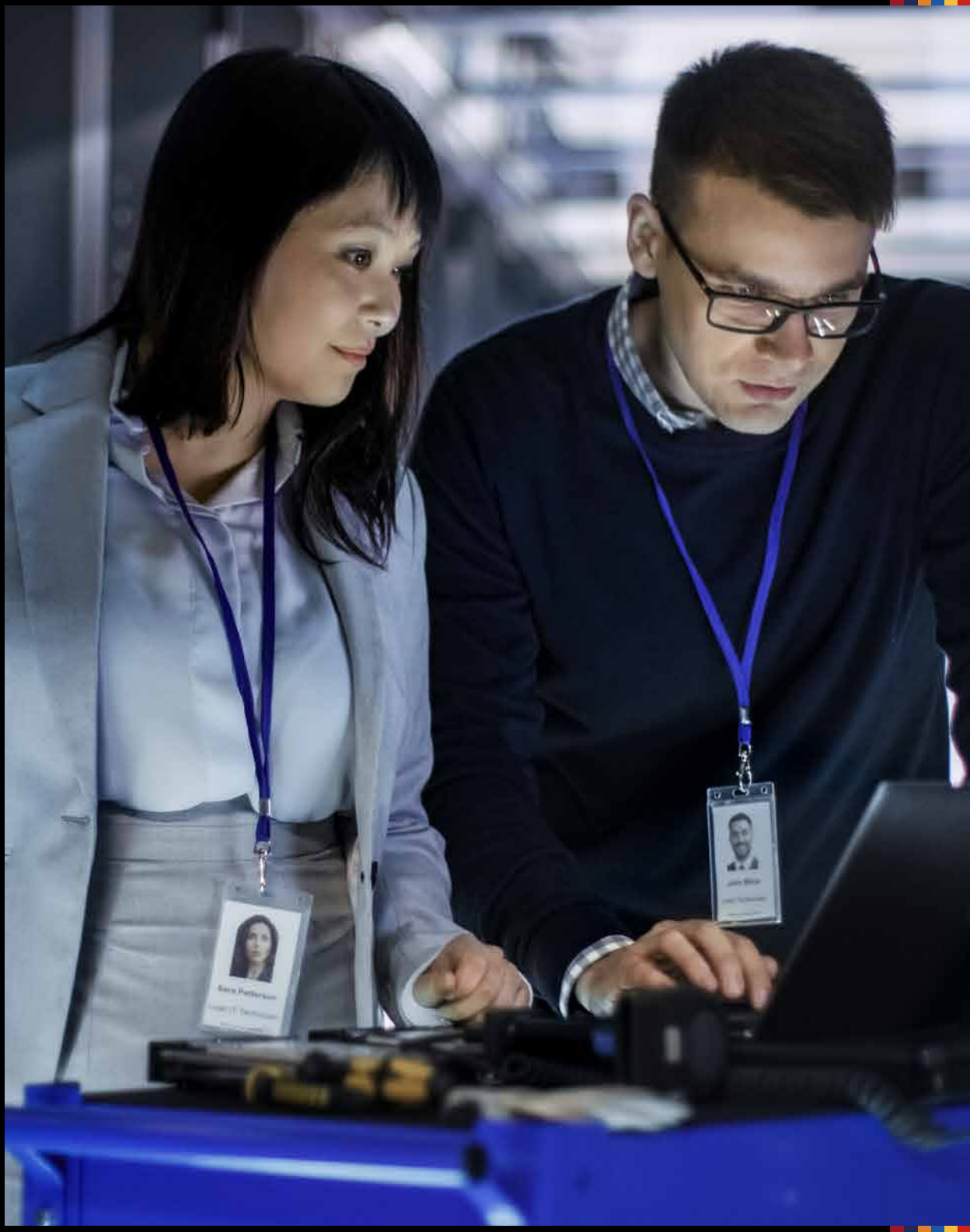
INFORMATION**AGE**

CYBER SECURITY EXPERTS SERIES




For details on how to become
an ACS Certified Professional
(Cyber Security), visit acs.org.au.
Shift

Andrew Johnson

Foreword

"A strong cyber security ecosystem is a mandatory pre-requisite for continued economic growth."

The 2017 and 2018 editions of Australia's Digital Pulse highlighted the tremendous opportunities enabled by technology, with digital technologies forecast to be worth $139 billion to the Australian economy in 2020 – equating to seven per cent of GDP.

Further adoption of digital technologies could add an extra $66 billion to Australia's GDP over the next five years. Deloitte Access Economics modelling also suggests that a greater focus on cyber security by Australian businesses could increase business investment by 5.5% and wages by 2.0%, employing an additional 60,000 people by 2030.

These opportunities need to be earned however, and are not owed. A strong cyber security ecosystem is a mandatory prerequisite for continued economic growth. On average, a cybercrime attack costs a business in Australia more than $400,000. Who can businesses trust to get the fundamentals right?

With heightened awareness of the need to lift cyber resilience in Australia, an ACS Cyber Taskforce headed by senior cyber security expert Professor Jill Slay, was established to review global cyber security frameworks and identify best practice professional benchmarks that would be fit for purpose here in Australia. Frameworks examined included:

- US Department of Defense Information Assurance Workforce Improvement Program
- National Institute of Standards and Technology, US Department of Commerce
- National Initiative for Cybersecurity Education, Cybersecurity Workforce Framework
- US Department of Labor Cybersecurity Industry Competency Model

In September 2017, ACS announced its extension of our professional certifications scheme by introducing Cyber Security specialisations.

I would like to thank ISC2 and ISACA for partnering with ACS on this launch. As part of determining professional practice benchmarks, certifications from both organisations were considered when levelling ACS' standard.

ACS' flagship publication *Information Age* has since showcased a number of professionals achieving ACS certifications in cyber security. This publication is a compilation of those articles and provides a fascinating insight into the multi-disciplinary nature of cyber security across a range of verticals including aviation, banking and finance, audit and risk, consulting, and healthcare.

By employing professionals with a CP (Cyber Security) certification, Australian businesses and government are well placed to lift the cyber resilience of their organisations.

Andrew Johnson
Chief Executive Officer

Contents

4

"I've seen so many companies in Australia who say, 'We're not compromised, we're OK, we have a firewall' and I say, 'So you're monitoring, you're actually looking for indicators of a compromise?' and they say, 'No, but we have antivirus and I'm sure if we get compromised, we'll start getting alerts from that'. That's not how it works."

Charles Widdis

Corporate espionage: it's real and it's terrifying. Hackers aren't stealing the information you'd expect.

Charles Widdis

By Roulla Yiacoumi

"If you're a company doing business with other countries, you can expect that you're being hacked – because they want to know your negotiating position."

A hacker breaks into a company's network, gives himself administrator access, then proceeds to steal a bunch of seemingly innocuous documents, bypassing financial records and bank accounts.

To the untrained eye, this makes no sense.

To cyber security expert Charles Widdis, this happens every day and is not surprising in the least.

"If you're a company doing business with other countries, you can expect that you're being hacked – because they want to know your negotiating position," says Widdis.

The unfortunate thing, Widdis adds, is that many executives who run these companies in Australia don't accept this really happens.

"I don't think they accept that there are people whose job it is – they get paid – to take your information. It's not some guy eating pizza with a bottle of coke in a dark room. It's an employee in a company that's attacking you.

"It's nothing personal, he doesn't dislike you – it's just a job. At the end of the day, he goes home, he's got a family to feed.

"In a previous job, we were dealing with an incident and noticed the attacks would die down almost on the dot at 5pm Beijing time, because the attacker's gone home for the night. Now, why is there nothing happening today, on Monday? It's a public holiday in China today. The reason you're not being attacked is because he's at home, enjoying his public holiday.

"It's a real thing and it goes on."

Are you watching?

Corporate espionage is often depicted as the stuff of movies, but in reality, organisations around the world are having information pilfered from their networks.

Last year, research centre Ponemon Institute revealed it takes companies an average of six months to detect a network intrusion, and a further two months to contain it.

That's six months of a hacker making their way through your system without anyone noticing, without anyone taking any action.

"Just having antivirus and a firewall, and the fact your machine isn't going up in a flaming mist, does not mean you're not being hacked," says Widdis.

"I've seen so many companies in Australia who say, 'We're not compromised, we're OK, we have a firewall' and I say, 'So you're monitoring, you're actually looking for indicators of a compromise?' and they say, 'No, but we have antivirus and I'm sure if we get compromised, we'll start getting alerts from that'. That's not how it works."

Widdis says that at one place he worked at years ago, hackers got in through an old unpatched machine.

"It had just been sitting there for years, unmaintained.

"They were now administrators on the company's own network. The company didn't know, and they didn't know for another two years."

"The compromise was a publicly disclosed vulnerability that needed to be patched.

"Because that company didn't have good patch management, the computer didn't get patched; because they didn't have good asset management, no one really knew it was there or what it was doing. It was just sitting there as it always had."

The machine was compromised in what Widdis describes as "very traditional, very textbook methods".

The hackers were able to escalate privileges, take control of the administrator account, create additional accounts, and compromise the entire back end, he says.

"They were now administrators on the company's own network. The company didn't know, and they didn't know for another two years."

Contrary to popular theory, these hackers do not want your money.

No, there is something far more valuable at a company deliberately targeted by hackers.

"One of the very interesting things, which I think some companies may underestimate, some of the information that was being taken out was very bland and very boring. It's the kind of information you would say, 'Who cares about that?'," says Widdis.

"They targeted the company's quality management system and a lot of their business process information was being taken out, as well as their research papers.

"The briefing that was given to the company by external consultants was, 'Well, you need to understand that these third world countries, they can copy the product, but what they don't have is your history. They don't have the reputation. They wouldn't know how you run a business that's a multinational and extremely successful.'

"Sometimes it's not your IT, but maybe it's things you don't put value to. You have a very good business management system, you have a very good quality management system and they want it – why bother building their own when you could just take someone else's?

"The boards and management, they get it that they need to protect their systems, they need to keep the lights on, but I think they continually underestimate espionage and the industrial attack side of it.

"I think that will increase, it's not going to stop because we're not doing enough to stop it; we're not doing enough to protect ourselves around those areas. It's not taken seriously."

A career in cyber security

Widdis has been working in cyber security before cyber security was even a thing, working his way through the ranks in a "very traditional IT career". He began working on a help desk, moved into network administration, network management, Windows management, and server

"What frightens me at the moment is losing control of our SCADA systems, of our safety systems; losing control of the ability to operate our infrastructure."

management. He then progressed to running IT for businesses, and doing design and build work for companies.

It wasn't until the mid-2000s, Widdis says, that security started to become a topic of concern.

"We'd always been doing patching, of course, and you had antivirus here and there, but it was around about 2005, 2006 that I think things started to turn in the industry and we realised that this security thing needs more than just your system admin guy or someone running around. We actually need someone to do this full time."

When he had an opportunity to become involved in some fraud work a previous employer was investigating, he took a role as a full-time security professional.

"I don't think I would have even thought of that as a career at the time, that this was a full-time thing. It was more of, there's a role here for someone to do security, and that seemed pretty interesting to me."

Widdis' expertise lies in ISM security management frameworks, implementing security frameworks for companies, and policy and governance around security.

"Add on to that, I work very closely with the industrial security, looking after or around industrial control systems, SCADA, manufacturing OT security, those kinds of areas," he said.

What keeps him up at night

Today, Widdis is the Security Strategy and Planning Manager in the utilities sector, at a major power distribution company in Victoria.

"We don't deal a lot with intellectual property or competitive advantage or things like that. We deal with: you turn the switch and your lights come on – and that relies on us being able to control the power grid, to control the network.

