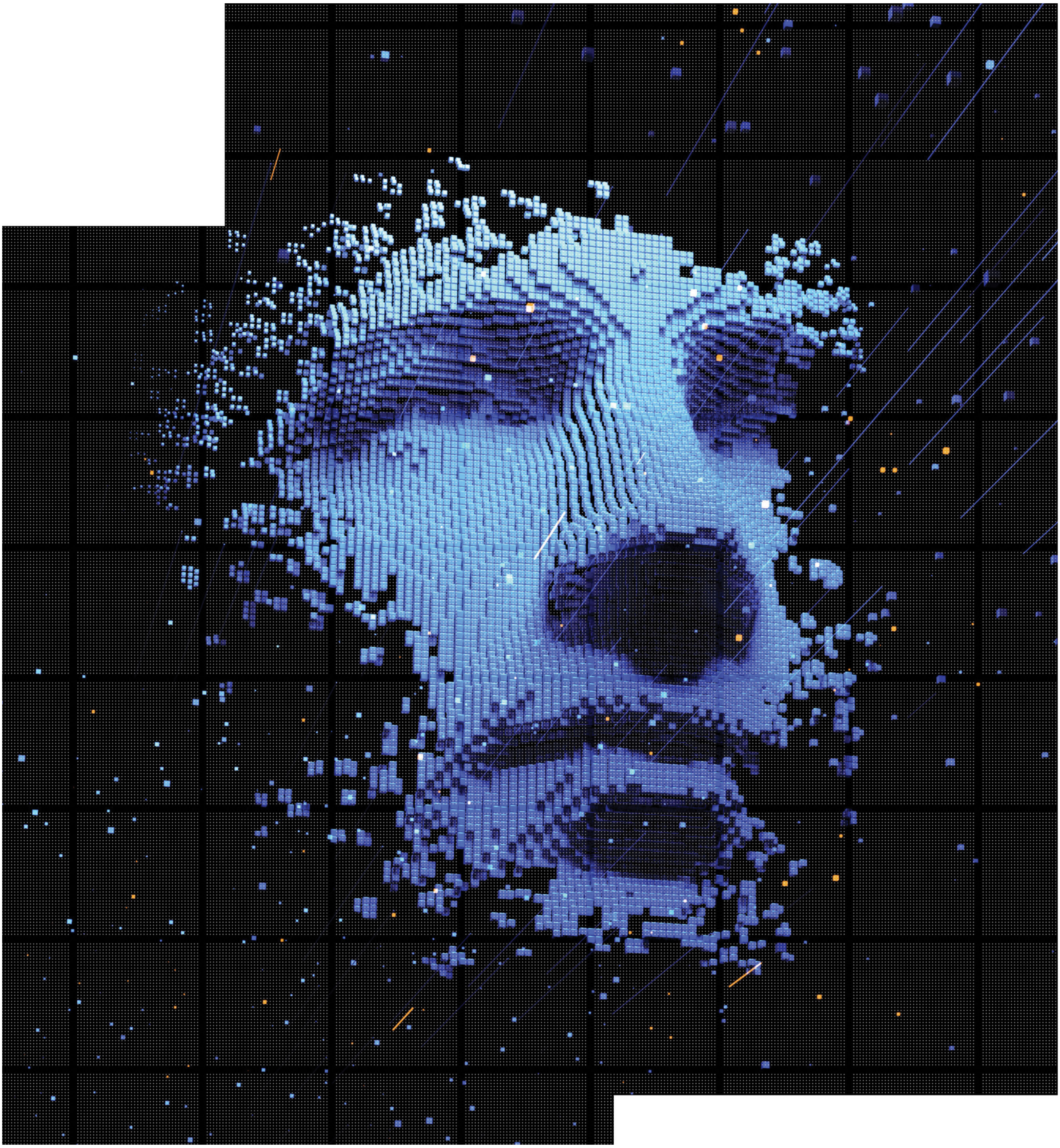


Cyber in 2023: evolving threats and resilience

January 2023

KordaMentha

2022 saw a significant increase in cybersecurity awareness across corporations and communities in Australia.

