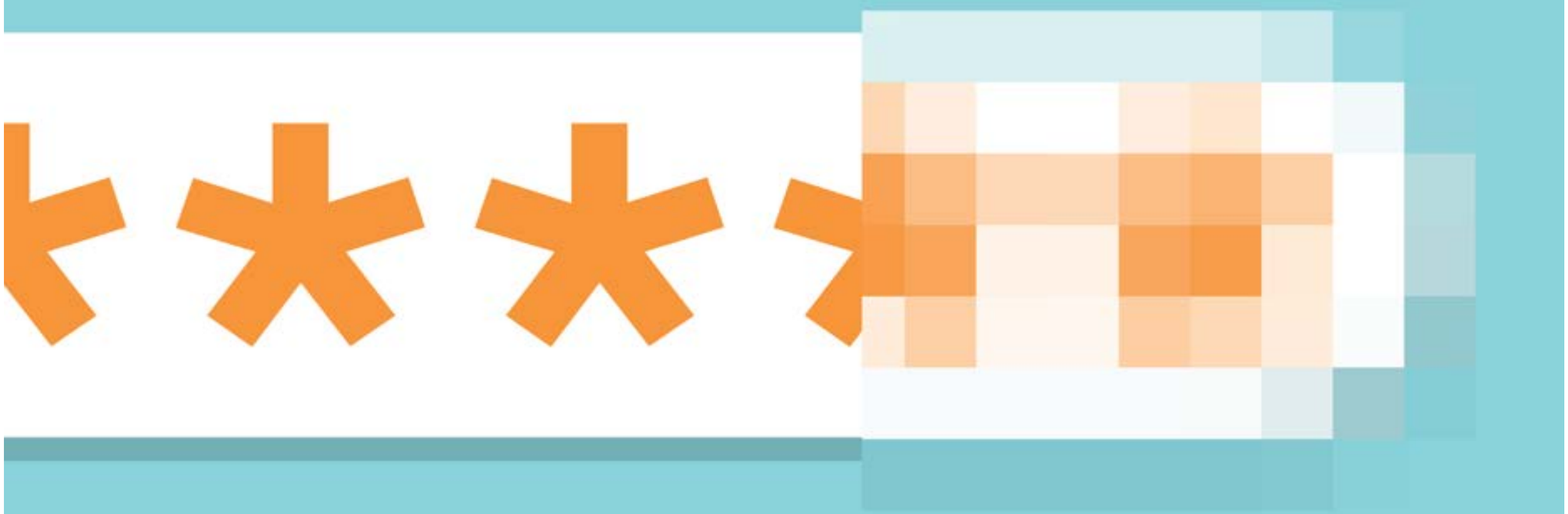
Six experts take us through the threats and opportunities facing us right now, in the next decade and beyond. Story by Jane Nicholls



The future of cybersecurity

The conversation is shifting

"Cybersecurity is an unhelpful term because as soon as you say it you enter this technical domain," says Hamish Hansford, deputy secretary at the Department of Home Affairs' Cyber and Infrastructure Security Centre. "Digital infrastructure and digital resilience are more powerful terms." He says making cybersecurity mainstream signals that it's an individual's job to be responsible for the security of their digital life – and for leaders and boards to stop delegating responsibility to IT teams.

Hansford says chief information security officers (CISOs) and CTOs have an important role in "reframing the view of the world", beginning with plain English conversations. "I see CISOs go to their board or CEO and say, 'We need $5 million for two-factor authentication for our new system', and they're just not speaking the same language. A better way to approach it is to say, 'I know we want to deploy this new technology. If we invest $5 million to make the product more secure I reckon we can make the company $100 million because it will build trust and make us more successful.'"

Being proactive will always be the golden rule for cybersecurity. "The most important thing is to make sure you're prepared," says John Baird, CEO of cybersecurity services firm Revio, but "prepared" doesn't necessarily mean spending a fortune on new security tech. "You should be figuring out your cybersecurity roadmap for the next 10 years, knowing it's going to change.

"Too many companies treat cybersecurity as a project: 'I'll buy this piece of software, deploy it, tick that box and there you go, we're safe.' But you're dealing with real-world adversaries who can spin on a dime and any defences you put up they will immediately start trying to find ways around them. It's about building a program of managing cybersecurity at the board level and the senior executive level for the long term. It's a forever problem."

Trust is on the way out

"Organisations and nations are moving to zero-trust architecture and by 2050 that will be the default security model embedded in all digital systems," says Mary Attard, security practice lead for Accenture Australia and New Zealand. Zero trust requires continuous real-time verification and assumes users inside and outside networks are untrustworthy until proven otherwise.

It also sets up systems on "least-privilege methodology", the digital version of "on a need-to-know basis". Access to company networks is becoming less like wandering around a food court and more like the slamming doors in the opening credits of 1960s secret-agent TV series *Get Smart*, with only a few permitted to go further than the lobby.

Attard says this is important for individuals, too. In the aftermath of numerous hacks exposing our precious stored personal data to cyber criminals, we're moving to digital credentials that can be shared with a verified source when they require it.