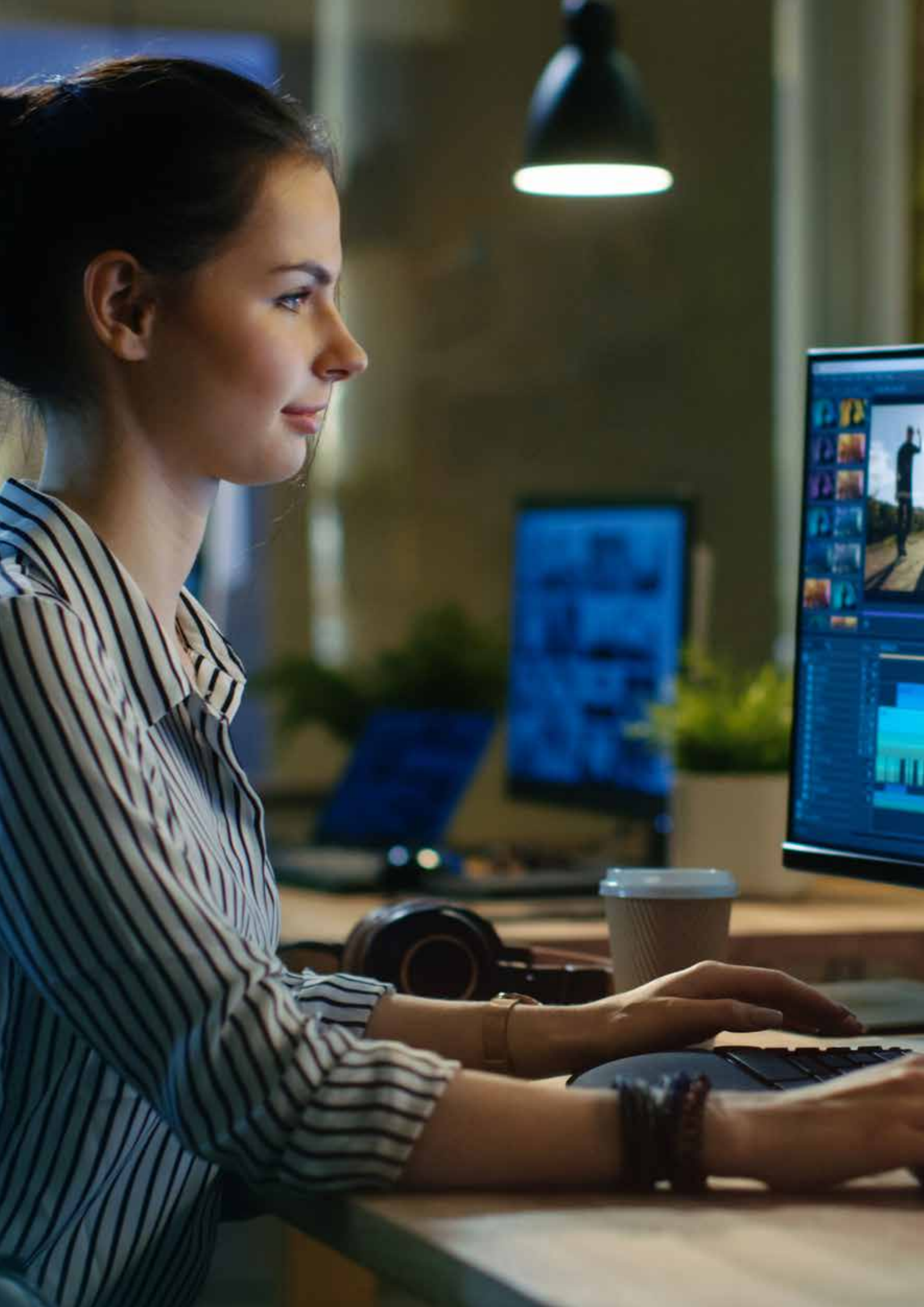
"What frightens me at the moment is losing control of our SCADA systems, of our safety systems; losing control of the ability to operate our infrastructure.

"It's being controlled by a random kid who's hacked in for fun, or it's being controlled by a malicious person who's now saying, 'We'll give you control back when you transfer 1,000 Bitcoin to us.'

"That's what concerns me."

Widdis says that in addition to escalated levels of corporate espionage, we can expect to see more ransomware attacks on individuals and a "few more large scale industrial incidents targeting industry, such as power and utilities" throughout the year

Charles Widdis is an ACS Certified Professional (Cyber Security).



"While CEOs may now be more willing to employ cyber security professionals to protect their organisations, there is still confusion when it comes to discerning who is and isn't an expert."

Garry Gaskell

An inconvenient (cyber) truth.
The reason we ignore cyber security recommendations.

Gary Gaskell

By Edward Pollitt

"I said to them, 'If you didn't seriously hire me to do the security architect's job, let's just say I never started and I'll walk out."

What's the best way to patch up a cyber security vulnerability?

Pretend it's not there, of course.

It might sound like a bad joke, but it's this attitude that has stood in the way of cyber security experts, such as Gary Gaskell, for the past 25 years.

Throughout his career, Gaskell has spent time spent working for universities, prominent banks and government departments.

And even as the 2013 Information Security Professional of the Year and a leading consultant in the field, there have been points in his career where his advice was falling on deaf ears.

"I was reflecting on why something like 20% of clients essentially rejected some of the observations because it was an inconvenient truth or something," Gaskell said.

"I thought, 'Okay, I've got to write better reports. I've got to be more logical.'"

However, upon further reflection, he soon realised the problem wasn't his reports.

Clients were choosing to believe that bad things wouldn't happen to them.

The early days

After a cryptography subject at the Queensland University of Technology sparked an interest in information security back in 1993, Gaskell has since devoted his career to ensuring cyber security is taken seriously.

Gaskell is one of the founding members of the Australian Information Security Association, taking the role of inaugural chair of the Brisbane branch in 2001.

And it's this passion for cyber security that nearly cost him a job with a bank early in his career.

"I particularly remember starting at the bank. They said, 'Look, I know we hired you as a security architect, but we really need someone to do this other [IT] work,' and I'm like, 'No, that's not my career plan. I think there's a bright future in cyber security.'"

"I declined, and I said to them, 'If you didn't seriously hire me to do the security architect's job, let's just say I never started and I'll walk out.' That was day two."
Gary stayed.

Smarter banking

Although it got off to a shaky start, Gaskell worked extensively with the banking sector in the early days of online banking.

One of his most memorable jobs came at the turn of the millennium with a major Australian bank, when he was tasked with creating the security plan for its first-ever internet banking system.

Fast forward 17 years and online banking in Australia is serious business.

"A CIO and CEO, who believes they're fundamentally excellent managers, they don't want to hear the message that they've totally mismanaged the security of a multimillion-dollar IT project."

In 2016, Australian comparison site Finder found that Australians made a total of 606 million transactions using online banking in the previous financial year, with 41% growth from 2014.

Just like its popularity, Gaskell has seen the security measures around online banking, and in other industries, transform in his time.

He explains that it is no longer a lack of security mechanisms from banks that poses the biggest risk when it comes online banking – it's us.

"Modern internet banking systems have really accepted that incidents will happen, and we don't."

But according to Gaskell, this is driving a shift in the way in which banks and other websites protect customers online.

"The biggest weak points are the endpoint devices that the users are using," he said. "So, there's not actually fundamentally trusted devices to log in from."

"The banks actually detect anomalies based on probably a hacked workstation or a hacked Android phone and limit the transactions.

"The balance has changed from being solely focused on preventive controls to having a serious focus on detection and preventing controls, detecting and responding to the incident."

Seeing the change

In Gaskell's current position of Principal Consultant for Infosec Services, he sees the differing approaches toward cyber security from a range of industries.

At times, he explains, businesses would still rather pretend nothing is wrong when a major cyber vulnerability appears.

"If you look at a system where it's had appalling security and it's really lacking, a CIO and CEO, who believes they're fundamentally excellent managers, they don't want to hear the message that they've totally mismanaged the security of a multimillion-dollar IT project.

"Let's face it – no one would!"

However, changing the perception and language used around cyber security is helping businesses choose to improve their cyber standards.

"Communicating to those people that it's not challenging their view of themselves as good managers, but pitching it as an improvement opportunity, so they can demonstrate how good a manager they are because they found these issues and they're going to fix it, so they own the problem."

Additionally, major incidents, such as the Equifax breaches last year, are now driving top-down change in boardrooms around the world.

"That's driven change because people are having board-level discussions and people go, 'Well, are we on top of this or are we not?'"

"The big change is executives and the Prime Minister are talking about it.

"That's driven change because people are having board-level discussions and people go, 'Well, are we on top of this or are we not?'

"Almost every CEO in Australia knows that the Target America and Equifax CEOs lost their jobs because of a major cyber breach.

"That's what's changed. Hence CEOs go, 'Well, where's my security manager? Has he or she got enough resources?'"

Who can you trust?

While CEOs may now be more willing to employ cyber security professionals to protect their organisations, there is still confusion when it comes to discerning who is and isn't an expert.

"Anyone who comes out of uni or downloads a couple of tools onto their laptop can overnight set up a web page and call themselves a security expert.

"You can't do that if you're a civil engineer, or a doctor, or a lawyer, but this is what happens [in cyber security].

"I see the wildly varying quality of work in my work by other people that have claimed to be security experts and too often, they've been quite naive."

Looking forward

What's the greatest fear of one of Australia's leading cyber experts?

"It's the fact that we've built our economy on a fragile system of software," he says.

"Software systems are very complex and we cannot produce software that is reliably secure in the current software market.

"How confident can we be connecting every business and government to the internet when there are vulnerabilities announced every day – somewhere between 10,000 and 18,000 of them in 2017.

"Essentially, we're crossing our fingers, hoping for the best – hoping that the really serious hackers target someone else."

Gary Gaskell is an ACS Certified Professional (Cyber Security).

"Aviation is now going through that rapid modernisation from an engineering-focused environment to an integrated digital environment driven by data."

Pierre Truter

Can a plane be hacked to fall out of the sky? And other questions to ask an aviation cyber security expert.

Pierre Truter

By Roulla Yiacoumi

"If data goes offline, aircraft will not fall out of the sky."

There's a scene in Die Hard 2 where the bad guys hack into the air traffic control system and change the altitude of ground level so that when the plane comes in for landing, it miscalculates where the ground is and smashes into the tarmac.

Could a cyber attacker really do that?

Aviation cyber security expert Pierre Truter laughs at the question.

"In theory, I think everything is possible," he says. "I think the reality is a little bit more complicated and I don't think you'd be able to do that easily."

That's a relief.

"Have you seen Die Hard 4?" Truter ping pongs back.

Ah, Die Hard 4. Where computer hackers bring down US transportation grids, the stock market, the power grid – pretty much any infrastructure that depends on computer systems to function.

"Die Hard 4 is a much more plausible scenario of what can happen," says Truter.

"Aviation is now going through that rapid modernisation from an engineering-focused environment for many years, moving into an integrated digital environment driven by data, and not so much by engineering as we have done in the past."

"We're looking at aircraft becoming more e-enabled, and we're looking at automation in the cockpit so that pilots have less to worry about."

"Even in air traffic control towers, we're looking at moving away from the old traditional towers where people sit in the towers, to what they call a digital environment – an electronic, digital air traffic control environment where people sit back in a room and rely on navigation aids and digital cameras to manage aircraft."

Welcome to the future.

Up, up and away

Truter has worked in IT for 35 years. Commencing with a role in the military building command control and missile systems, he moved into the aviation industry in 2003, with a 14-year career at Airservices Australia.

"Eight, nine years ago, I was representing Australia at a committee in Montreal which was planning this global automation of air traffic management to move into a digital environment," he says.

Truter was the chair of that committee for four years.

"As we were planning the global integration and modernisation of all these systems to create a back-end information environment to automate the aviation system, cyber security became a much more prominent issue," he says.

"I started focussing also on cyber security issues in the Air Traffic

"To me, the technology is not so much a challenge, but it's more the management aspect. How do you get the governance, the policies and the procedures to guide cyber security in this fragmented environment?"

Management domain about eight years ago. At the same time, I was also the Chief Information Security Officer for Airservices when I was looking after all cyber security for the air traffic management of the country.

"The question became, 'If we build this global network on how we can integrate all the back-end systems to enable the future digital Air Traffic Management system, how do you build cyber security in it from the beginning?' Global strategies say that we will have ground to ground, ground to air, and air to air System Wide Information Management (SWIM) by 2028, fully automated."

What does that mean?

"You won't have voice comms so much, but you will have data comms in future, integrating with the systems. If you have more data comms, you can build more automation into the system and enable aircraft to be more automated."

More automated?

"Yes, with all the data that it has on flight paths, and whether to fly around thunderstorms and danger areas. In aviation it is known as a 4-dimensional trajectory. That's part of what the upcoming global data framework is supposed to enable."

The global framework Truter speaks of is the set of rules to integrate the communications and data networks of 191 countries in the world.

"How do you do that," he asks, "when every country has got its own cyber security rules and regulations?"

Truter says the challenge is that cyber security is an issue that cuts across all components of aviation.

"At the moment, aviation is still in, let's call it, three silos. You have the air traffic control environment, which is mostly managed by the state. We have the airport's environment which is mostly privatised, and then you have the airlines which are totally separate privatised organisations.

"But this full aviation ecosystem is modernising at the moment, and we still have this fragmented approach.

"To me, the technology is not so much a challenge, but it's more the management aspect. How do you get the governance, the policies and the procedures to guide cyber security in this fragmented environment?

"How do you build cyber security by design, in the beginning, as we modernise the systems?

"To me, that is the biggest challenge for cyber security in aviation at the moment."

Ready to board

If the thought of an airplane making its own decisions frightens you, you probably won't like this next bit.

"If you look at the documents of the global air navigation plan from the International Civil Aviation Organisation (ICAO), it states that they would like to reduce pilots in the cockpit to one person in the future because the rest of the workload will be taken over by automation.

"It's becoming much more difficult to stay ahead of the hackers because the attack vector is becoming so much bigger as we move to fully automated systems."

"At the last aviation show in Singapore about two months ago, they had the first discussion of what a cockpit would look like for an aircraft with only one pilot in the cockpit, and a lot of automation in the whole ecosystem. This will first be introduced in cargo aircraft.

"At the moment, it is possible to fly aircraft without the pilot. We've seen the military do that many, many times. Technically, it's possible, but to move into that environment for commercial aviation – that I think is their biggest challenge."

You read that correctly. Commercial airliners will probably one day fly themselves.

While we're still getting our heads around driverless cars, buses and trucks, the thought of an airliner flying itself with 200+ people on board is terrifying.

"I personally think it will be many, many years before the public will be happy to accept something like that," Truter says.

Phew.

"I would really like to fly with a pilot in the cockpit," says Truter.

"I would not like to leave everything to artificial intelligence and automated systems because there's always that one in a million chance when you need to land the aircraft in the Hudson, when you still need a pilot that can make some decisions."