In the past 12 months, cyber attacks have accelerated, as forecast. These attacks have placed organisations in the spotlight and publicly challenged their reputations. Worst, they have impacted a large portion of Australia's population.

Cybercriminals pursued higher profile targets than before, peaking with headline-grabbing data breaches at Optus and Medibank. Combined, the two breaches impacted more than 10 million consumers, leaving the community with a lingering sense that these instances may only get worse.

As we predicted, 2022 saw greater momentum around the introduction and evolution of regulations and guidelines to foster and drive a national uplift in cyber defences across industries.

On the legal front, the Australian Securities and Investment Commission launched its first Federal Court action with a case alleging cybersecurity failures at financial institution RI Advice. It set a strong precedent in the Australian financial industry, adding further weight on the accountabilities of directors and corporate officers with regards to cybersecurity.

The Australian Institute of Company Directors, in collaboration with the Cyber Security Cooperative Research Centre, also established a benchmark for all businesses. publishing five cybersecurity governance principles and further reinforcing the accountability of board directors around cyber risks.

As those at the top came to terms with impending change, cybersecurity cemented a place among rock-solid career choices for both new job seekers and experienced workers seeking more promising roles in 'the great reshuffle'. Employee-driven data breaches – the 'human threat' – also became more apparent.

By the end of the 2021-22 financial year, The Australian Cyber Security Centre's annual figures showed cyber attacks having risen 13 per cent.[1] The 76,000-plus cybercrime reports equated to one every seven minutes, compared to one every eight minutes the year prior.

Heading into 2023, it is clear organisations will face new and more insidious methods of data theft, operational disruption and reputational damage. We predict threat actors to continue successfully exploiting the human element with the increased use of sophisticated means, including AI and deepfake technology. Critical infrastructure providers will be subject to further scrutiny in their cyber resilience, particularly in a degrading international and geopolitical order.

Following the legislation of increased penalties for companies that fail to protect customer data, privacy laws will be modernised in the coming year. A range of changes are expected that will provide citizens with greater privacy protection and corporations with a mandate to improve their data protection practices. We will also see changes around the protection and retention of client data as consumers demand greater transparency on how their personal information is handled.

01

Increased insider threats and vulnerabilities: the human element

Most cyber attacks exploit a human element. Typically, mistakes are made due to deficient awareness of cybersecurity. Organisational data breaches triggered by a phishing email, for example, are commonly due to an employee failing to recognise the threat, clicking a link and unwittingly handing control of an entire organisation's systems over to a hacker who then holds it to ransom.

However, we have also seen a rise in malicious threats instigated by internal stakeholders, such as a disgruntled employee or contractor. Now, organisations are pursuing more comprehensive security measures, including forensic data collection – and malicious perpetrators can expect to face new and severe punitive measures.

An emerging twist on the issue of insider threat is the rise of criminals now targeting employees via social engineering and identity-theft methods. These are often phone-based, involving SIM-swapping to facilitate account takeover. We have also seen threat actors accessing employees' personal email accounts at target organisations, paying employees, suppliers or business partners of target organisations for access to credentials and multi-factor authentication (MFA) approval and intruding in the ongoing crisis-communication calls of their targets.[2] One such group, Lapsus$, gained notoriety after a series of attacks against Microsoft and Samsung. Arrests were made, but the group re-appeared to launch an attack against Uber. These kinds of threats can be challenging to protect against and prepare for.

In 2023, senior executives also need to be far more aware of their heightened vulnerability when working outside the office on their personal devices and unsecured connections. The first line of defence in this area is education and awareness. Organisations now cannot ignore the importance of training staff, at all levels of seniority, in recognising potential cyber threats and vulnerabilities, particularly when dealing with sensitive organisational data. To be efficient, education and awareness programs must be underpinned by an effective cybersecurity culture.

