News article

Jul 2024

Is Australia prepared for a catastrophic cyber event?: Forbes

ChatGPT, the metaverse, Web3 and the various manifestations that every technology company is throwing at consumers is leading to a black hole for our data.

Craig Archdeacon
Head of Cyber Assurance
Email craig.archdeacon@waterstons.com

Getty images

The internet grew up with no rules. There is no agreement anywhere among developers or users about system safety and security worldwide.

Accenture's ANZ Security Director, Jacqui Kernot, sees a problem with that.

"There's much more connection to the internet and technology systems, and that's happening across all industries," Kernot says in an interview with Forbes Australia.

"The resources industry, where a lot of the operational technology and the machines that do things, they've all got computers in them now. Even in your home … the dryer, the fridge …everything's online. While it means I can download a new cycle for my washing machine, which is fantastic, it ultimately means that it's all connected to the internet and can be accessed, changed, or controlled."

Kernot says one of the dynamics of the pandemic was that it "really industrialised cybercrime".

"A lot of people in developing countries were left without work, and the global economy shutting down in a way that it did cause many socio-economic problems. Becoming a cybercriminal is a great career path in many countries that don't have the opportunities we are lucky enough to have in Australia," she says.

Kernot explains that ransomware gangs are more professional and use a more commercial business model today.

"Everything's about making money, so they're much more professional because if you make a ransomware attack and then don't return people's data, the next target won't pay the ransom. They want to make sure people pay the ransom. If you like, we've really started making an industrial system out of it, and it's globally widespread."

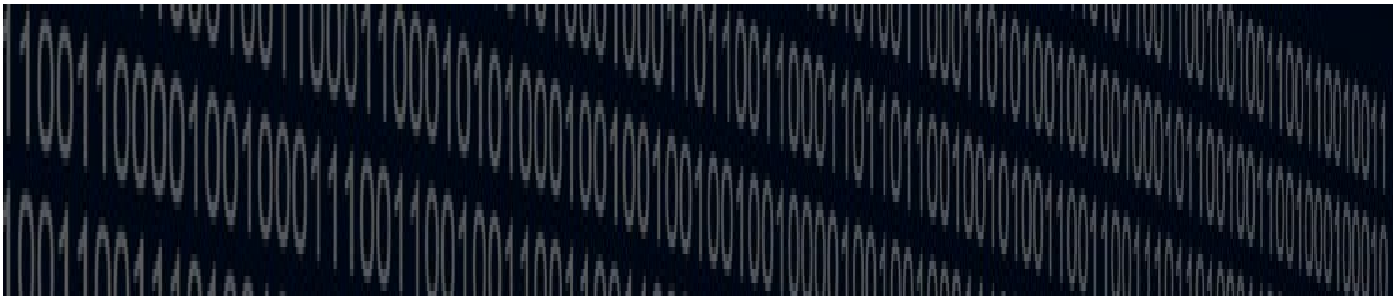
Kernot says, "The internet grew up without any rules. Traffic has rules and roads have rules, and countries have governments. The internet covers all countries. There's no agreed-on system or regulation for safety or security. That's starting to be looked at now. We've got all these systems connected to everything that don't have any regulations or rules and no consistent rules across countries and governments. And a huge cybercrime problem."