Hack attack

Truter says that in a much more integrated aviation environment, it's possible to see an air traffic control system hacked and shut down.

The result? Chaos.

"You can just imagine if you take a big airport like Sydney and you shut it down – nothing can move. Sydney being a big hub, just imagine if nothing can get in and out of Sydney for a few hours. You disrupt your whole aviation network in the country. The economy of the country takes a huge knock."

There are three possible reasons for a cyber attack, says Truter.

"You've got firstly the people that try to hack in to get a feather in the hat, and say, 'You know, I hacked an air traffic control system. Now, I can become part of the web group Anonymous'. That's one scenario.

"We've seen some of the other scenarios where state organisations will just hack into your organisation and not disrupt anything, but just sit on your network, waiting for that one day that they need to shut down your air traffic control system or disrupt your air traffic control system. That's the second scenario.

"In the third scenario, we've seen that systems can be shut down, like we've seen like in any other industry and they say, 'Pay me five Bitcoins so you can have access to your systems again', so the same scenario that you have in banks and

"There's always that one in a million chance when you need to land the aircraft in the Hudson, when you still need a pilot that can make some decisions."

everything else can happen in air traffic control environments, exactly the same."

"The problem is just that the air traffic controller environment or aviation has such a big impact on the economy of the country, and I think that's the biggest risk that we have in the aviation industry."

"It's becoming much more difficult to stay ahead of hackers because the attack vector is becoming so much bigger as we move to fully automated systems in future."

"The problem is just that the air traffic controller environment or aviation has such a big impact on the economy of the country, and I think that's the biggest risk that we have in the aviation industry."

"It's becoming much more difficult to stay ahead of hackers because the attack vector is becoming so much bigger as we move to fully automated systems in future."

Truter says that what really scares him is not the fact that somebody will hack in and shut down systems or delete data "because we prepare for something like that, in all eventuality."

"If data goes offline, aircraft will not fall out of the sky," he says.

"What scares most of us is when people hack into your system and start changing the data slowly but surely, and you cannot see the changes in the system. That's much more risky.

"As an example, when somebody comes in and constantly changes the arrival and departure dates of aircraft, that would disrupt your whole network.

"It's more just corrupting the data than destroying the data. Changing the data in the system is much more a risky proposition from an aviation perspective.

"That's one of the biggest risks that I see in the next few years."

Staying the course

Today, Truter works for a private aviation supplier.

"I'm now more involved from the industry side to look at the cyber security standards and frameworks for the people that are building the global aviation industry.

"I'm more from the supplier side now, and asking, how do we build this in future. How do you set the global governance standards, local security standards, to build the global aviation system?

"My focus is on how do you create a standard, a framework, templates, and policies and strategies for the aviation ecosystem, which includes air traffic management, airport, and airlines, that full ecosystem. What is the framework to determine all the risks as you modernise the system? That's where my focus is."

As systems are modernised in the future, the challenge lies in bringing the government systems and private industry together to come up with one framework to secure commercial aviation, Truter explains.

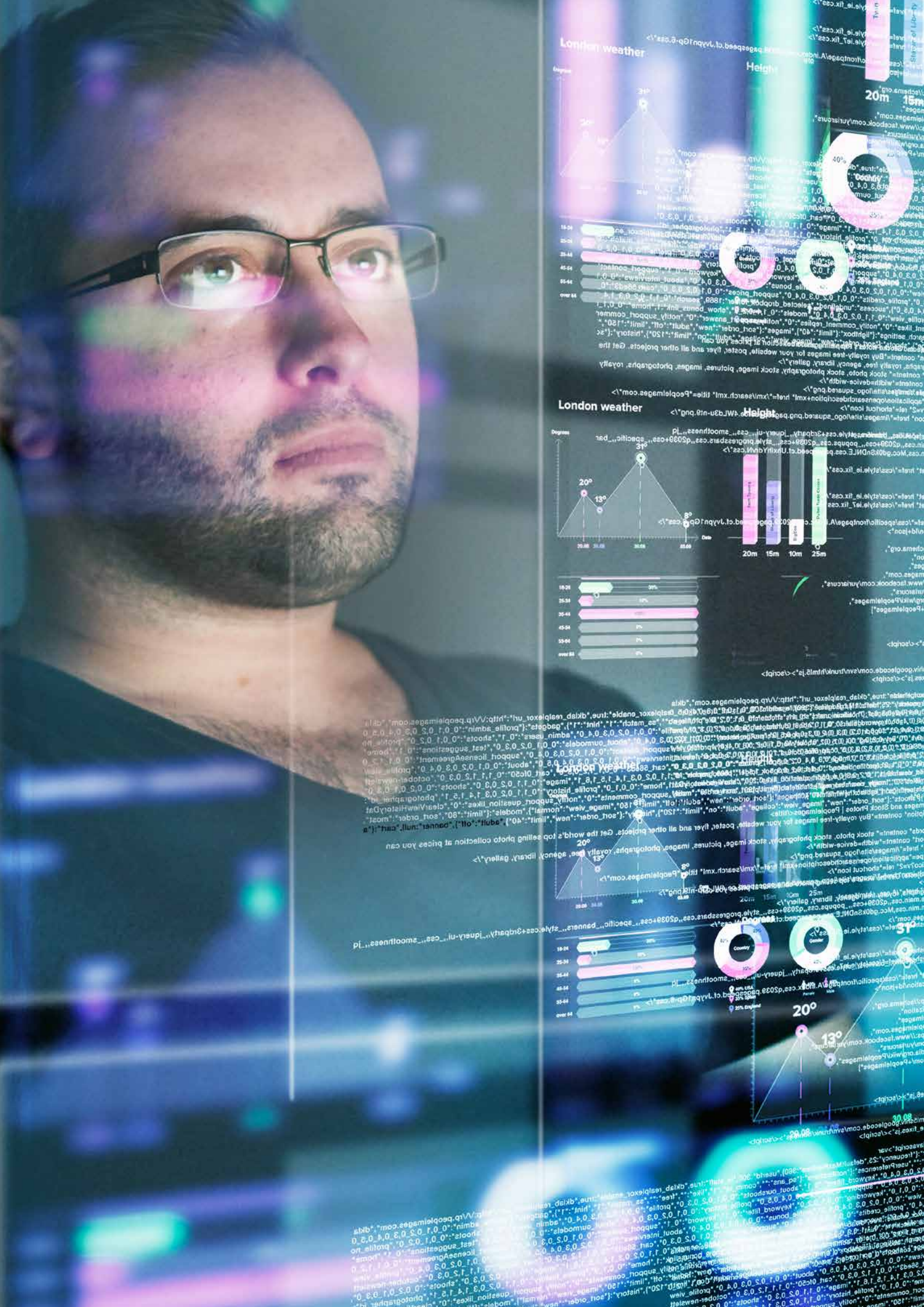
"Because you've got one part that lies in government that follows the government rules and standards, but a lot of it is private organisations, like airlines and airports. They follow their own security standards.

"For the Federal Government, cyber security for critical infrastructure is also a sovereign issue.

"How do you set up one framework for the ecosystem that combines commercial interest and government interest under one banner and build a secure system?

"That's the biggest challenge, and that's really what keeps me up at night."

Pierre Truter is an ACS Certified Professional (Cyber Security).


London weather
Height
20m
15m
10m
25m
20°
13°
8°
31°
Degrees
Date
Country
Gender
40% USA
20% England

"We need industry bodies, like ACS and ISACA, to look at opportunities for members to allow them to continue to help their professional development in their own time – to make sure that women are encouraged to come back into the workforce."

Jo Stewart-Rattray

From boardroom to the UN.

Cyber expert at the top of her IT governance game.

Jo Stewart-Rattray

By David Braue

"There is a lot of focus on cyber but still not necessarily a good understanding of what it incorporates. We are protecting our perimeters, but what we really have to concentrate on is protecting our data."

It's not the first place you'd expect to find an Australian business technology consultant, but when Jo Stewart-Rattray stepped into the United Nations General Assembly in New York City in March, she felt like a life's ambition had been achieved.

"It was a life-changing experience and I don't say that lightly," Stewart-Rattray recalls of the trip that saw her join a contingent of high-level Australian representatives participating in the 62nd Session of the UN Commission on the Status of Women in March.

"When I stepped through the diplomatic entrance at the UN, walked down the corridor of flags, and set foot in the UN general assembly – the tears flowed."

"For someone who had wanted to make a difference at the UN since I was 7 years old, it was the most incredible experience."

Stewart-Rattray spent two weeks as one of two civilian representatives within the official delegation from Australia – which included Minister for Women Kelly O'Dwyer, Australian Ambassador for Women and Girls Dr Sharman Stone, Sex Discrimination Commissioner Kate Jenkins, and others.

Their goal: to help resolve an impasse from previous sessions, which ended without a consensus, and nut out a detailed action plan covering ways to use access to technology to empower rural girls and women in both developed and developing countries.

A fortnight of sharing, learning, and energy bar-powered all-night sessions finally helped the delegates – who hailed from 193 member states in total – reach a consensus and outline a way forward.

And when the gavel came down on that session, Stewart-Rattray says, there were cheers and tears galore.

"The room went ballistic," she recalls. "There were people crying and laughing, and it was such a feeling of achievement. I was hugging an African woman and I still have no idea what her name was."

"I came back to Australia thinking that my dream had been achieved because I had helped make a difference, to help empower rural women and girls globally."

Cyber security awareness for the board

New York City is a long way from Stewart-Rattray's usual work in Adelaide, where she works as Director of Information Security & IT Assurance with commercial advisory firm BRM Holdich.

With a string of industry certifications under her belt, Stewart-Rattray has a national scope that sees her working with board members and C-level executives to help them navigate the complexities of cyber security and, increasingly in recent times, technology governance.

That governance focus has been driven by increasingly onerous

"It's not a dark art, and some of the most simple cyber hygiene rules can be put in place to help an organisation on its way,"

requirements of legislation such as Australia's new notifiable data breaches (NDB) scheme and the European Union's general data protection regulation (GDPR), which have become the poster children for an evolving privacy climate built around consumer-driven data protections.

"There is a lot of focus on cyber but still not necessarily a good understanding of what it incorporates," Stewart-Rattray explains. "We are protecting our perimeters, but what we really have to concentrate on is protecting our data."

Protection is only one part of the challenge, however: visibility and control are just as important.

This is a point that every company will encounter when they receive their first request for a dump of the data the company holds on them, or a Right To Be Forgotten request that requires the company to delete all data on a person.

"It's not a dark art, and some of the most simple cyber hygiene rules can be put in place to help an organisation on its way," she says.

"The first thing is for organisations to understand what data they're collecting and why."

"Ask whether it's going to be used for the purpose for which it's collected. If not, it's no longer acceptable behaviour to hold it."

A long road to the UN

If educating executives about security is Stewart-Rattray's job, engaging with her adopted industry is her passion.

One of the industry's most easily recognisable personalities, she is a regular speaker on the conference circuit and long-time executive member of IT governance association ISACA.

Having served in numerous ISACA roles since 2004 and been appointed international director of ISACA in 2015, Stewart-Rattray now acts as global leader for the organisation's SheLeadsTech program, which aims to increase the representation of women in the tech workforce and tech leadership roles.

She has also served as Chair of the Australian Computer Society's South Australian branch executive committee; served as General Manager of group information technology for the Experience Australia Group; chaired ISACA's Professional Influence & Advocacy Committee; and held myriad other governance-related roles since she began her career working in infrastructure services.

Yet despite her enthusiasm, when pressed as to why she got into the IT-governance space Stewart-Rattray says it was an acquired taste.

"I can't say that I suddenly woke up one day and decided I was going to

"We need industry bodies, like ACS and ISACA, to look at opportunities for members to allow them to continue to help their professional development in their own time – to make sure that women are encouraged to come back into the workforce."

be an information or cyber security governance specialist," she explains.

"It evolves over time and you begin to realise what floats your boat – but it's not always something that floats everyone's boat."

The importance of governance and information security became increasingly clear many years ago, when she was working in infrastructure services and co-ordinating information security with teams of engineers charged with maintaining the integrity of an electricity grid.

"That was a really interesting period for me," she recalls. "I was responsible for both operational IT - the SCADA and operational control systems – as well as business IT. I learned so much; it was just extraordinary."

Big, hairy, audacious goals

For someone who is so engaged with teaching industry leaders, Stewart-Rattray's calendar is also loaded with learning opportunities.

Her professional life has been marked by continuous learning, to which her five information-security credentials – CISM (Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT), CISA (Certified Information Systems Auditor), CRISC (Certified in Risk and Information Systems Control), and CP (IP3P/ACS Certified Professional Cyber Security) – attest.

Yet while her credentials speak volumes about her ability to drive change throughout her client organisations, it is her work with causes such as SheLeadsTech that continue to represent a key focus for her energies.

Addressing the chronic underrepresentation of women in tech positions – particularly leadership positions – remains "a big, hairy, audacious goal" but Stewart-Rattray is up for the challenge.

Raised in country Victoria, she is particularly attuned to helping develop career paths and technological engagement for girls and women in rural areas – hence the excitement over the global focus of the UN mission.

"We're looking to help women prepare to lead," she says. "But there's an age group where we lose women, generally around those child-rearing years."

"We need industry bodies, like ACS and ISACA, to look at opportunities for members to allow them to continue to help their professional development in their own time – to make sure that women are encouraged to come back into the workforce."