The human element is playing a large part in driving the push for business leaders to be held further accountable for the cybersecurity of their organisations, and driving a maturation of cybersecurity governance across industries.

02

Critical infrastructure threat expands to Internet of Things

Cyber risks to critical infrastructure are well-documented – criminals disrupting delivery of vital services, such as electricity, water, oil or gas. In 2023, we will see further expansion of the playing field into both Operational Technology (OT) and Internet of Things (IoT) because of vulnerabilities being overlooked during product development.[3] There are an estimated 17 billion IoT devices in the world, from the basic – like home office printers and garage openers - to systems of a more critical nature, such as those in modern cars and medical systems. The growing problem is that virtually each one of those devices may present vulnerabilities that could be exploited.

Authorities worldwide are moving to regulate the area after several isolated incidents. One of the most notable cases last year involved a cybersecurity expert who found a way to remotely control the windows, horns and keyless driving systems of 25 Tesla electric vehicles across 13 countries.[4] Several years prior, a similar incident saw security researchers call attention to vulnerabilities in many new cars by revealing how they remotely commandeered the controls of a Jeep Cherokee to the degree that they could disable the brakes, and control the windshield wipers and radio.[5]

Now authorities are racing to get ahead of criminals. The European Union's cybersecurity regulations for cars came into effect in July last year,[6] but there are billions of other IoT devices with gaps to be identified and managed.

03

AI: the double-edged sword

AI can benefit society in a myriad of ways. Its capabilities have allowed machines to move far beyond basic number-crunching into decision-making tasks, paving the way for the development of self-driving cars and better fraud detection. AI is also now behind systems that provide mental health support, legal advice and aid in diagnosing disease. Cybersecurity is another prime beneficiary of AI with algorithms proving invaluable for detecting and responding to suspected incidents, identifying vulnerabilities and helping in identity verification.

No doubt 2023 will see a boom in AI applications and their benefits. Pitchbook reports investors poured at least $1.37 billion into generative-AI companies across 78 deals last year.[7] Also in 2022, Microsoft invested $3 billion in Open AI which designed ChatGPT, a model that interacts in a conversational manner and generates text in response to different prompts. Microsoft is now reportedly in talks to invest another $10 billion into OpenAI.

But as we know, good things can also turn bad. ChatGPT's ability to answer texts, generate content, translate languages and summarise text has already caused a stir in education worldwide simply because it allows students to cheat so easily. The University of Sydney is now citing 'generating content using artificial intelligence' as a means of cheating within its academic policy.[8] The positive potential of AI can also be leveraged for malicious purposes, and we expect to see more cybercriminals using powerful AI tools for ill-gotten gains. The ChatGPT example sounds a loud warning to corporate executives and the business world in general: AI means developing a new understanding of what it means to trust machines – or not.

The tech industry is also witnessing an increase in highly convincing AI-generated deepfakes – that is, synthetic media of a type that can fool almost anyone.[9] Experts are even warning of a 'deepfake apocalypse' on the horizon thanks to the kind of advances in generative AI we have detailed above. Over the next few years, it is forecast the internet will be flooded with forged videos and audio touting false information.[10]

