Microsoft

Navigating the new cybersecurity threat landscape

How to securely accelerate your digital transformation

Foreword

Ann Johnson
Vice President, Strategic,
Enterprise & Cybersecurity
Microsoft

Cybersecurity is difficult and it's not going to get any easier. Running a large environment means managing huge volumes of attempted breaches every day. This is big business. Cybersecurity Ventures estimates cybercrime will cost more than $US6 trillion a year by 2021.

Given the sheer volume of attacks, it should come as no surprise that the Australian Cyber Security Centre (ACSC) reports that 90 per cent of companies listed on the Australian Securities Exchange have experienced some sort of data breach. The Australian Government estimates that cybercrime costs the national economy up to $17 billion a year.

Digital transformation has raised the stakes, with 69 per cent of senior executives telling Forbes that this is forcing fundamental changes to security strategies. If you're going to open your organisation up to new customers, new markets and anytime, anywhere access, you need to do it securely.

This report is not meant to scare. Rather, it's designed to educate and inform. While stories about high-profile data breaches justifiably attract headlines, it's important to keep things in perspective.

Microsoft recently hosted a group of cybersecurity leaders from some of Australia's best-known companies and government departments. We wanted to explore how these threats manifest in their world and get their views on new regulations coming into effect in 2018. It was also an opportunity to hear how they find and retain talent in a highly competitive market, while exploring the value of public and private sector partnerships.

We plan to build on this valuable discussion with future events involving more Australian cybersecurity experts. As business and technology leaders we have a shared responsibility to address the challenge. Forums like this support our collective goals.

Executive summary

People are still the biggest cybersecurity threat for every organisation. Not some hooded hacker in a faraway country but the employees unsuspectingly clicking on malicious links as they go about their daily business. Although technology helps, there’s still a need for continuous learning to minimise risk.

Instead of focusing on the number of people who still click on malicious links, there’s great value in encouraging people to report suspicious emails. This proactive approach has the potential to turn your whole organisation into an early warning system.

Cyber leaders are worried about rapid growth in the number of sensors connecting to the internet of things (IoT) because security measures are often lagging or tacked on after the fact. Recent high-profile attacks have been relatively unsophisticated, which means we must focus on securing systems now in readiness for an inevitable wave of more sophisticated attacks.

Senior executives generally have three cybersecurity concerns – staying out of the news, minimising costs and avoiding unnecessary project delays. Many company directors aren’t adequately informed and place too much faith in the security measures implemented by their organisation.

Supply chains are a weak link for every organisation because of the complexity of the ecosystem. In some cases, it can be very difficult to get third parties to meet compliance standards. Some of the world’s most high-profile cyberattacks have been launched through external suppliers and this continues to worry Australia’s leading Chief Information Security Officers (CISOs).

When disaster strikes it’s important to get out ahead of the problem, communicating quickly and clearly wherever possible. But this can be difficult because it’s often hard to know exactly what’s happened in the immediate aftermath of a cyberattack.

Computer science graduates don’t necessarily make the best cybersecurity hires. Australian CISOs are tackling skills shortages with graduate training programs while hiring an eclectic mix of talent including military veterans, psychologists and communication specialists.

Leading public and private sector CISOs already communicate regularly but there’s still room to improve knowledge sharing between government departments and industry. There’s great potential for banks, telcos and utilities to drive industry-wide collaboration on a global scale.

Cyber can no longer be an afterthought. Security teams must avoid being seen as a roadblock and work with application development teams to help achieve goals without unnecessary disruption. Security is a team sport and everybody needs to be part of the solution.

> “Everything is moving so quickly but my biggest concern is that The Shadow Brokers are sitting on some clever stuff right now and just waiting to pull the trigger.”
>
> **Narelle Devine**
> CISO, Department of Human Services

Chapter 1

The threat landscape

Human behaviour is and will continue to be your biggest cybersecurity risk. Technology helps but will never replace the need to train your people. Look for opportunities to make everybody in your organisation part of team security. The cognitive diversity that comes from engaging people with different perspectives and skillsets will greatly increase the strength of your defence. Beyond the universal threat of human behaviour, cyber threat looks different from one industry to the next. Understanding your specific risks will help you develop a plan to minimise exposure. When it comes to dealing with third-party suppliers, asking for compliance certifications will demonstrate a commitment to your data security.