Jo Stewart-Rattray is an ACS Certified Professional (Cyber Security).

"The initial perception of cyber security is that it is within the technical realm or may relate to some form of tool. But I would argue that it's a mere enabler and that it's one of the core components that a senior leader within an organisation should be highly cognisant of."

Roland Padilla

Balancing cyber with business. It's about understanding external risks and internal management.

Roland Padilla

By Edward Pollitt.

"Cyber security is increasingly becoming a business engagement, involving collaborations with key stakeholders, management of investments, and considerations of global contexts."

Cyber security is as much about humans as it is technology.

That's what government cyber expert Dr Roland Padilla has learned after an ICT career spanning more than two decades.

Currently working with the Federal Government in overseeing compliance with relevant legislation, Padilla said cyber security should be driven by a combination of handling external risks and a strong internal risk management culture.

"I view cyber security as an integral part in integrating the concept of not just technology but also business and policy," he told *Information Age*.

Padilla has spent the majority of his time working at the cross-section between cyber security, business management and academia.

He described modern-day cyber security as a converging Venn diagram, with technological advances, policies, and business management overlapping.

"Cyber security is increasingly becoming a business engagement, involving collaborations with key stakeholders, management of investments, and considerations of global contexts," he said.

"Yes, I do agree that the initial perception of cyber security is that it is within the technical realm or may relate to some form of tool."

"But I would argue that it's a mere enabler and that it's one of the core components that a senior leader within an organisation should be highly cognisant of.

"So, it has to be looked at in terms of risk management, such as mitigating exposure to vulnerabilities and to cyber exploitations, including external and internal."

Finding the balance

It's this interest in balancing business requirements and cyber security that has prompted Padilla to begin a Master of Business Administration (MBA) at the Australian National University.

He explains that he believes completing these studies will provide him with a "different perspective" on the world of ICT security.

Prior to his MBA, Padilla completed a Masters with first-class honours and PhD at the University of Melbourne, where he investigated the business value in cloud computing.

Again, combining business and technological innovation allowed him to advance his ability as a cyber security professional.

As part of his research he interviewed 21 different Australian business managers on their uses and perspectives on cloud computing.

"There has to be a so-called synchronisation of experiences and knowledge between the academic community, the private sector and the public sector."

This primary research gave him meaningful industry insights, he says.

"I was able to investigate the problems encountered by managers and by investigating these problems, I fed that into my research," he said.

"I communicated that to the academic community through peer-reviewed publications, as well as to the broader practitioner community through presentations.

"I shared my findings and provided my insights and eventually it led me to where I am now."

Challenging our knowledge

Alongside his professional commitments with the Federal Government, Padilla is also employed by the Australian Centre for Cyber Security as a Casual Academic.

"The reason for me doing that is to keep me sharp and up to date with knowledge. It keeps me engaged with the academic community and with the students whom I value in terms of their insights," he said.

In his role, he assists students completing their Masters of Cyber Security with their coursework while also marking and assessing various tasks.

This position provides him with a front row seat to view the state of cyber security education in Australia.

Working with postgraduate students, he says most if not all do have relevant industry experiences, including both the private and public sector, and that the overall ability of the cohort appears strong.

"I have a sense that they certainly bring with them a wealth of insights," he said. "There's a high level of experience and knowledge that these postgraduate students do contribute to their course."

While he can see first-hand the strength of the postgraduate sector, Padilla still believes cyber security education in Australia could be improved through strengthening industry ties.

"There has to be a so-called synchronisation of experiences and knowledge between the academic community, the private sector and the public sector."

"So, with that, the intended outcome would be for the students to be able to learn specific courses that are aligned with industry practice.

"With this alignment, with this technicality, and relevance, the students would be highly employable for numerous sectors such as the government and the private sector."

Creating advocacy

And for the industry overall?

"There are still a lot of improvements to be made. We just have to observe what other nations are doing in terms of investments and building their respective cyber workforce," he says.

"However, we have been observing efforts made by the Australian government, private and academic sector relating to improving advocacy towards cyber security."

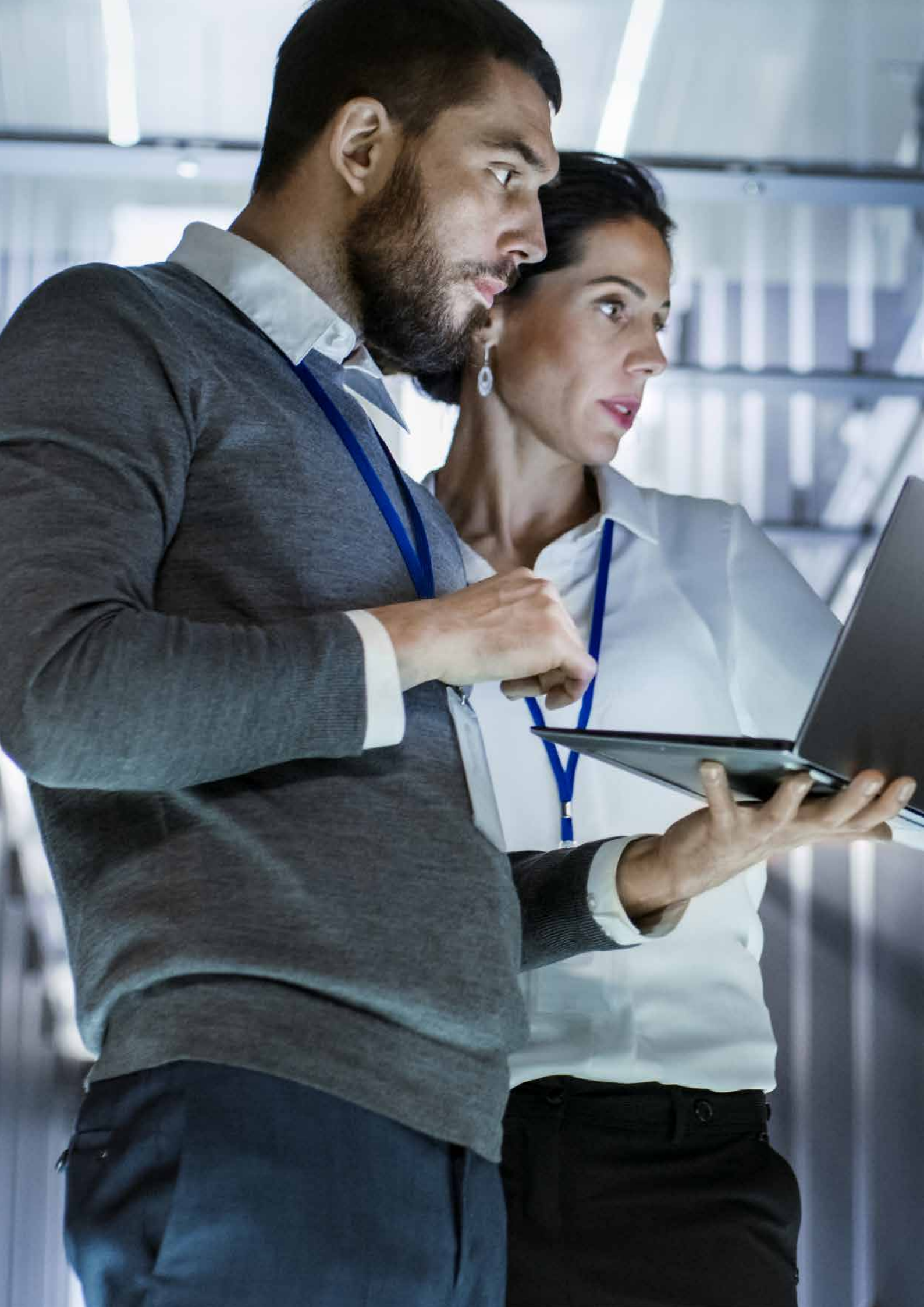
He outlined open source reporting from the government's official cyber security strategy and the Department of Defence's 2016 white paper as positive public initiatives that increase visibility when it comes to cyber security, while also recognising similar efforts from the private sector.

"So, I would say that we are on the right track, we're getting there," he said.

"Cyber security is here to stay."

"The challenge at this stage is building the appropriate cyber security workforce, and there have been indicators that the Australian government has been committed and supportive of that."

Dr Roland Padilla is an ACS Certified Professional (Cyber Security).



"Now, we have a specialised IT industry that is quite crucial in everyday function. Whether it's day-to-day function, your social activities, whether it is banking, whether it is your professional work. Anything that you do, you need to now consider cyber security."

Dinkar Sharma

How the census breach put cyber on the map. It was the wake-up call Australia needed.

Dinkar Sharma

By Edward Pollitt

"Any kind of incident is an eye-opener. It (the Census breach) contributed towards creating more awareness and Australia now treats cyber attacks as extremely serious."

On 9 August 2016, the Australian census website received four denial-of-service attacks, shutting down the first-ever predominantly online census.

Fears of compromised data swirled through the media and thrust cyber security into the public eye.

But IT professional at the Department of Human Services, Dinkar Sharma, believes the breach – that the Australian Bureau of Statistics (ABS) claimed did not compromise anyone's data – has helped the state of cyber security in Australia.

"Any kind of incident is an eye-opener," he tells *Information Age*.

"It contributed towards creating more awareness and Australia now treats cyber attacks as extremely serious.

"It is great to see that people are taking more interest in cyber security."

And in terms of the attacks that occurred on that August night?

"I believe the ABS took extra care and immediately disabled access to the census website when they discovered multiple Distributed Denial of Service incidents occurring."

According to Sharma, the growing awareness towards cyber security is not just due to widely-publicised breaches such as the 2016 census, but it can be attributed to the constant threats an everyday citizen faces.

"Your whole life depends on cyber security now," he says.

"Before, people could rob you physically.

"Now they don't need to. They can just sit in one corner in an air-conditioned room, and they can take your whole wealth."

Cyber security for the everyday Australian

Sharma first fell into cyber security when, with just a Bachelor of Information Technology to his name, he was tasked with creating a cyber security domain for a cyber operations centre's Quality Assurance Environment.

Since then, he has seen technology and computing become an increasingly vital aspect of everyday life, and with that, cyber security become a household necessity.

"Now, we have a specialised IT industry that is quite crucial in everyday function.

"Whether it's day-to-day function, your social activities, whether it is banking, whether it is your professional work.

"Anything that you do, you need to now consider cyber security."

And while the increased awareness and advocacy for cyber security in recent years is undeniable, there is work still to be done.

"Information can be obtained from social networking, and using their identity, can be used to access pretty much their life savings."

What can you do?

Although the responsibility of cyber security advocacy and awareness traditionally sits with government agencies and industry professionals, Sharma believes a changing of the guard may be in order.

"I think awareness is something that we all need to share, everywhere you go, it is our moral responsibility that we educate."

"We can inform other people to be safe, inform them on how they can do their transactions over the internet safely.

"That definitely increases the knowledge."

Internet banking is one area he believes security is being taken seriously amongst the general public, due to the obvious financial risks.

However, other seemingly innocuous online activities pose the greatest risk when it comes to everyday cyber security, according to Sharma.

"People are more aware of doing internet banking safely," he says. "They're not aware of how to protect their credentials."

"They're not aware of how to safely use social networking. Information can be obtained from there, and using their identity, can be used to access pretty much their life savings."

Sharing responsibility

In terms of cyber security advocacy, an individual can only do so much, says Sharma.

Likewise, a single organisation has limited reach, whether public or private.

This is why he believes that industry partnerships are so important when it comes to educating the greater public on the importance of cyber security.

"Everyone needs to contribute constantly towards cyber security improvements and awareness," Sharma says.

"We are witnessing lots of strong government initiatives – even private industries are taking more interest and working together to improve the way they conduct business.

"We are seeing more conferences, more seminars and more sharing of ideas towards cyber security awareness.

"Public/private partnerships are vital in overcoming weaknesses; these types of initiatives can lead to highly beneficial solutions."

Keeping up to pace

Although Sharma supports the advocacy work of the government and private sector, he is mindful that awareness can only get you so far when it comes to cyber security.

"There is a strong need for formal education in cyber security," he says.

"There are online threats and behaviours that are impossible for security software to detect.

"Becoming educated about threats and the best practices against them will make it immensely difficult for a cybercriminal to access our data."

Sharma has continued to upskill throughout his career.

Seminars, networking events, certification courses and even IT awareness courses have all helped him keep pace with cyber trends.

"Evolving myself and increasing my knowledge every day as I go helps, because the IT industry is very cutting edge and is drastically changing every day."

Dinkar Sharma is an ACS Certified Professional (Cyber Security).

"An ethical hacker is a trusted person who attempts to penetrate an organisation's IT systems and networks using the same knowledge and tools as a malicious hacker, but in a legitimate and ethical manner."

Patrick Yau

The business of ethical hacking. You can find holes the easy way or the hard way.

Patrick Yau

By Edward Pollitt

"The main benefit of ethical hacking is to help businesses understand where the cyber security weaknesses are in their systems and networks."

Would you pay someone to hack into your own system?

"To beat a hacker, you need to think like a hacker," says senior IT consultant and certified ethical hacker, Patrick Eulogius Yau.

The term 'ethical hacking' was coined in 1995 by former IBM Vice President of Internet Technology, John Patrick, to describe the process in which a system is knowingly tested for any vulnerabilities.