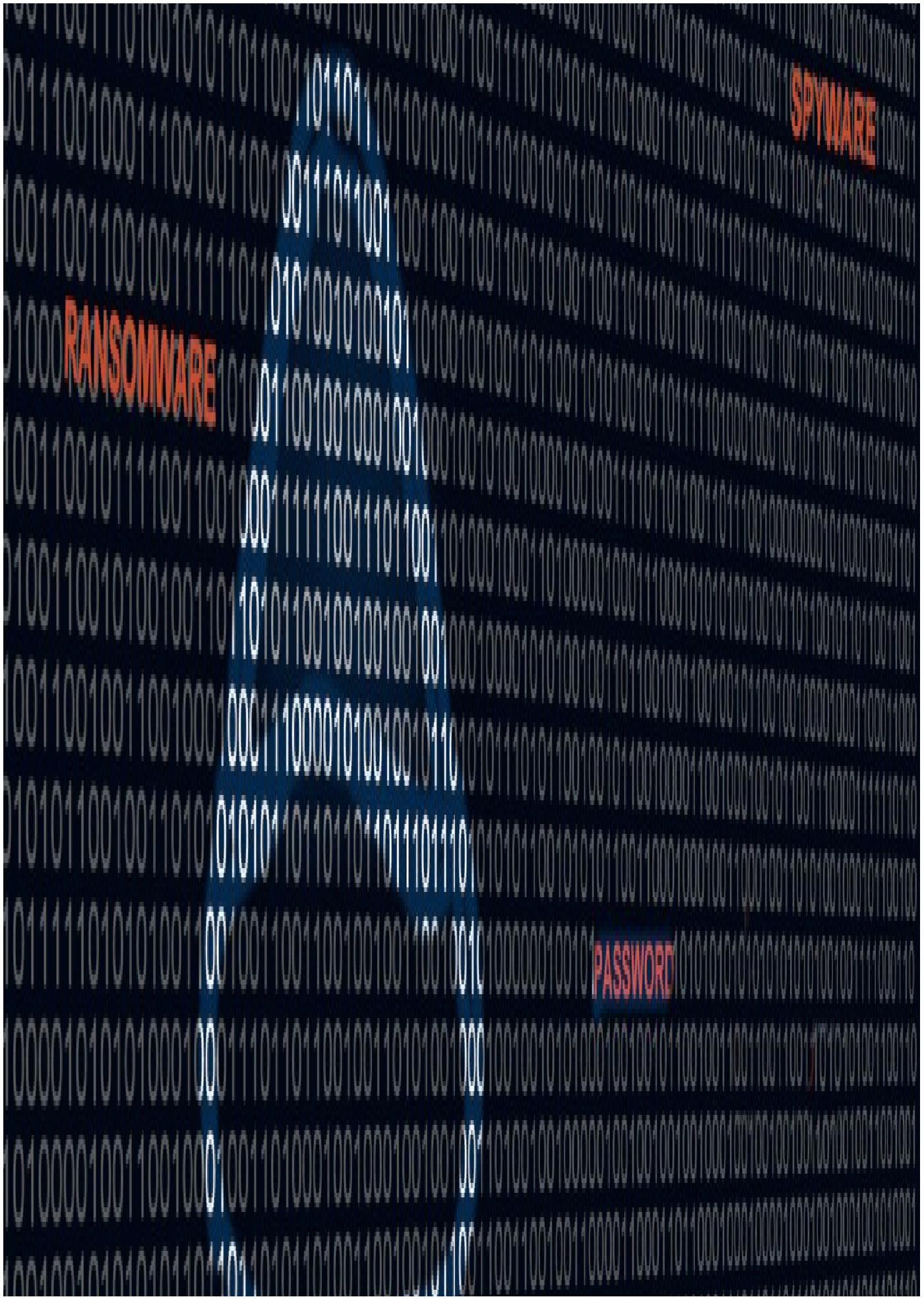
Kernot says the more things we connect, the more likely we can bring them down if they're subject to attack – a catastrophic cyber event. Geopolitical instability, such as the conflict in Ukraine, the impact of the recession and the post-Covid era "all create a bit of a perfect storm" without any actual rules or regulations or a way to apply cybersecurity and safety globally across the world consistently.