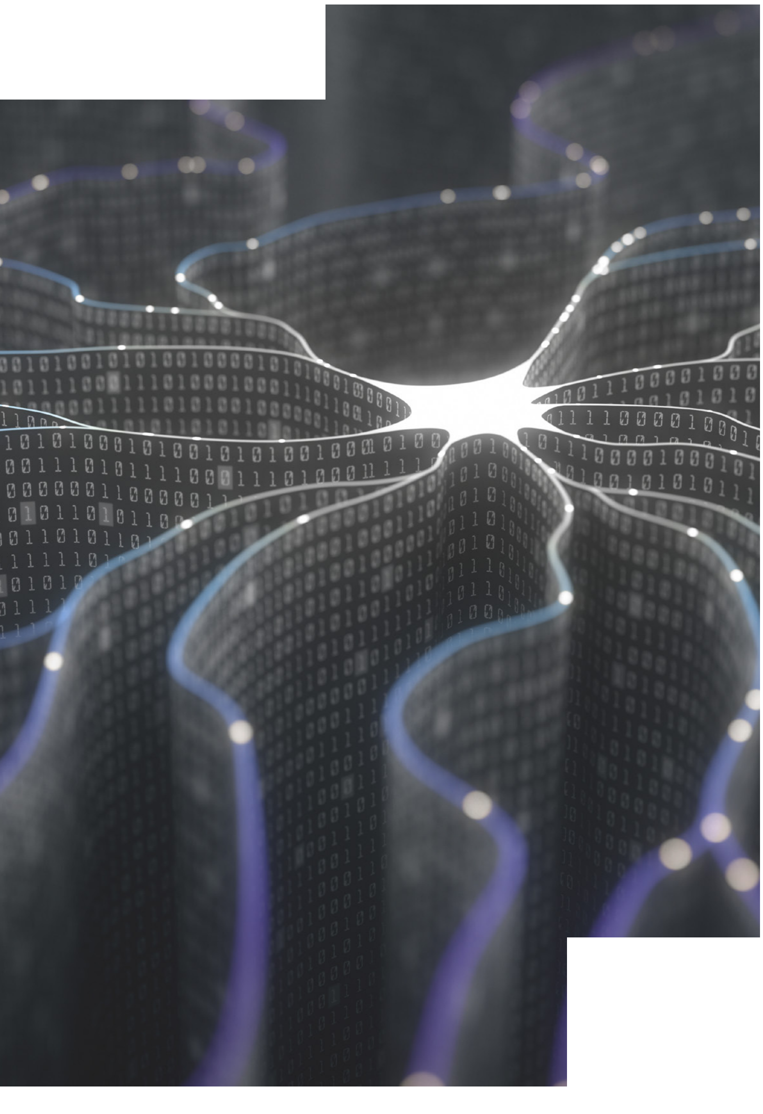
In 2023, organisations and their executives will be in the firing line as criminals attempt to dupe executives and others via deepfake technology that changes vocal tones and creates simulated video to impersonate colleagues or external business partners. These computer-generated videos and phone calls that look and sound like trusted individuals can be used to convince victims to execute an online task, as simple as sending an email, with disastrous consequences. Automated identity verification technology that can detect true human liveness and similar software will become one of the many vital parts of cybersecurity defence.

04

Prepare for rising cybercrime during economic downturns

It's a historical fact that crime rates rise during times of economic hardship. Criminals are more likely to keep moving online in 2023 as it provides them with greater anonymity and lower risk of capture. Punishments for cybercrime related convictions also remain relatively weak, despite the rise in regulations worldwide governing cybersecurity management.

At the same time, organisations need to prepare for the additional budgetary challenges that will be imposed on them as the regulatory environment becomes tighter. 2023 will see requirements for greater efficiency in managing cyber budgets.



05

Tougher privacy laws support the shift to data minimisation

In coming years, corporates will be facing the serious matter of dramatic increases in penalties for privacy breaches being proposed by the federal government.

The *Security Legislation Amendment (Critical Infrastructure) Bill 2021* has already ruled that owners of key infrastructure assets must notify the government as soon as a cybersecurity incident becomes apparent. In the case of a serious incident involving critical assets, such as water or electricity, the providers of these services must follow an extensive list of directions dictated by the Minister for Home Affairs.[11]

In response to high-profile cybercrimes, the Australian Parliament has passed key privacy reforms under the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022*. The legislation significantly increases penalties for serious and repeated privacy breaches – maximum penalties can now reach the greater of AUD 50 million, three times the benefit of a contravention or (where the benefit can't be determined) 30% of domestic turnover.[12]

A recent review of the Privacy Act has further led to proposals for greater penalties should an organisation be accused of allowing private client information to fall into the wrong hands.