"Digital credentials prevent the over-sharing of information on paper forms," she says. "The ownership of our identity is going to come back to the individual and that's exciting. You'll have a digital wallet with credentials to share at border control, almost like a tap-on tap-off system that verifies who you are without having to fill in your date of birth on a piece of paper that heads off somewhere and you don't control where it goes."

Staying one step ahead

Backups are your best friend in the event of a ransomware attack. Revio's John Baird has been helping clients to apply them in a novel way. "We've just built a financial services firm's system from scratch, using what's known as infrastructure as code [IaC]," he says. "What once would have been a physical server is now a virtual machine in the cloud. You write a set of code to define the machine, how big it is, its memory, processor, how the network works, operating system. When you run that code it builds the machine to your specifications and sets up the software using an image that's offline not doing anything. It's a frozen image so hackers can't attack it."

The bones and muscles of a computing system are spun in the cloud following this code, recreating it on command. Then comes the alchemy – the virtual body is reattached to the virtual brain, the data that brings it to life. "Think about it like this: a computer has two sets of data. One gives it an identity, tells it what it is, how it works and what it's to do. The other one is the data set that it uses to do all of that." Separated, the "body" and the "brain" aren't much use to anyone, which enhances security.

Once the IaC was up and running for Revio's client, they realised they could delete the "body" of the system each night. "They delete half their machines and don't have to pay for the cloud storage overnight. An hour before they start in the morning they run the script, build the machine and attach it to the data storage. When they finish for the day, they throw it out – if it was infected, they've just blown that away."

Tech is catching up with sci-fi

The more we adopt connected devices – the Internet of Things or IoT – the greater our vulnerability becomes. Earlier this year, legislation was passed that required minimum security standards for connected devices under the federal government's Cyber Security Act. The standards come into effect in March next year and will continue to be updated.

The risks will only continue to ramp up around technologies such as driverless cars. "What security do we have that a threat actor can't go in and disable the vehicle?" says Sally-Ann Williams, CEO of leading tech incubator Cicada Innovations.

"We don't talk enough about supply-chain vulnerability and where there could be leakages in the devices we use and the services we procure. It's everything from mobile devices to transportation and at a nation-state level, we need to be looking at where we procure our satellite services, too."

This clear and present danger has the potential to inflict harm well into the future. What liabilities lurk in the technology that's critical to a mass-transit system, manufacturing line or operating theatre? With multiple components sourced from third-party vendors, the risk only grows.

"It becomes really complex because you're going down layer upon layer upon layer – nobody builds everything end-to-end themselves," says Williams, who spent almost 13 years with Google earlier in her career.

"There's potential vulnerability in that entire hardware physical stack, the software layer and the human behaviour layer – that's what we should be thinking about right now. Corporate Australia has to understand its supply chain because it goes across every single sector and I don't think we have a good handle on how much of that is in the private sector and how much of it is reliant on other countries. It's a new geopolitical risk."

New-wave security challenges

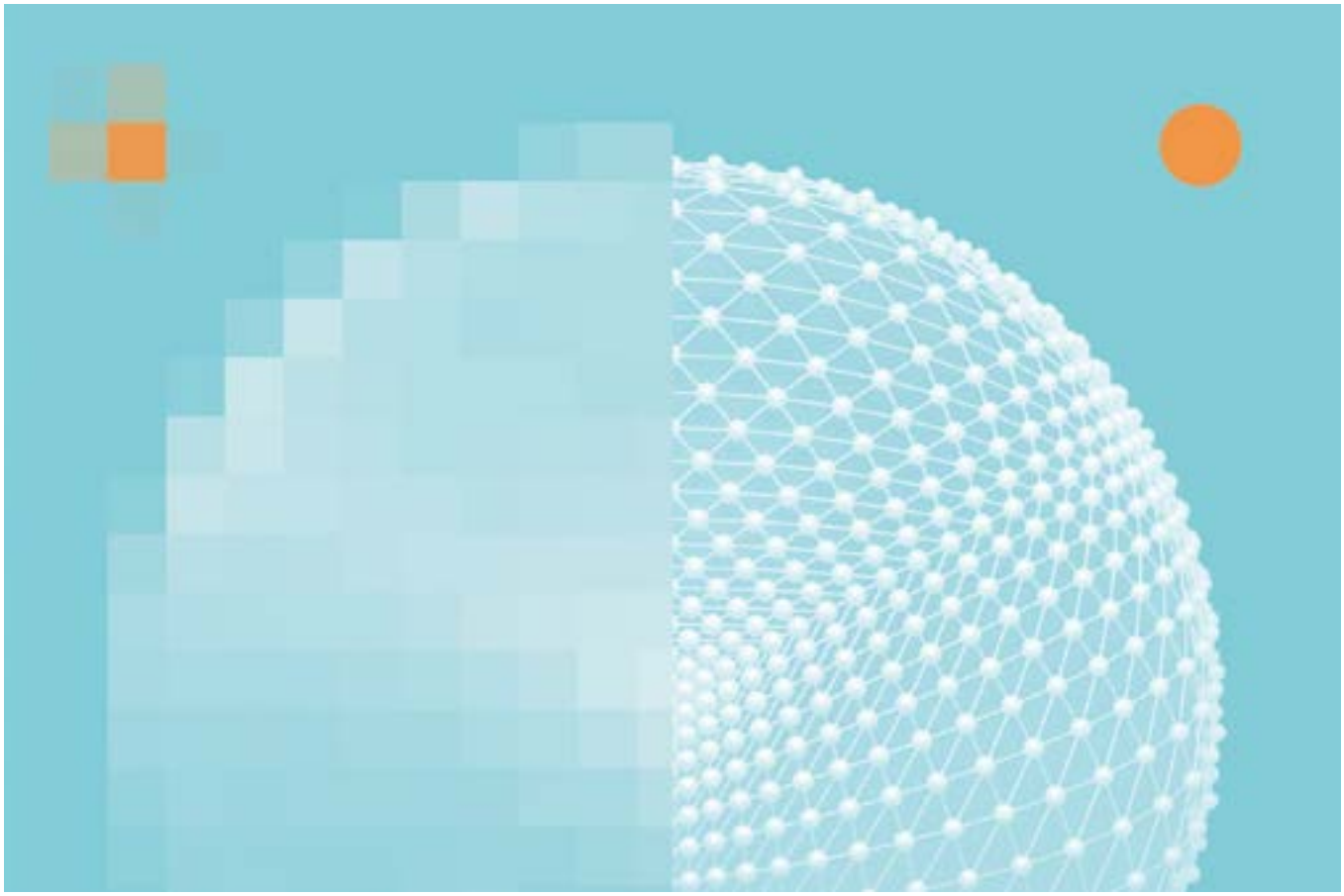
"Everybody gets really concerned about AI but it's still pretty dumb," says Williams. "What happens when it gets to the generative level, where it can self-perpetuate, grow and learn, and get the ability to attack and take down infrastructure and assets?