Ethical hacking is now commonplace in the cyber security industry, serving as a way for businesses to identify and fix any weaknesses before a real hack occurs.

"An ethical hacker is a trusted person who attempts to penetrate an organisation's IT systems and networks using the same knowledge and tools as a malicious hacker, but in a legitimate and ethical manner," says Yau.

"Ethical hacking is a series of processes to determine the target system's vulnerabilities and weaknesses.

"The result is used to recommend preventive and corrective countermeasures that mitigate the risk of a cyber attack."

Why the need?

Yau became an IT Controls Assessment auditor in 1993, where he covered security policy, password policy and access control.

Since then, he has seen cyber crime sophisticate, and the stakes get higher.

"People are now concerned with privacy," says Yau. "Attacks are getting more severe and the cost of being attacked is getting higher, but there is a lack of skilled cyber security professionals."

Despite this, ethical hacking has emerged as a way for businesses, and even government, to ensure they are one step ahead of a cyber attack.

"The main benefit of ethical hacking is to help businesses understand where the cyber security weaknesses are in their systems and networks."

"Ethical hacking can help to protect government systems and networks in order to fight against cyber terrorism and national security breaches."

"Security is a continuous process – if you are secure this minute that does not mean you are secure the next minute – therefore, continuous testing with the latest tools and techniques is necessary."

Although such measures require high levels of upkeep, Yau explains that taking the initiative will benefit the business overall.

"Security is a continuous process – if you are secure this minute that does not mean you are secure the next minute – therefore, continuous testing with the latest tools and techniques is necessary."

"Businesses will be in a strong position to ensure their most sensitive data and reputation are well protected," he said.

Organisations looking to protect their networks using an ethical hacker can expect to pay upwards of $8,000 for five days' work.

What makes a good hacker?

Yau's ethical hacking certification was provided by EC-Council and is designed to "immerse you into the hacker mindset."

"Generally speaking, an ethical hacking course is training people to be a legitimate threat agent."

He explained that an ethical hacker must be skilled in password cracking, phishing, denial-of-service, spamming, email hacking, routers and firewalls hacking, handheld devices hacking, GPS hacking and WiFi hacking.

But with this vast portfolio of malicious skills to their name, Yau explains, the most critical component of ethical hacking for students to learn is "to have good professional ethics and conduct."

While completing their ethical hacking certification, students are made to sign an ethical code of conduct, something many businesses also enforce.

However, Yau believes more stringent measures are required to make sure that ethical hackers remain ethical.

"In my opinion, knowledge, tools and skills can be trained but ethics and professional conduct are difficult to train, since they involve attitude and personal character.

"Training institutions should consider performing screening to ensure it has the 'right and proper' students."

Creating Australia's next cyber experts

Although he has spent almost the entirety of his career working in Asia, Yau was formally trained in Australia, receiving a Bachelor of Science in Computer Science and a Master of Commerce in Information Systems from the University of New South Wales.

It was this theoretical grounding in the IT industry that allowed him to begin to explore the world of cyber security.

"From a technical perspective, you need know the concepts of operating system, database, network and system development before you can apply security."

However, what really brought Yau success in the industry was when he began to combine international qualifications and on-the-job training with his academic training.

He recommends any up-and-comers follow his lead.

"Cyber security is an evolving industry and staying abreast of the latest trends, threats, and changes is critical.

"The consequences are fatal – it can be literally life and death."

"Hence, obtaining both an academic degree and a good mix of overseas certifications in the field of IT or cyber security is ideal for today's era."

He also highlighted the development of postgraduate programs in cyber security, which are now being offered in Australia, as beneficial to the industry.

Spotting the weaknesses

As a consultant, Yau works with businesses from different industries on their cyber security development.

What this has taught him is that some industries are better placed than others.

"Healthcare industries are particularly vulnerable in comparison to retail and financial industries.

"These store patient information, medical information, payment information and other intellectual properties.

"Attackers can use identity theft or ransomware to attack healthcare industries, preventing organisations from accessing critical system or information.

"The result of this could be catastrophic due to loss of sensitive or proprietary information and the disruption to regular operations."

He also explained that as technology continues to develop, the cyber risks we face will get even scarier.

"IoT devices incorporated into patients' bodies for medical purposes pose a risk.

"With IoT hacking, attackers could exercise direct control over medical equipment, such as shutting down or locking out the equipment.

"The consequences are fatal – it can be literally life and death."

Patrick Yau is an ACS Certified Professional (Cyber Security).

"I think it's natural that blockchain falls into the cyber security portfolio because it actually enhances the security of data when transactions are being processed in the distributed environment."

Jeff Yong Xun Xie

Is blockchain the future of cyber security? Why banning ICOs will hinder innovation.

Jeff Yong Xun Xie

By Edward Pollitt

"It [an ICO ban] is sort of a roadblock for the blockchain technology innovation, because once it has been banned, it is unlikely that the number of blockchain companies will thrive in these countries."

Blockchain is perhaps the hottest thing in tech right now.

It's the decentralised ledger technology that undermines cryptocurrencies and is already starting to transform supply chain management.

And according to one senior analyst at a global intelligence firm – it could be the future of cyber security.

Jeff Yong Xun Xie is a Senior Security Analyst at IDC Asia Pacific.

He analyses the latest cyber security industry trends and assesses the viability of different solutions on the market.

"I think it's natural that blockchain falls into the cyber security portfolio because, first of all, blockchain actually enhances the security of data when transactions are being processed in the distributed environment," he says.

Having had major reports published on the topic, Xie is a leading figure at the intersection of blockchain and cyber security.

He explains it is the decentralisation of the technology that makes blockchain such a valuable asset when it comes to cyber security.

"It gives you an automatic chain of cyber security baseline whereby people are not able to just hack into centralised storage and manipulate the data," he says.

"That preserves the integrity, and no one can easily hold majority control of the blockchain. That will then preserve and broker the trust within those transactions."

Banning ICOs

The idea of blockchain in cyber security is one that is beginning to gain traction.

However, in some regions, blockchain technology faces an uphill regulatory battle which is hindering its effectiveness in cyber.

"The technology itself is an opportunity, but since it is often tied to cryptocurrency, which is one of the underlying factors of blockchain, we see a lot of government legislations and regulations coming up around ICOs [initial coin offerings] and not so much on blockchain technology," says Xie.

He cited countries that had completely banned ICOs, such as China and South Korea, and the potential long-term harm this could cause to the development of blockchain.

"It [an ICO ban] is sort of a roadblock for the blockchain technology innovation, because once it has been banned, it is unlikely that the number of blockchain companies will thrive in these countries, as raising funds through ICOs is the conventional way blockchain start-ups kick off their projects.

"We're in a digital age where a lot of things are going digital. Especially when it comes to IoT, I think it is especially important that cyber security be incorporated as part of the design of the product that is being offered."

"The big players with deep pockets focusing on the technology may stay, but start-ups, which form a sizable part of the blockchain innovation scene, might simply turn to other countries.

"Bans on ICOs and cryptocurrencies may actually be hindering the blockchain technology innovations.

"But we can see many countries are also researching and trying to understand more about the technology.

"I certainly hope that moving forward – with proper regulation – regulation will actually help to drive the innovation of blockchain technology."

The IoT revolution

Xie's work is not limited to blockchain.

Rather, his focus is on emerging technologies and the impact they have on cyber security.

With Internet of Things (IoT) technologies now beginning to enter the mainstream, Xie is already investigating what a more connected world means when it comes cyber threats and vulnerabilities.

"We're in a digital age where a lot of things are going digital," he says. "Especially when it comes to IoT, I think it is especially important that cyber security be incorporated as part of the design of the product that is being offered."

IoT technology promises to transform manufacturing, healthcare, transport and retail industries through creating more interconnected and adaptive networks.

Additionally, smart homes and cities will offer users an immersive everyday experience.

However, the improved productivity and potential cost saving could bring some new vulnerabilities, according to Xie.

"Anything digital and connected is actually an avenue for cyber attackers to get in and to take control of your life."

The healthcare industry in particular is capitalising on some of the opportunities presented by IoT technologies.

"Traditionally, with a pacemaker, we had the issue of the healthcare service providers not being able to update them.

"We then start to see some of the researchers exploring the integration of wi-fi capabilities into a pacemaker.

"Well, that gives convenience to healthcare service providers to let them to access and monitor the performance of the pacemaker in a patient.

"It also opens an opportunity for cyber attackers to take control over the pacemaker – that in turn opens up another can of worms where the risks involved is actually life and death."

"As individuals and even kids start to get online there's a lot of risk involved there. You don't know who is on the other side of things."

And would Xie ever use a wi-fi-enabled pacemaker?

No way.

"I would definitely opt for an offline pacemaker for my heart."

Cyber, business and people

Xie also works with businesses to identify emerging challenges and strengthen their cyber capabilities.

He explains that his greatest challenge here is highlighting cyber security as not just an ICT risk, but a business risk.

"Security is as strong as the weakest link," he says. "So, you may have the most sophisticated and high-end security systems, but if your employees are not properly trained, just a simple act of plugging in and inserting a USB into their work systems could just bypass all your expensive technology."

Creating this change, and ensuring cyber security training receives the necessary funding, must be driven from boardrooms, not IT desks, he says.

"Cyber security should be driven from the top down.

"The business leaders should be the ones advocating cyber security initiatives and practising what they preach."

This is for good reason.

Xie describes 'whaling' – a new phenomenon where email phishing scams target business leaders.

It is a term originating from Las Vegas, where extra time and effort is spent on getting the 'high rollers' into the casinos.

In the security world, this extra time and effort is spent on creating seemingly legitimate and urgent phishing scams that will con a C-suite executive into handing over important business information or credentials.

"These are the people that are actually not as careful; CEOs and top business leaders are the ones clicking on such links."

The example he gives is of a CFO being sent a fake link from the bank to urgently reset a compromised company credential.

"It may not necessarily be easier, but it usually results in a more lucrative heist."

Imagining the future

Xie has just welcomed the birth of his first child.

And his introduction to parenthood is already causing him to think about how technology will change the future, and the importance of cyber security.

"The first thing that I'm worried about is when he grows up and starts to get in touch with technology," he says.

"As individuals and even kids start to get online there's a lot of risk involved there.

"You don't know who is on the other side of things.

"Nowadays, putting an iPad or mobile phone in their hands may be further exposing them and more dangerous than letting them go out on their own."

Jeff Yong Xun Xie is an ACS Certified Professional (Cyber Security).

"I see a lot of IT providers calling themselves cyber experts and just panicking when an incident is reported. They cause panic, particularly with SMBs, by saying 'you had a breach and you need to report it'. But I don't think that's the way to approach it."

David Rudduck

The value of training your staff in cyber. Security skills pay off big time.

David Rudduck

By David Braue

"It was never our intention to focus in this space, but when you're looking at who is likely to use your services, it's clear that they see value in it."

If big businesses think the storied information-security skills gap is hitting them hard, they should spare a thought for David Rudduck's clientele.

As managing director of Gold Coast-based Insane Technologies, Rudduck has long provided technology consulting and security capabilities that the region's largely small business community simply can't afford or manage.

With more than 20 years of technology and security consulting under his belt, he has had time to build those capabilities internally.

"We've always been very careful about security," he says. "It's just the way we are wired."

Long-term investment in security capabilities has particularly paid off over the past seven years, with increasing levels of cyber security attacks raising awareness – and exposure.

Recognising the looming demand for security capabilities, Rudduck has been investing heavily in his own staff.

The firm laid down a concerted program of training and certification, which has proven immensely popular with its employees and boosted staff retention as well as customer satisfaction.

"This path for new hires takes them through a series of information security courses and certifications that I wanted them to achieve," Rudduck says. "And it has been working."

Helping small businesses with big problems

The investment in staff certifications has meant helping a broad range of Gold Coast-based small businesses – particularly in industries flooded with sensitive information such as healthcare, legal services, financial services, and the like.

Increasing legal and governance requirements are pushing those firms to better consider the exposure of their information, and Insane Technologies' investments in focused security capabilities have been just the answer.

"It was never our intention to focus in this space, but when you're looking at who is likely to use your services, it's clear that they see value in it," Rudduck says.

"Because we were so particular about the fact that these companies had certain records they didn't want leaked – and that we took certain steps to prevent that – our approach resonated with these types of clients."

That approach included not only developing internal skills that positioned Insane Technologies as a centre of cyber security excellence, but in regularly engaging with small businesses that often only realised their security exposure after what Rudduck calls "'oh shit' moments'."

"These companies have certain records that they don't want leaked," he explains, "and you can see it on their faces when all of a sudden they realise that this whole cyber thing is

"You can see it on their faces when all of a sudden they realise that this whole cyber thing is actually quite scary – and that they are just as likely to be a target as anyone else."

actually quite scary – and that they are just as likely to be a target as anyone else."

Directing the cyber insurance industry

Cyber security remains a nascent area within Australia's insurance sector, but growing awareness of cyber risk has created opportunities for security consultancies with the proven skills to deal with cyber incidents head on.

For the team at Insane Technologies, this opportunity has rapidly turned into a significant new business after a small insurance industry project led to an introduction which eventually saw Insane's skilled security team tapped to provide on-call incident-response services on behalf of a cyber insurance provider.

Providing a rapid and effective security response is something most small businesses absolutely struggle to do, Rudduck says, but those businesses can significantly improve their chances with the financial backing of progressive insurance companies backed by the forensic security skills of a firm like Insane Technologies.