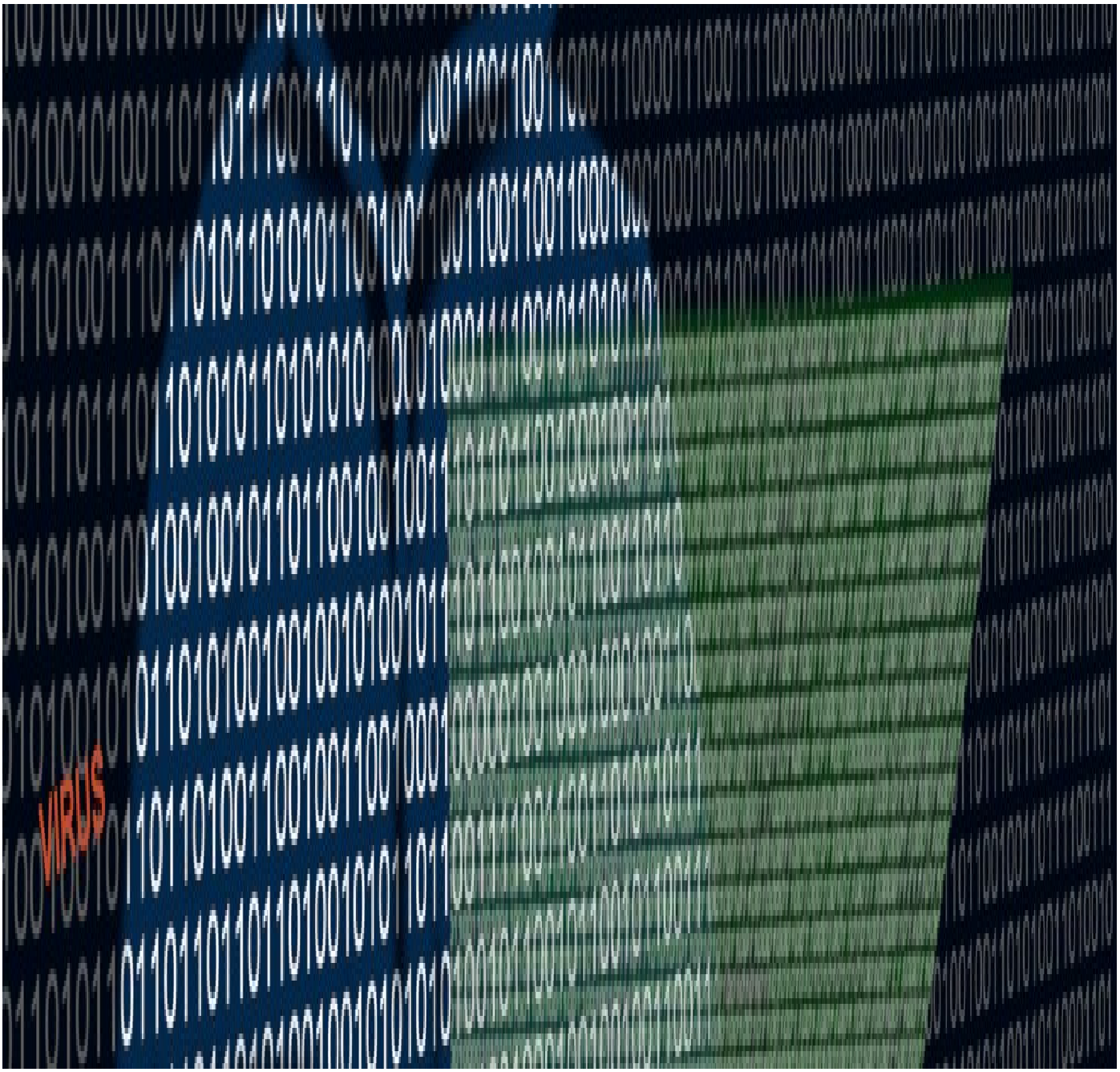
2022 showed things need to change

In 2022, Australians saw many big names in industry and government become targets for cyber attacks. The Australian Cyber Security Centre received over 76,000 reports of cybercrimes in the 2021-22 financial year, an increase of nearly 13% from the previous financial year. As a result, everyday Australians lost a staggering $98 million, says Michael Horton, Executive Vice President & Country Manager, Australia and New Zealand at HCLTech.

"These breaches present serious issues for the protection of Australian citizens' data, Australian customers' confidence in online services and products, and for businesses themselves who now face significant reputational damage and potential fines of $50 million or more," says Horton.




SPYWARE
RANSOMWARE
PASSWORD



Getty Images

"One of the widespread problems in Australia is the talent shortage in the IT and cybersecurity sectors. Put simply, if there's a shortage of expertise, there will be security gaps that can be exploited. There is currently a shortage of thousands of cybersecurity experts across Australia and New Zealand, which is forecast to only worsen over the coming years."

Horton says that ongoing government reform on cyber security and data collection, like the recent review of the Privacy Act, is a step in the right direction. Still, cyberattacks don't typically happen due to a single point of failure, more from the failure of an entire security system.

He says that extensive upgrades to a business's digital infrastructure are essential to enhancing a business's cybersecurity and mitigating risk. Still, there is no single quick fix for these attacks. Instead, Australians, industries, and governments must implement significant changes to reduce their susceptibility to cybercrime.

The Tenable 2022 Threat Landscape Report revealed 2.29 billion records were exposed worldwide in 2022. The Exposure Management company's Security Response Team analysed 1,335 breach data incidents publicly disclosed between November 2021 and October 2022. The report says 68% of the exposed records were in the APAC region, and 31% at organisations in North America, Europe, the Middle East and Africa combined.