"Right now AI is such a resource-intensive effort that the truly incredible powers are held by a few actors while most of us use it for efficiency applications. It's an inverse curve: as AI becomes much more prevalent, accessible, less energy-dense and the cost comes down, the capability of the average user will increase and the potential for more people to disrupt things from their backyard goes up. Whenever we have more people doing things, the propensity to do bad is greater."

And not just on Earth. Williams sees the increasingly crowded frontier of space technology as a cyber risk that's coming in hot. "There are so many privately held capabilities and satellites up in space now, many owned by very wealthy individuals. What are the unintended consequences of that?" she asks. "Space is so critical to communications and service delivery but what governance and controls are held around those things?"

Cicada Innovations runs the annual Tech23 event, which showcases Australia's most promising deep-tech startups. Working with these inspiring innovations and those being developed at Cicada itself gives Williams a glimpse of future risks. "We've got a couple of companies looking at brain-computer interfaces. What happens if that technology becomes widely adopted?"

The manufacture of connected medical devices such as pacemakers is already being monitored by regulators. In 2022, Australia's Therapeutic Goods Administration released guidance for the industry, concerned about medical devices being hacked to steal patient data or cause harm.



Quantum risk is already here

The power of quantum computing comes from doing everything everywhere all at once. While still in the early stages of development, it's on track to solving previously intractable problems across a range of industries. But in the wrong hands, it could wreak havoc on existing cybersecurity defences.

There remain myriad technical issues to overcome in order to scale quantum computing and it will be the 2030s or beyond before it's broadly accessible but it looms on the horizon as a massive cybersecurity timebomb, with the potential to break existing cryptography algorithms. While that's years off, Associate Professor Sushmita Ruj from the School of Computer Science and Engineering at UNSW in Sydney says that hackers are already stealing and stockpiling encrypted data in anticipation. "It's known as 'harvest now, decrypt later'."

That's why the time to start securing data using post-quantum cryptography (PQC) is now. "The magic of maths is able to secure data. We don't need quantum computers to structure algorithms that can withstand attacks from quantum computing," says Ruj, who leads UNSW's quantum safety project. "Wherever your organisation is using classical cryptography you need to convert to PQC. And things are happening already – NIST, the National Institute for Standards and Technology in the United States, has been standardising post-quantum cryptographic algorithms."

Many software and cloud service providers are working with NIST to support the development and adoption of PQC algorithms and governments around the world are rolling out new compliance regulations. The problem is identifying where quantum-vulnerable cryptography algorithms are placed in a system. Alexey Bocharnikov, director of cybersecurity strategy and regional leader for quantum security at Accenture, shares a metaphor he heard at a recent cybersecurity conference. "Think of the cryptographic algorithms as nails you use to build your house. Over time some of those nails have become rusty and need to be changed," he says.

"But you have nails all over your house and because you can't see most of them, you don't know where the strong ones are and where the ones that require replacement with new rust-resistant nails are."

Bocharnikov says that massive computational resources are required to adopt these new PQC algorithms. "That's why organisations started on this journey even before the new standards came into play – because you can't do it overnight."