The partnership created new opportunities for underwriters that have struggled to engage proactively with small businesses that sit off the radar of the conventional enterprise consulting giants.

"Insurance underwriters are used to dealing with the Big 4 for their incident response capabilities," Rudduck explains, "but the only thing more expensive than lawyers is digital forensics."

"Underwriters were concerned that the Big 4 are very expensive, and the SMB market struggles to justify the expense – so after we did a small job for an underwriter, we ended up becoming one of three global response centres that provide follow-the-sun response."

A measured response

Although that sort of contract is a significant win for a security provider, it also requires a higher level of commitment.

Amongst the terms of the partnership, for example, is a requirement that Insane Technologies be ready to respond and triage new incidents within 15 minutes of their being reported.

Particularly in the context of Australia's new notifiable data breaches (NDB) legislation, Rudduck says, rapid triage has become especially important.

"I see a lot of IT providers calling themselves cyber experts and just panicking when an incident is reported," he explains.

"They cause panic, particularly with SMBs, by saying 'you had a breach and you need to report it'. But I don't think that's the way to approach it."

While companies "definitely" need to notify customers if there has been a security breach, Rudduck says, careful analysis and remediation of security incidents is an essential first step.

"Cyber is just the marketing name for information security and governance. But it's something that had to happen, because as incidents occur there is real damage happening."

Despite years of repeated warnings, that analysis phase all too often turns up the same old "really basic things" – "low-hanging fruit" such as remote access servers sitting open to the public Internet; users setting simple passwords, or "really poor" credential reuse that exposes multiple systems when users use the same credentials across business and personal services.

Users habituated to sloppy password habits continue to create challenges for security providers and companies alike, but over time Rudduck has learned that giving users regular ear-bashings about password habits can be counter-productive.

"Whenever we do a cyber security awareness talk, we make a joke about people who have 'holiday1' as their password," he explains. "There are always smirks in the audience. But if you force them to change their passwords regularly, that password just becomes 'holiday2'."

As an alternative, Rudduck's team recommends teaching users to take alternative password approaches, with 12 characters as a minimum and passphrases used to help users remember them.

"If it's long, you have a better chance of remembering it," he explains. "And it's complex."

Ongoing cyber health

Regular exposure to small businesses' routine issues around cyber security have helped Rudduck and his team build a reputation serving niche Gold Coast markets such as film production.

One interesting engagement, for example, saw the firm charged with securing the digital workflow of the nine-month production of the film The Chronicles of Narnia: Voyage of The Dawn Treader.

Regardless of the product or service they provide, Rudduck says, small businesses share many common cyber security requirements and there are many opportunities for those that can provide them quickly and cost-effectively.

"Cyber is just the marketing name for information security and governance," Rudduck says. "But it's something that had to happen, because as incidents occur there is real damage happening."

Growing engagement with cyber insurance providers has reinforced the importance of regular network security health checks, which Insane Technologies conducts for its customers as part of a holistic approach to cyber security defences and effective response.

"You can put in all the technical controls you want, but at the end of the day you're dealing with people," Rudduck says. "And if the controls slow them down, they will find a way around them. You have to look at it from the user's perspective first, then find controls that will work for the business."

David Rudduck is an ACS Certified Professional (Cyber Security).

"If you want to be compliant, you have no choice but to follow these new regulations. All of them. But we also need to balance the business aspects and that's where the complications come into play."

Raymond Frangie

The dangers of 'non-existent' cyber security. Too many smart buildings are at major risk of attack.

Raymond Frangie

By David Braue

"Many construction and engineering companies just don't understand the implications. There is no real consideration for the security of these sensors and networks – and that's where I come into play."

There are three monitors on Raymond Frangie's desk, each highlighting another front in his fight to support the cause of better cyber security.

But even that is a reduction, he admits. There used to be five screens, but he whittled down the number because even 20-year cyber security veterans have their limits.

Not that you'd know it.

As a senior cyber security consultant with global engineering company Norman Disney & Young, he has a box seat into the planning that goes into major building developments including prisons, hospitals, and "almost every single industry there is."

And he isn't sure he's comfortable with what he sees.

Cyber security, he says, is filled with people who understand the risks of the new, connected way of working – and try their best to minimise those risks.

Engineering is also full of people who manage risk for a living but who are inadvertently leaving themselves exposed to a whole new breed of risk.

That risk comes from the increasing interconnectedness of things – both new devices being brought onto corporate networks, and building automation and other engineering systems whose increasingly automated nature makes them sitting ducks for malicious cyber criminals.

"We're seeing smart buildings filled with sensors and the convergence of sensors," Frangie explains, cautioning about the lingering risks of "non-existent" cyber security in an age where ever more sophisticated buildings are being constructed with high-tech features and filled with connected, potentially vulnerable devices.

"Many construction and engineering companies just don't understand the implications. There is no real consideration for the security of these sensors and networks – and that's where I come into play."

Securing the unsecurable

As the firm's lead cyber security consultant in NSW, Frangie's plate is full most days – hence the multitude of monitors on which he works.

He has been heartened by a growing focus on improving cyber security compliance – most notably through new legislation such as the Notifiable Data Breaches (NDB) scheme and the EU's General Data Protection Regulation (GDPR).

But just knowing something has to be done, and making sure it is actually done, are two very different things.

"If you want to be compliant, you have no choice but to follow these new regulations. All of them," he says.

"But we also need to balance the business aspects and that's where the complications come into play."

"Everyone is rushing to meet standards and frameworks like ISO 27001, the NIST Cyber Security Framework, or even Australia's very own Information Security Manual, but collaboration is non-existent."

Complications?

He's talking about smart device manufacturers, for example, who are happy to build sophisticated control systems, voice-activated announcements, load balancing algorithms and many other sellable features into their products.

When it comes to security, however, the same vendors often balk at the expense.

"We see a lot of sensors going into buildings because they provide the availability and data that the buildings want. But they don't understand the implications of having all this data."

"Some vendors will say 'why would we implement security when it's too expensive?' But when you're constructing a building, you may put a device in it that's intended to last 25 to 30 years – and if nobody is touching that and checking its security, hackers will see that as low-hanging fruit."

Going off the rails

Builders might be able to get away with leaving temperature sensors exposed, but in other infrastructure-intensive industries, Frangie is seeing a worrying level of disregard for cyber security – and it could have significant consequences.

Even where there is recognition of the risks, the lack of industry-wide collaboration is leaving soft spots in industries that can't afford them.

Rail networks, for example, have been rushing to develop cyber security standards – but each state has its own, and the level of collaboration between states is alarmingly absent.

"Everyone is rushing to meet standards and frameworks like ISO 27001, the NIST Cyber Security Framework, or even Australia's very own Information Security Manual, but collaboration is non-existent," Frangie explains.

"Unfortunately, it's like other industries where they rush to do things and don't actually understand the implications.

"Many of these standards come from business people, but don't address technical controls.

"And different controls work with different industries."

Education is critically important if these efforts are ever to bear fruit for the long term, Frangie says – and he has seen first-hand just how bad the situation is.

In a previous role doing security audits with an information-security consultancy, he says, "some of these companies just don't actually understand what a cyber security attack is. They don't have the education and awareness to understand that something could cause an attack later."

These companies are generally focused on delivery – which invariably means storing mountains of confidential data in

"We are moving towards a smart future. It's inevitable. And we can't stop the smartness of the world happening – so we need to make sure we have enough cyber security professionals out there."

Microsoft Excel spreadsheets that remain non-password protected, unencrypted and freely distributed via email and USB stick.

Laptops loaded with confidential information go missing all the time, but most businesses don't have a backup plan.

Even small amounts of information, if collected and cross-matched with other information, can become deadly for a company that finds itself defending an egregious breach of customer or partner data.

Building a solid foundation

In industries as critical as construction and engineering, that threat is a constant presence for specialists like Frangie, who sees the industry overwhelmed by insecurity that it doesn't have the wherewithal – or the resources – to address meaningfully.

"I know of a hospital five minutes from here that has a chiller controller exposed to the Internet," he says.

"If you look at the hacker search engines, you can see numerous building protocols just exposed online.

"And what will happen when a hacker takes that out?"

Fixing the problem requires a three-pronged focus – confidentiality, integrity, and availability – which is a lot more than most industries are giving at the moment, he warns.

"Cyber security and information security needs to be in every single part of the R&D project, and every single phase of the execution," he says. "You need to review it before you hit every milestone, and confirm that you have good, dedicated cyber security staff dedicated to this."

Few of those staff would have been in the game as long as Frangie, who has a list of industry certifications as long as your arm, including formal qualifications such as a Master of Information Systems Security, and the first person in NSW to be awarded the ASC Certified Professional (Cyber Security) qualification.

He will also begin teaching Computer Security to undergraduates at Western Sydney University next semester and is looking forward to doing his part to help an industry that is crying out for qualified cyber security professionals.

Those professionals will face intimidating odds as the continuing explosion of the Internet of Things (IoT) – whether inside buildings or outside of them – promulgates new potential security breaches in their millions.

"We are moving towards a smart future," he says, noting industry predictions that the world will have a trillion Internet-connected sensors within the next few decades.

"It's inevitable. And we can't stop the smartness of the world happening – so we need to make sure we have enough cyber security professionals out there."

He's certainly in it for the long run.

"I enjoy cyber security because I get to spread my wings," he says.

"There are so many engineering aspects that I don't think I'll be getting bored any time soon."

Raymond Frangie is an ACS Certified Professional (Cyber Security).

"There don't seem to be any levers that company directors can pull to exert control over the information in their organisations. They largely sit back and rely on the best efforts of their CISO if they have one – and take their advice. But everyone's advice is going to be different."

Craig Horne

Why business needs cyber security in-a-box. Not everyone can afford a $250,000 CISO.

Craig Horne

By David Braue

"It's really quite confronting and bizarre that in this day and age, some organisations with very large security budgets can still suffer a ransomware attack and lose weeks of productivity for an entire global organisation."

Craig Horne may be an academic now, but it was the years he spent working in signals intelligence as a military reservist that made it clear to him just how important information security is.

Hostile forces – and, often, even friendly ones – were intensely interested in intercepting secret communications. The primary role of signals intelligence experts is to ensure that doesn't happen.

That work "gave me insight into how information can be protected in some of the most hostile environments in the world," Horne recalls.

Horne left the Australian Army Reserve after 14 years and has leveraged his expertise into a technical career that has included sales, business analysis, project management, and other roles.

It was a logical progression for someone who was, as Horne puts it, "a bit of a lockpicker as a kid". But it was also the gateway into a long-running career that has taken Horne from the battlefields of the Middle East to the front line of corporate technology sales and administration.

Horne's stint as a reservist came about after years working as a system administrator, fresh out of university.

He wanted to investigate career options in the military but "didn't want to become institutionalised," he recalls. "I'd always had a civilian career."

As a compromise, he opted for a reservist career that would allow him to enjoy the best of both worlds.

That time helped him hone his security skills through his reserve work, during a period in which he completed a Master of Business Administration and became acutely aware of the corporate challenges that cyber security posed for businesses of all kinds.

This extended to directorial advice, and Horne soon found himself applying his business and cyber security skills in an advisory capacity.

Strategy in a box

One of the recurring themes during Horne's advisory work was just how hard it is for businesses to develop a consistent and effective cyber security culture, across departments and boardrooms.

Company directors need solutions to their problems, not just explanations of their problems – and that gave him an idea about a way to combine his strengths and interests.

"There don't seem to be any levers that company directors can pull to exert control over the information in their organisations," Horne explains.

"They largely sit back and rely on the best efforts of their CISO [chief information security officer] – if they have one – and take their advice. But everyone's advice is going to be different."

The resultant project has been one of Horne's biggest endeavours.

He is currently working towards towards a PhD at the University of Melbourne, where he is trying to distil the best-practice elements

"The issue, as I see it, is that organisational boundaries are becoming more porous. The idea that corporations were fortresses where you could put up castle walls and protect your information, is long gone."

of information security into a repeatable, effective series of steps that any director can follow.

Strategy in a box, if you will.

It hasn't been easy going. Since he began research in April 2014, Horne has conducted interviews with dozens of CISOs at "some of Australia's largest organisations".

Several consistent themes have emerged from the research, which Horne has honed into a two-pronged framework for understanding effective data security.

First, companies need to understand the value of their data. This includes the identification and assessment of the value of the organisation's data – which can often be harder than expected to ascertain.

Second, companies need a clear understanding of the barriers, constraints, and threats to information arising from access by third parties.

These threats may be explicit – as in the constant threat of outsider compromise – or completely hidden, as when data is stored on a cloud service that replicates it into other jurisdictions.

"Suddenly you've got a GDPR issue without even knowing it," says Horne.

Such threats are part and parcel of doing business in today's information-driven world, and they require institutionalised mechanisms of control that continue to be hard to develop and maintain.

"The notion of control is changing," Horne explains. "In the past, control was highly prized – and it was the price that organisations paid to achieve flexibility, collaboration, scalability, cost-effectiveness, and the other benefits of the cloud."

Even as companies now try to wrestle back that control, they are finding that it hasn't been easy at all.

"The issue, as I see it, is that organisational boundaries are becoming more porous," Horne says. "The idea that corporations were fortresses where you could put up castle walls and protect your information, is long gone."