Businesses need to prepare to respond to incidents

The Forecast 2023 McGrathNicol report found that 69% of Australian businesses have experienced a ransomware attack in the past five years.

The increasing prevalence of cyber-attacks has highlighted the need for businesses to better prepare for and plan a response to such incidents, says McGrathNicol Cyber Partner Shane Bell.

"With increased regulatory oversight and legislation being introduced by the federal government, Australian organisations will need to develop robust cyber programs to address cyber risk. A key component of any cyber program must be developing a rapid incident response plan – and regular testing of this – to ensure that an organisation can effectively respond to a cyber attack when it does occur," he says in the report.

"There is a growing expectation for organisations to demonstrate high cyber security readiness. By conducting regular vulnerability assessments and penetration testing, as well as implementing security controls such as firewalls, Endpoint Detection and Response (EDR), and continuous monitoring and detection of abnormal behaviour, organisations can significantly reduce the risk of becoming another cyber statistic in 2023."

Nefarious means

Jonathan Jackson, Director of Engineering, APAC & Japan at BlackBerry, notes that Australia is well known as a nation of early adopters – and like any new technology, conversational AI bots like ChatGPT are being tested by different industries and individuals for all kinds of purposes.

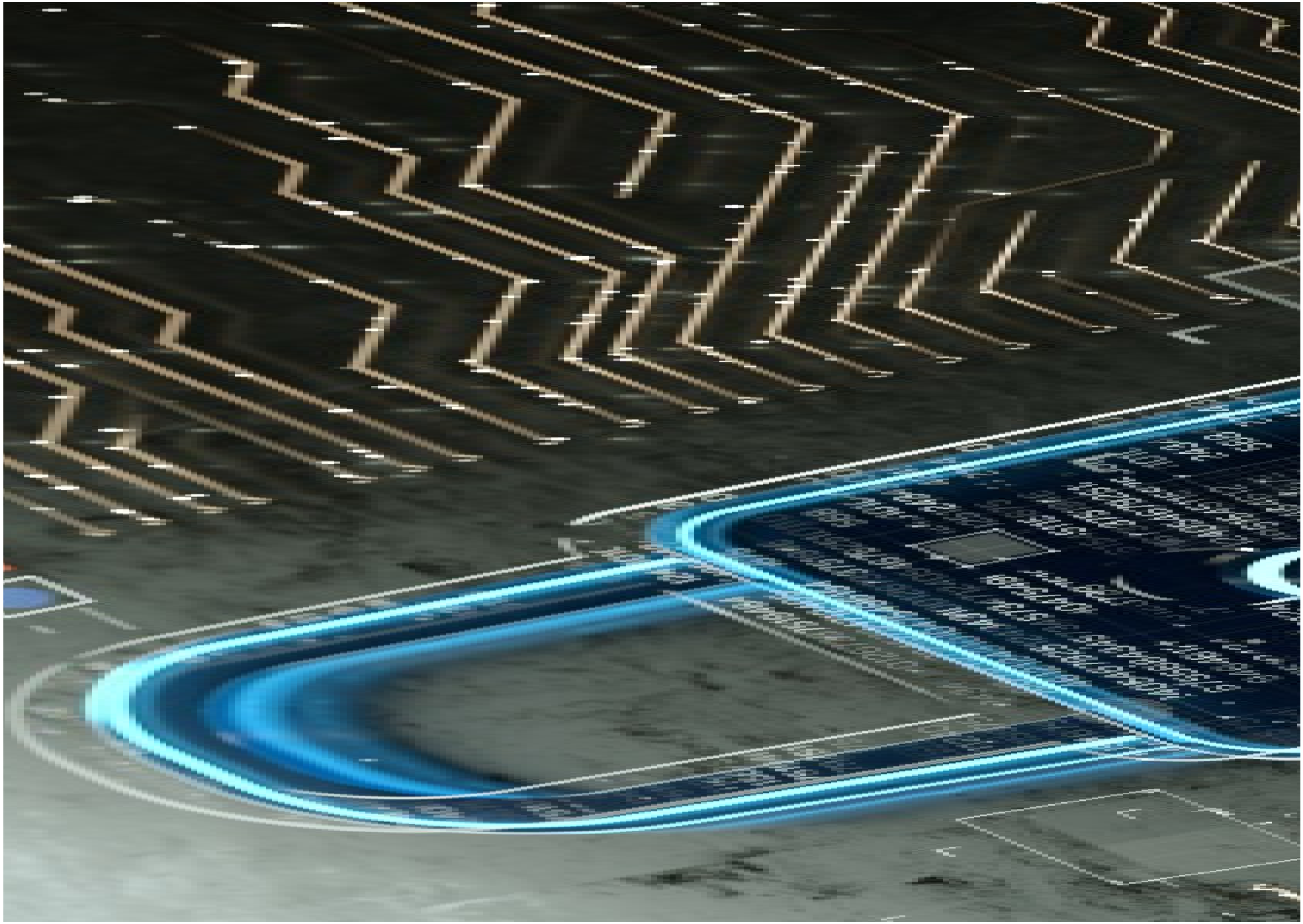
"However, at BlackBerry, we know hackers are also testing it for nefarious means. More than half of Australian IT directors we recently surveyed believe that we are less than a year away from the first successful ChatGPT cyberattack in Australia. With Microsoft now fusing ChatGPT-like technology into their search engine Bing and the launch of Google Bard, such fast-paced innovation will enhance how we work, live and learn – however it also indicates the threat of an AI cyberattack isn't far away.