This heightened attention around penalties has elevated the lucrative nature of data theft. As a result, we expect to see organisations moving to minimise the amount of data stored, along with more stringent rules and regulations around the collection, storage and destruction of private information. The Office of the Australian Information Commissioner and the federal government will be aggressively pursuing privacy breaches and turning up the heat on corporations to effectively protect the personal data of Australians.

In summary, 2023 is the year organisations need to be more cyber smart than ever, not only focussing on defence but also effective response. Cybersecurity resilience, harm reduction and reputational protection will need to be at the forefront of every organisation's mind in coming months.

Contact us

If you have any cybersecurity queries you would like to discuss, please contact:

Brendan Read
Partner | Brisbane

T: +61 7 3338 0254
E: bread@kordamentha.com

Guillaume Noé
Executive Director | Brisbane

T: +61 7 3338 0269
E: guillaume.noe@kordamentha.com

Tony Vizza
Executive Director | Sydney

T: +61 2 8257 3032
E: tvizza@kordamentha.com

References

1 Australian Cyber Security Centre, ACSC Annual Cyber Threat Report, July 2021 to June 2022 (November 4 2022) <https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022>

2 Microsoft, DEV-0537 criminal actor targeting organizations for data exfiltration and destruction (22 March 2022) <https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/>

3 Elizabeth MacBride, The dark web's criminal minds see IoT as the next big hacking prize (January 2023) CNBC <https://www.cnbc.com/2023/01/09/the-dark-webs-criminal-minds-see-iot-as-the-next-big-hacking-prize.html>

4 Grace Kay, A 19-year-old security researcher describes how he remotely hacked into over 25 Teslas (January 26 2022) Business Insider <https://www.businessinsider.com/teen-security-researcher-describes-how-he-hacked-into-25-teslas-2022-1>

5 Zach Guzman, Hackers remotely kill Jeep's engine on highway (July 21 2022) CNBC <https://www.cnbc.com/2015/07/21/hackers-remotely-kill-jeep-engine-on-highway.html>

6 UNECE, UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles (24 June 2020) <https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll>

7 Yolanda Redrup, Aussie VCs ready for the next tech boom: Generative AI (January 16 2023) Australian Financial Review <https://www.afr.com/technology/aussie-vcs-ready-for-the-next-tech-boom-generative-ai-20230112-p5cc7w>

8 Lauren Croft, 'Authentic' law school assessments to combat use of ChatGPT to cheat (23 January 2023) Lawyers Weekly <https://www.lawyersweekly.com.au/newlaw/36513-authenticlaw-school-assessments-to-combat-use-of-chatgpt-to-cheat>

9 Alice Cumming, 'Increase in very convincing AI-generated deepfakes' causing rise in fraud expert hires in 2023 (January 18 2023) Business Leader <https://www.businessleader.co.uk/increase-convincing-ai-generated-deepfakes-causing-fraud-expert-hires-2023/>

10 Matteo Wong, We Haven't Seen the Worst of Fake News (December 21 2022) The Atlantic <https://www.theatlantic.com/technology/archive/2022/12/deepfake-synthetic-mediatechnology-rise-disinformation/672519/>

11 Security Legislation Amendment (Critical Infrastructure) Bill 2021 (Cth)

12 The Hon Mark Dreyfus KC MP., 'Parliament approves Government's privacy penalty bill'(Media Release, 28 November 2022) 4 <https://ministers.ag.gov.au/media-centre/parliament-approves-governments-privacy-penalty-bill-28-11 2022#:~:text=The%20Privacy%20Legislation%20Amendment%20(Enforcement,the%20misuse%20of%20information%3B%20or>