Rebuilding the castle walls

New technological development – including cloud-based storage, social media and mobile phones – ended the days of perimeter-based security.

Sensitive data is flowing within and between these domains at an unprecedented pace, and companies simply aren't keeping up.

"My research so far is showing that even large organisations are not paying enough attention to these porous boundaries," Horne says.

"Some are, and some aren't – but it's really quite confronting and bizarre that in this day and age, some organisations with very large security budgets can still suffer a ransomware attack and lose weeks of productivity for an entire global organisation".

Fixing the situation will require, among other things, efforts to better understand and proceduralise the process of applying information

"In the past, control was highly prized – and it was the price that organisations paid to achieve flexibility, collaboration, scalability, cost-effectiveness, and the other benefits of the cloud."

security within a corporate context.

This is where Horne's idea for a 'strategy-in-a-box' solution continues to resonate – and where he hopes to make a difference by helping companies muster the executive support to address the security loopholes that are so regularly compromised.

As he wraps up his PhD work, Horne is working to commercialise his findings and help different kinds of businesses get a better grip on the exposure that their newly transformed businesses are creating.

Getting there won't be easy, he admits. But he's counting on support from the many companies that can't afford $250,000 CISO salaries – and need any help they can get through other means.

The key to getting the message through, he believes, is not only winning hearts and minds in the boardroom, but getting all members of the ecosystem onboard.

University settings, such as the one where Horne spends most of his time at the moment, are a great example.

"Researchers travel globally and collaborate with other researchers," he explains. "They're in a situation where information is required to be shared across borders and network boundaries, yet still remain secure and accessible."

"If you impose security controls on them to the point where it becomes unusable, you will retard productivity."

A time for compliance

To whatever extent his idea for cyber security-in-a-box transforms executive awareness of cyber security imperatives, Horne's commitment to improving cyber security practice has taken his career in other directions as well.

He has been active within ACS for several years. Previously he was the Chair of the Victorian branch, and this year expanded that role to become national Vice President.

The timing couldn't have been more interesting or relevant to his work, Horne says. With Australia's new notifiable data breaches (NDB) scheme having come into effect in February and GDPR in play in May, notions of information control are more important than ever.

Requirements for compliance with these standards vary widely between organisations but Horne says the general lack of awareness is likely to drive his work in many valuable directions.

"I'd love to be able to help provide really pragmatic, practical advice and steps that would guide company directors on how to secure their company information," he says.

"At the moment it seems that most advice about security is at an operational or technical level – and it would be great if that could be turned around."

Craig Horne is an ACS Certified Professional (Cyber Security).

"Maintaining client legal privilege is extremely important and it's what clients expect. Law firms handle a lot of sensitive information, and it is of the utmost importance that the confidentiality of their clients is maintained."

Georg Thomas

Protecting privileged information.
How does cyber security impact legal ethics?

Georg Thomas

By Edward Pollitt

"I think in the next probably six to 36 months, we're going to start seeing the CISO (Chief Information Security Officer) role transitioning to CSO (Chief Security Officer)."

In the legal world, when a client shares confidential information with his or her lawyer, they can rest easy in the knowledge that this information will be protected.

Legal professional privilege protects confidential communications and documents shared between a lawyer and client.

If a lawyer breaches this confidentiality without the client's permission, they may be liable for a breach of contract and could face ramifications.

But what happens if this sensitive information falls into the hands of someone else?

When it comes to cyber security, that someone could be a penetration tester – employed to "ethically" hack a system to find unknown vulnerabilities.

If a law firm hires a penetration tester, there's a risk that information protected under professional privilege may be exposed as part of the testing.

Is this something that then needs to be disclosed with the client? Does the penetration tester now have a duty to protect the confidentiality of this information?

These are the kinds of questions that Georg Thomas grapples with daily.

Based in Melbourne, Thomas is the National Security & Risk Manager at commercial law firm Corrs Chambers Westgarth.

Speaking with *Information Age*, he broke down this ethical question piece by piece.

"Maintaining client legal privilege is extremely important and it's what clients expect," he says about this ethical issue.

"Law firms handle a lot of sensitive information, and it is of the utmost importance that the confidentiality of their clients is maintained."

Experience in the field

Having worked in penetration testing earlier in his career, both as a tester and manager, Thomas understands that sometimes you might gain access to something that is not for your eyes.

From there it comes down to good management, he says.

"A penetration tester may inadvertently gain access to such [sensitive] information and it really comes down to how that is then handled and what controls are in place to deal with those scenarios."

"For example, before the engagement commences, it's fundamental to ensure a non-disclosure agreement has been executed. Testers must also be required to immediately notify the firm if they gain access to anything that is potentially sensitive."

But handling data that is not your own is becoming increasingly complicated and regulated.

Recent law and regulation changes, such as the Notifiable Data Breaches scheme and EU General Data Protection Regulation (GDPR), require an organisation to know

"A penetration tester may inadvertently gain access to such [sensitive] information and it really comes down to how that is then handled and what controls are in place to deal with those scenarios."

where its data is and how it is being used.

As well as facing such issues at a professional level, Thomas also has an academic perspective on the topic.

Currently completing a PhD through Charles Sturt University, his thesis looks at the issue of professionalism and ethical hacking in law firms and as part of his research he is speaking with relevant professionals.

"We've had discussions about what the requirements of penetration testing are, should be, and whether disclosure is required," he noted.

"From a client perspective it comes down to the age-old question of: 'What comes first? The chicken or the egg?'

"There's the expectation that a firm is doing its due diligence, conducting security reviews, and getting the appropriate tests done to help provide some level of assurance that its security is adequate.

"On the flip side, there may be a requirement to notify in the potential event of disclosure.

"Solid vetting of the security professionals themselves, appropriate contractual requirements, and also making sure that scoping of engagements is undertaken to ensure that anything that is sensitive is excluded from the engagement is key."

Security on Wall Street

Thomas's current role with Corrs Chambers Westgarth has him assessing information security risks at the independent Australian law firm.

He explains that this largely involves broadening security approaches beyond a technical focus.

Only returning to Melbourne recently, it was four years in New York that showed Thomas the high stakes of cyber security.

Beginning his security role as Director, Information Security Management at technology consultancy firm Kraft & Kennedy in 2013, he arrived in New York just in time for one of the most significant breaches ever seen.

"I think the JP Morgan breach for me was the breach that really stood out," he says about the 2014 attack that was believed to have compromised data from 76 million households.

"Because at the time that I moved to the US, I was consulting to law firms, and a lot of the financial institutions had started to really focus on supply chain management. These financial institutions were starting to conduct thorough risk assessments against their third parties, something that we are now starting to see more of here.

"I had actually been engaged by a lot of firms in the US to assist them with these overwhelming [compliance] questionnaires and it became fairly evident at that stage

"Solid vetting of the security professionals themselves, appropriate contractual requirements, and also making sure that scoping of engagements is undertaken to ensure that anything that is sensitive is excluded from the engagement is key."

that there was a lot of work to be done in that area."

Following his law firm consultancy work with Kraft & Kennedy, Thomas changed beats in 2015 when he joined leading tax and advisory firm Grant Thornton in a role that saw him consulting to SEC-regulated companies and Fortune 500 companies.

It was in this role where he led a team of ethical hackers to test the security controls of these colossal companies.

And the experience of replicating the mindset of a hacker has been invaluable, he says.

"It helped me understand how a hacker thinks," he explains.

"When you understand that technical level of detail 'if I want to get to from point A to my target at point B, how am I to go about doing that? I need to consider what security controls are in place and how to get around them as well as what systems I can exploit to meet my objective.' That knowledge helps me identify vulnerabilities and risk areas that I can then work to remediate.

"I think it has been invaluable having that very deep technical background in the security field."

Then versus now

With law firms, financial institutions and tax advisories all in his repertoire, Thomas has spent much of his career working in industries with clients that can't afford to be breached.

And through this career he has seen dramatic change in the cyber security industry and in the attitude of his clients.

"It's chalk and cheese," he says about then versus now.

"Where they are now is far more advanced than they were four or five years ago.

"I wonder whether a lot of that change had been client driven. That's certainly been my experience – that the clients have helped drive change in security culture in many instances.

"As I observed in the US when I was there, we are starting to see an increase here from clients to complete security assessments so they can validate that everyone in their supply chain has an appropriate level of security controls."

He also believes we are on the verge of an industry-wide change when it comes to management.

With the focus now broadening beyond purely technology security and risk, security managers will take on further responsibility.

"I think in the next probably six to 36 months, we're going to start seeing the CISO (Chief Information Security Officer) role transitioning to CSO (Chief Security Officer)," he says.

"Security executives and managers are now not solely focused on technology security, but are branching outside that and becoming more generalist.

"It has started already happening, but I think we are going to see an increase in that the focus isn't just on information security; it's on security in general.

"It's a big job, but someone has to do it. I think that it's going to really benefit the security of an organisation with this much broader view."

Georg Thomas is an ACS Certified Professional (Cyber Security).

"In the late 1980s, computing was relatively embryonic in businesses, and it was all very centralised with very limited interconnection to the outside world. Similar attacks to those today already existed, people were hacked into via their modems, and there very much were computer fraud issues in the early days. But it was limited by the technology, and the problems were related to the state of the technology."

David Thompson

The next era of cyber security.
IoT will change everything.

David Thompson

By David Braue

"The early fraud challenges – around the value of digital information and the ability to copy, duplicate, and misuse it for personal or competitive advantage – still exist."

A former police officer detective who was among the first people in the world to run a dedicated computer crimes division, David Thompson has seen it all.

Starting from scratch in the late 1980s, Thompson – then a ten-year fraud investigator with the Victoria Police – set up and lead the Computer Crime Squad for a further 10 years before retiring to the private sector during the 'dot com' boom to commence his current role as an information security and forensics consultant.

His current firm, FSR Consulting, provides cyber security consulting and digital forensics capabilities to companies that are increasingly wrestling with the complexities of security in an era of digital transformation.

Yet those complexities are not just the result of innovative new cyber security compromises and attacker tactics, Thompson says.

Rather, the evolution of cyber security risks over the last 30 years has been driven largely by the immediacy provided by increased connectivity.

"In the late 1980s, computing was relatively embryonic in businesses, and it was all very centralised with very limited interconnection to the outside world," he recalls.

"Similar attacks to those today already existed; people were hacked into via their modems, and there very much were computer fraud issues in the early days. But it was limited by the technology, and the problems were related to the state of the technology."

Over time, however – and particularly as the Internet emerged and then grew to become a global communications force – the massive scale, ease of interconnectivity and security best practices risks rapidly evolved industry exposure to increased potential criminal exploitation.

The interconnectedness of things

Working in the private sector, Thompson regularly sees common and persisting issues creating vulnerabilities for organisations.

"The early fraud challenges – around the value of digital information and the ability to copy, duplicate, and misuse it for personal or competitive advantage – still exist," he explains.

"It's really about misuse of systems that people are entrusted to use for their day-to-day work."

Businesses are still struggling to recognise the value of their information before wayward employees or outsiders do – and this, Thompson warns, is creating endemic vulnerabilities that executives are failing to tackle head-on.

"People have become more aware of cyber security issues over time, but they have many other business issues to focus on as well," he says.

"It's really about misuse of systems that people are entrusted to use for their day-to-day work."

"This has made it slow to get the attention of senior business executives – which means that organisations need to call in consulting assistance to give cyber security the proactive and reactive attention needed."

Organisations would be well advised to call in that assistance sooner rather than later. With the Internet of Things (IoT) paradigm rapidly adding new vulnerabilities and touch points to enterprise networks, Thompson warns that things are about to change dramatically once again.

"We are right on the cusp of a major technology explosion into what people are calling the hyperconnected world," he explains.

"This is that world of IoT, smart systems and ubiquitous computing in which everything is connected to everything, and digital things are being connected to physical things."

"It's a new phase of the digital world, like when the Internet came along, and the threats and potential issues have a greater potential of occurring."

Think forensically

With Australia's notifiable data breaches (NDB) scheme and the European Union's general data protection regulation (GDPR) now in place and consumer data right (CDR) legislation looming, Australian organisations must have a better grip on their data and tighter controls over it than ever before.

Those regulations "are helping people realise that this is a critical issue for business," Thompson says, "and that they will need to be able to identify data breaches and report them when they affect other people."

"It's raising the awareness of the obligations of everybody to protect and respect others' personal data."

To meet the requirements of this heightened regulatory environment, Thompson says, businesses should be investing not only in defensive technologies but also working hard to implement proactive monitoring and logging tools that track exactly what is happening in their environment.

"We're at a point in time," Thompson explains, "where the digital world is rapidly changing and about to expand into a whole new period where physical cyber connections, smart autonomous systems and IoT devices will bring new risks and increased potential for breaches and attacks."

Such capabilities not only offer direction for forensic investigators in the event of a breach, but when paired with automation they can improve and hasten the company's ability to quickly detect and respond to security incidents.

"The more that people have recorded in their system, the more prepared they are for investigations of the facts," Thompson explains. "Proactive monitoring and logging are very important to help respond to an incident."

"It's raising the awareness of the obligations of everybody to protect and respect others' personal data."

Matching threat levels and threat response

That ability – or the lack thereof – is what keeps Thompson up at night.

The biggest threat we face at the moment, he explains, is "the complexity of systems and the ability of owners and operators to truly understand what their systems are doing – and what they're interconnected with."