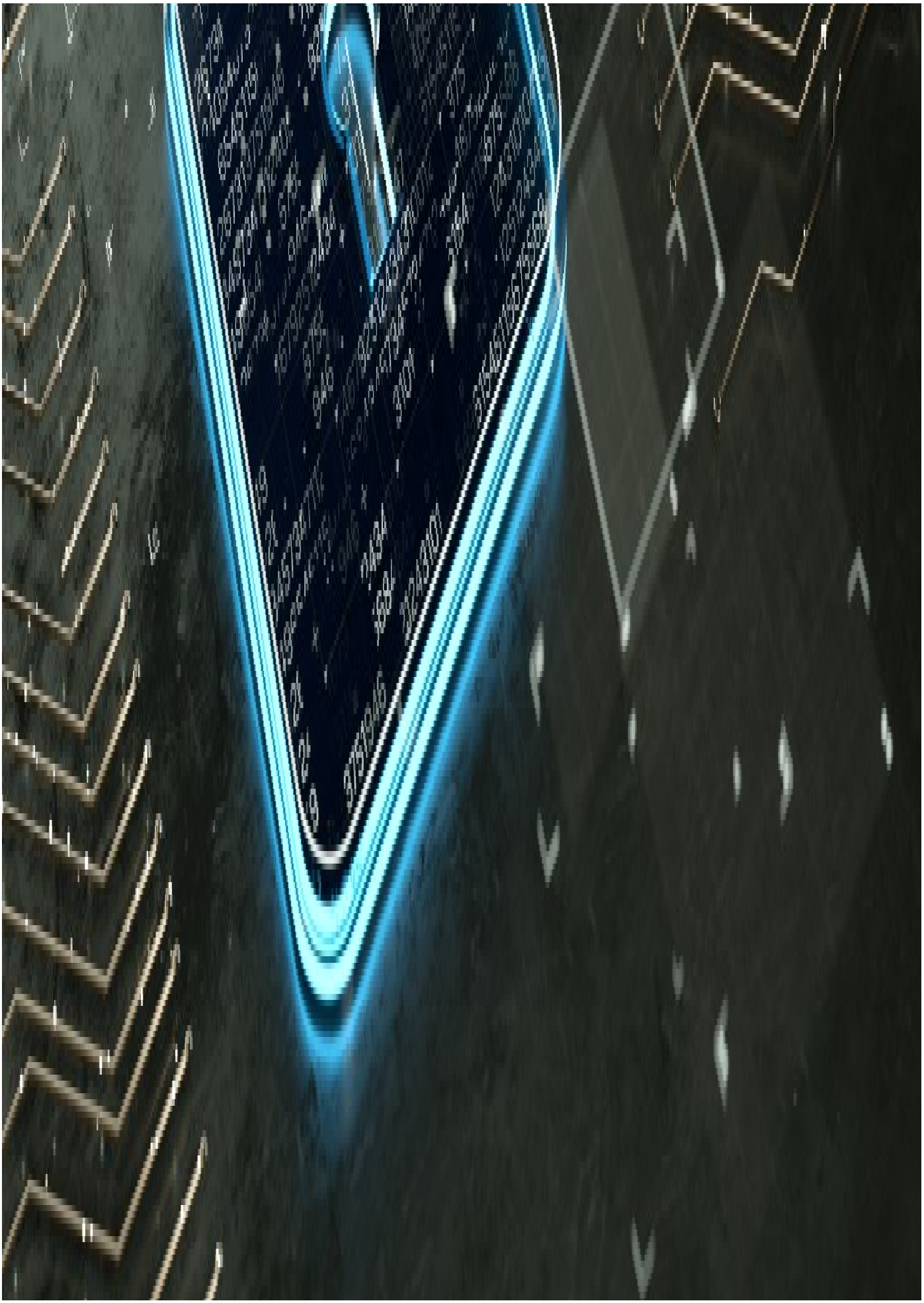
"AI is fast-tracking practical knowledge mining, but the same is true for malware coders. The ever-evolving cybersecurity industry is often likened to a never-ending cat-and-mouse or whack-a-mole game where the bad guys keep popping up. In the past, these bad actors relied on their experience, forums, and security researcher blog posts to understand different malicious techniques and convert them into code. Still, advanced programs like ChatGPT have given them another arrow in their quiver to test their efficacy to wreak digital havoc."

Jackson says AI can be used in several ways to carry out cyberattacks, like automated scanning for vulnerabilities and new attack techniques. AI can also create convincing phishing emails, text messages, and social media posts to trick people into providing sensitive information or installing malware. AI-generated deep fake videos can be used to impersonate officials or organisations in phishing attacks.

"The growing use of AI in developing new threats makes it even more critical to stay one step ahead by using 'good' AI to fight threats on the offensive. Organisations must continue to focus on improving prevention and detection. This is a good opportunity to look at how to include more AI in different threat classification processes and cybersecurity strategies."

Jackson notes that one of the key advantages of using AI in cybersecurity is its ability to identify anomalies and threats in the telemetry of vast data sets, like a needle in a massive haystack. The sheer volume of data generated by modern networks and tools makes it impossible for humans to keep up. He says AI can vectorise and contextualise data much faster, making it more efficient at identifying threats.





Getty Images

Humans are ‘the most vulnerable point of exploitation’

Gartner predicts that by 2025, lack of talent or human failure will be responsible for over half of significant cyber incidents. The number of cyber and social engineering attacks against people is spiking as threat actors increasingly see humans as the most vulnerable point of exploitation.

A Gartner survey conducted in May and June 2022 among 1,310 employees revealed that 69% had bypassed their organisation’s cybersecurity guidance in the past 12 months. In the survey, 74% of employees said they would bypass cybersecurity guidance if it helped them or their team achieve a business objective.

“Friction that slows down employees and leads to insecure behaviour is a significant driver of insider risk,” says Paul Furtado, VP Analyst, Gartner.

To confront this rising threat, Gartner predicts that half of the medium to large enterprises will adopt formal programs to manage insider risk by 2025, up from 10% today. A focused insider risk management program should proactively and predictively identify behaviours that may result in the potential exfiltration of corporate assets or other damaging actions and provide corrective guidance, not punishment.

“CISOs must increasingly consider insider risk when developing a cybersecurity program,” says Furtado. “Traditional cybersecurity tools have limited visibility into threats from within.”

KnowBe4’s Jacqueline Jayne, a security awareness advocate, says customers impacted by a data breach need to realise that the likelihood that they will become a target of social engineers increases significantly. Victims of any data loss should be very cautious regarding future communications and pay close attention to any links in messages or requests for more information, Jayne says.

But what if it’s not you, it’s your building

Cyber security must be a part of the conversation at every step as smart buildings get smarter – and older buildings are retrofitted with the latest technology.

Ryan O’Kell, Head of Cyber Security at Waterstons, recently scoped the Australian IP Address space and identified 5,956 Building Management Systems open to the broader internet.

While this does not necessarily present an immediate risk, the bigger picture is that 5,956 buildings have their entire management system accessible from anywhere in the world with an internet connection. If just one of those is misconfigured or is missing vendor security patches, it represents an entire building's system that can be manipulated by anyone with an internet connection anywhere in the world, he says.

A white paper by Waterstons and Cundall reveals the downfalls of cyber security in the industry and highlights the importance and vital role boards play, the essential role humans play, and the next steps to secure the industry. Cundall Partner Julian Sutherland says getting cyber security settings right is essential to ensure business processes and asset performance are always protected.

Thanks for partnering with us on this article, Is Australia prepared for a catastrophic cyber event? - Forbes Australia