"Forensic rigour is required to investigate and prove what has occurred to a high enough level of proof, whether in a commercial dispute situation or a complex legal situation."

"We need a more robust and thorough version of the things that we talked about 30 years ago."

By inventorying their data assets and implementing secure process structures, companies can keep themselves ahead of potential compromises and minimise their exposure to the fast-expanding interconnectedness of things.

Yet with the three key defensive tactics – including cyber security and digital risk issues in broader risk management frameworks, undertaking regular threat and vulnerability assessments, and monitoring and logging system and user activity – Thompson also warns of the importance of a fourth key element.

That element is cultural change – ensuring that staff understand the issues at hand and the threats they face, as well as their role in the corporate response.

Ultimately, companies should have in place a holistic program that allows them to understand what their risks are, what controls they should put in place, and how to respond if they unfortunately have an incident.

"It's a matter of choosing those controls to meet the level of concern you have about the threat," Thompson says. "It's never going to go away; it's a totally digital business world now, and digital security issues are just a part of normal business."

David Thompson is an ACS Certified Professional (Cyber Security).

"One of the things I learned very early on was that when we are developing something, you can't just do that in isolation, we need stakeholders involved, ideally at several levels in the organisation. This feedback loop is both useful and satisfying; seeing what you've implemented being used by other people is one of the things I get a real buzz out of."

Jennifer Ellerton

The breach is coming from inside the house. Who has the right to access information?

Jennifer Ellerton

By David Braue

"A team of us analysed the business situation, then designed, engineered, and deployed a whole enterprise software platform from scratch. It was years later that people started calling this 'digital transformation'."

It was early in her career that Jennifer Ellerton learned the importance of bringing information security into the discussion early on.

Working as a software engineer with software giant Oracle in the 1990s, she was involved with projects including the development of an enterprise platform for the Western Australian Department of Education and the WA's Department of Transport's Online Register of Encumbered Vehicles (REVs) – "one of the first cloud solutions rolled out in WA," she recalls.

Those and other projects reinforced information-management concepts she had learned while completing her Bachelor of Computer Science Honours just a few years earlier.

"A team of us analysed the business situation, then designed, engineered, and deployed a whole enterprise software platform from scratch," she says of her work in building centralised databases and software designed for high availability and sensitivity.

"It was years later that people started calling this 'digital transformation'. I came from a background where we took risk and security very seriously from the beginning."

Security into business

That security nous was reinforced over time, with Ellerton programming bespoke applications and Oracle integrations using ETL, API, Java, PL/SQL, C and C++.

Yet despite her evolving awareness of data integrity and security issues, it was the business aspects of her degree work that helped focus her interests in applications and information security.

"I realised that I loved two things," she recalls. "One was the software related to business, aka business-aligned software, and second was the interaction with people."

"Learning Oracle was a wonderful grounding for me because it meant I could reach out to the international market."

That opportunity came when Oracle's US headquarters recruited worldwide for developers to work on its ERP suite within its R&D department.

Ellerton was one of two people chosen from the Australian team, and thus began an international career that included stints developing Oracle for oil and gas producers; managing a multi-lingual technology team delivering data solutions for SwissLife in Zurich; and managing teams from geographically-diverse locations to deliver major client-facing ICT projects as a director of Morgan Stanley in New York City.

In 2013, Ellerton returned to Australia after nearly ten years

"I realised that I loved two things. One was the software related to business, aka business-aligned software, and second was the interaction with people."

abroad. She set out to apply that international experience to help Australian organisations strengthen their information security policies, tools and procedures.

She took charge of managing sensitive health data and formalising partnerships to set up CAP-compliant labs for a medical research start-up which has since been acquired.

In her current role as an independent contractor – via consultancy Managed Information and Cybersecurity (MIC) – she is working closely with a WA engineering firm protecting their information.

She reflects on 20 years of real-world project implementations and notes that the importance of information security has only grown over time.

"We've been working in digital transformation and modernising infrastructure," she says. "But it's critical to make sure that strong information security tools and procedures are in place."

Improving cyber security awareness

There's increasing awareness around the importance of information security, Ellerton says, noting that executives have come to the table thanks to a growing climate of data governance and compliance requirements.

"The emphasis has shifted," she explains, "because there have been breaches, and the government has put legislation in place – plus, the media is actively reporting on these topics."

"Now you have some executives who didn't take much notice of their data in the past taking notice. It's a conversation that's already started, and it makes my job easier when I talk with executives."

Yet simply starting that conversation is only part of the cyber security engagement: it has to be both deep and enduring.

This includes a high-level commitment to addressing cyber security from an executive perspective – which includes clear reporting structures – and a CISO who reports directly to the CEO.

Leveraging this structure allows the creation of agile feedback loops in which risks can be identified, projects structured and executed, and feedback secured from all levels of the business within a short period.

"One of the things I learned very early on was that when we are developing something, you can't just do that in isolation, we need stakeholders involved, ideally at several levels in the organisation," Ellerton explains.

"This feedback loop is both useful and satisfying; seeing what you've implemented being used by other people is one of the things I get a real buzz out of."

"Executives need to pay attention because culture comes from the top – and they need to ensure that the person looking after digital transformation is taking security very seriously."

Ensuring effective security throughout this process requires careful attention to key cyber security elements such as management of privileged accounts and other internal controls.

"The defence in depth approach is important, but there is also the insider threat," she says. "That's what I focus on – looking at the data within the organisation and implementing a need-to-know basis for data access."

"And that means involving the whole organisation, looking at the roles within that organisation, and determining exactly which people should have access to which areas. This process has been similar in all of my projects."

Insider threats are a recurring and often underappreciated issue in even the most progressive organisation. The Verizon Data Breach Investigations Report (DBIR) 2018, for one, noted that up to 28% of breaches were due to internal actors – although this surged to 56% of breaches in healthcare environments.

The risks of transformation

Managing data – and access to that data from both outside and inside the organisation – is therefore critical for any cyber security culture.

And while she has learned enough over the years to know what goes into a successful cyber security infrastructure, Ellerton also knows what can go wrong.

With many companies only recently taking cyber security seriously, she says, compromises such as the recent PageUp data breach highlighted the inadvertent risks that employees face – often despite the best intentions of their employers.

"What's worrying about [PageUp]," she says, "is that it shines a light on how easily our personal data can be exposed. It could happen to any of us."

Digital transformation-minded executives need to heed these risks and imbue their drive for change with a constant reminder of the humanity of what they are looking after, she said.

"It's really important that we understand that when there is a data breach, it's actually someone's personal data."

"Executives need to remember these breaches carry serious risks to the organisation," she continues, and that "ordinary people and the media are increasingly aware of the danger of potential for their data to be lost.

"Executives need to pay attention because culture comes from the top – and they need to ensure that the person looking after digital transformation is taking security very seriously."

Over time, this culture – supported by privileged access controls – will drive enduring transformation at the employee level, Ellerton says.

"Your people need to be not only aware of security risks, but need to have DNA inside them that says, 'I've got to be really careful about every click that I enter into the system'," she explains.

"Information security is something that everyone needs to be involved with – and it's all got to start somewhere."

Jennifer Ellerton is an ACS Certified Professional (Cyber Security).

"That's where you understand that some of that security is a bit of a trade-off. It's a bell curve between flexibility, convenience, and security. You can make it very easy for people to walk up, check in and jump on a plane – but how do you know it was the right person, and that you've asked enough questions to prove who they are?"

Nick Brant

Data under constant attack.
Why you should live and breathe security.

Nick Brant

By David Braue

"Some ideas are good ones, but they just move from the manual and analogue world into the digital world."

Recent decades have seen researchers looking for ever-stronger methods of public-private key encryption, even as law-enforcement authorities enlist the federal government in a war on the technology's wrongful use.

But with so much focus on the current encryption debate, it's easy to forget that some of the best encryption ideas were invented decades ago – long before the advent of the modern computer. One-time pad (OTP) methods, for example, were first described in the 1880s and used a method of paper-based key tapes that was considered unbreakable throughout the military conflicts of the 20th century.

Such methods may now seem antiquated to many, but a renewal of thinking around interception-proof encryption means "some of the stuff we had in the manual world is making a comeback," says Nick Brant, Chief Information Officer with Brisbane-based accounting and business advisory firm BDO.

"Some ideas are good ones, but they just move from the manual and analogue world into the digital world."

Brant completed a BSc in computer science at the University of NSW, and subsequently completed a graduate diploma of information systems at the University of Canberra.

But it was during his military service, in the Royal Australian Corps of Signals (RASigs), where he learned the ins and outs of OTP and other encryption methods used to fulfil the fundamental mission to secure the communication of information.

He has subsequently been able to leverage the mindset he developed at RASigs in a range of information-management positions at the likes of Virgin Blue, GHD Group, Brisbane City Council and now BDO Australia.

And as the government rails against encryption that's too strong for it to circumvent, Brant says, the high profile of encryption is feeding renewed considerations about the best way to protect data in a climate of constant attack.

The endpoint problem

In an enterprise context, growth in the number of endpoints used within businesses has become a significant problem for any company.

Brant learned this first-hand at airline Virgin Blue (now Virgin Australia), where the need for extremely strong authentication capabilities was balanced with customers' demand for convenience through features like online check-in and self-service kiosks.

"That's where you understand that some of that security is a bit of a trade-off," he says. "It's a bell curve between flexibility, convenience, and security. You can make it very easy for people to walk up, check in and jump on a plane – but how do you

"People always had sensitive client records locked in their businesses – but you had to go to the business to take them, whereas now you just have to go to a keyboard."

know it was the right person, and that you've asked enough questions to prove who they are?"

That consideration is a real issue in conventional enterprise deployments, as well.

As businesses wrestle with reining in bring your own device (BYOD) policies that have seen them flooded with employee smartphones and tablets, enterprise security managers must balance the need to securely authenticate users with the need to not make that process unduly burdensome.

That's why two-factor authentication (2FA) has grown in popularity, since it combines conventional password-based authentication with a layer of security based on a message delivered to a hardware device.

Those authentication codes aren't generally used for encryption, but they could be – and that's why Brant sees importance in remembering where we've come from when planning contemporary endpoint-security policies.

"Security isn't anything new in a digital world," he says. "It's always been around, but these days it's probably a bit more front-of-mind. People always had sensitive client records locked in their businesses – but you had to go to the business to take them, whereas now you just have to go to a keyboard."

The other security problem

Authentication is only one of the problems setting the agenda for today's information-security managers. The other significant endpoint that must be secured is humans themselves.

That can be even harder than securing devices, since humans have a habit of doing unpredictable and habitual things even when they've been told not to – like clicking on emails that may well lead them to malware.

"Sometimes technology isn't always the answer," Brant says. "People still open spam emails and click on the wrong link, and in the cold hard light of day you show them and they say, 'I don't know why I did that'.

"It's normally when they're rushing, multitasking, finishing a few emails as they race out the door. The only way to stop them, technically, is to stop all emails and that's not feasible."

More workable alternatives include actively testing users' clicking proclivities by subscribing to a self-spamming service, as well as encouraging (or forcing) them to undergo online training courses, webinars, and other activities.

Brant also points out the merits of threat-intelligence services – which offer better analytical tools for keeping up with the general threat climate, and correlating user activities to known dangerous sites – as well as the need to keep on top of

"I had good habits drilled into me in the military days. Security is just an integral part of everything you do, and sometimes the easiest way to get rid of a data risk is to just purge it."

patching the many applications used in the typical enterprise.

"You've still got many businesses out there that are still on unpatched software and doing no maintenance," he said. "They have never changed their passwords."

"It's just a risk waiting to happen, unfortunately, and I don't know how you get the message across."

Getting the message across

Ultimately, both past and current experience have reminded Brant that security in enterprises, as in the military, is something that must be lived and breathed every day.

Regular security drills and tests are a significant part of this. "It's like being a firefighter in that you train for the unfortunate situation," he explains. "It's for a situation that you don't want to happen."

That includes regular liaisons with board and C-level executives to frame the current threat climate in terms of business risk and compliance with mandates such as privacy protections and the looming threat of sanctions under the notifiable data breaches (NDB) scheme.

"The beauty of NDB is that it raised the issue at the board and executive level, and it became easier to have those non-technical discussions around the data and the risks it poses.

"It has been easy for organisations to get the support of executive committees to put more rigorous processes in place so that things aren't, for example, just put online.

"They need to be assessed and approved, with consideration of the implications if it does get breached."

That includes evaluating the need for processes that rely on personal data – for example, the use of driver licences for authentication – and a cold hard look at how long that data must be retained.

"I had good habits drilled into me in the military days," Brant says. "Security is just an integral part of everything you do, and sometimes the easiest way to get rid of a data risk is to just purge it.

"Every new project, and every new system, must be considered in the same way we look at availability and maintainability, performance, and redundancy.

"It's all about that matrix between flexibility, convenience, and process; to make sure you keep security at the endpoint."

Nick Brant is an ACS Certified Professional (Cyber Security).


For details on how to become
an ACS Certified Professional
(Cyber Security), visit acs.org.au.
Shift
CYBER SECURITY
CYBER SECURITY

ACS
International Tower One
Level 27, 100 Barangaroo Avenue
Sydney NSW 2000

P: 02 9299 3666
F: 02 9299 3997
E: info@acs.org.au
W: www.acs.org.au