Chapter 1 – The threat landscape

We're only human

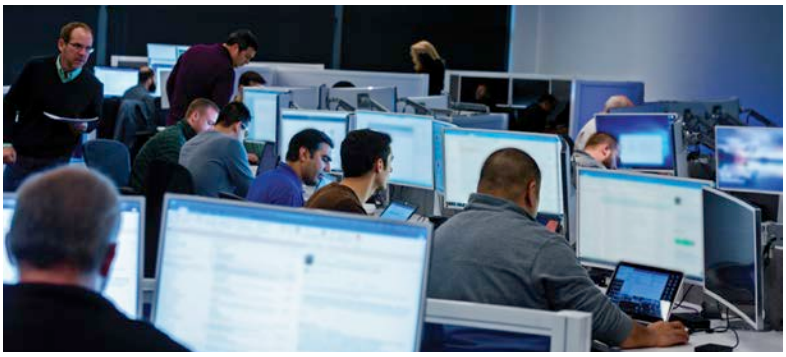
The threats that worry security teams vary from one organisation to the next but some are universal. One stands out – human error. According to Verizon's latest Data Breach Investigation Report, two out of every three instances of malware linked to data breaches were installed via malicious email attachments. Phishing attacks are a fertile hunting ground for hackers.

Recalling a time when his team ran a phishing test with an email from a fictitious delivery company, Telstra's CISO Craig Hancock was disappointed to find 30 per cent of people clicked on the link.

Microsoft Vice President, Strategic, Enterprise & Cybersecurity, Ann Johnson recalls a similar incident at a leadership offsite, where her team phished the 800 attendees by asking them to select a meal for the opening dinner. More than half took the bait. She says there's a need for continuous training but admits this is something the whole industry is bad at.

In fairness to the people who unsuspectingly click on phishing links, some of them are highly sophisticated and look like genuine messages from reputable sources. It's almost impossible to spot one of these malicious emails so it's hardly surprising people make mistakes. This is why tech controls are needed to support user awareness training.

IT departments have been talking about the need for security education for as long as people have had personal computers.



But as automation gathers pace, a new question comes to mind: Will technology tools get to a point where user error can be taken out of the equation? As much as it would make their lives easier, our panel doesn't think so.

Instead of continuing to obsess over the percentage of users who click on a phishing attack, former ANZ Banking Group CISO Steve Glynn says organisations should put more focus on a different metric. Now consulting on privacy and cybersecurity as a principal with elevenM, he suggests there would be greater value in tracking the number of people who report incidents.

"We're measuring the wrong thing," he says. "We should be focusing on the number of people who report a phishing attack because that turns everybody into a potential early warning system like canaries in a coalmine. That's a cybersecurity metric we'd all like to see increasing."

"We're measuring the wrong thing. We should be focusing on the number of people who report a phishing attack because that turns everybody into a potential early warning system like canaries in a coalmine."

Steve Glynn
Principal, elevenM Consulting

Chapter 1 – The threat landscape

Emerging threats

If user error is the most common concern among security teams, what keeps their leaders awake in different industries? Threat, like beauty it seems, is in the eye of the beholder. As somebody with security responsibility for the country's largest communications network, it's no surprise Telstra's Hancock views the sensor-based internet of things (IoT) as the internet of threats.

"IoT is growing at an astonishing velocity and creating a massive attack surface," he says. "It's moving at an incredible pace and the entire industry is now playing catch up to embed security."

For Queensland Health CISO, John Borchi, IoT is also a major focus. Understandably, he's most concerned about the security of medical equipment that keeps people alive. Managing this network of critical devices has become increasingly complicated in recent years as healthcare moves out of the highly controlled hospital environment. Some devices, like pacemakers, are implanted into people's bodies.

Attacks on the trust-based SWIFT network as a major concern in the banking industry. Institutions around the world use this network to transfer billions of dollars every day but hackers have successfully compromised it to steal large sums of money. The first reported attack of its kind netted more than $US81 million from the central bank of Bangladesh, according to a report in The New York Times.

Narelle Devine, CISO at the Department of Human Services (DHS), is responsible for sensitive data for critical Australian service delivery agencies including Centrelink, Medicare and Child Support. She predicts the worst is yet to come.

"Everything is moving so quickly but my biggest concern is that The Shadow Brokers are sitting on some clever stuff right now and just waiting to pull the trigger," she says. "Some of the global attacks we've seen recently were really unsophisticated. What's coming next?"

Our panel members say cybersecurity conversations with senior leadership usually fall into one of three buckets – staying out of the news, minimising costs and avoiding unnecessary project delays. It's difficult to say no to security budgets, because nobody wants to be the person who refused to sign investment off if something then goes wrong, but significant spending still attracts scrutiny.

Microsoft's Johnson says digital transformation has raised the cybersecurity stakes. Organisations want to make it easy for customers, employees and partners to access the right information when they need it but this presents challenges.

"If you're going to open your organisation up to new customers, new markets and anytime, anywhere access, you need to do it securely," she says. "That's part of the digital journey but it's a challenge because sensors were being added to everything before anybody considered security. You need to manage those devices and the data they generate effectively at the speed of business."

"If you're going to open your organisation up to new customers, new markets and anytime, anywhere access, you need to do it securely."

Ann Johnson
Vice President, Strategic, Enterprise & Cybersecurity, Microsoft

Chapter 1 – The threat landscape

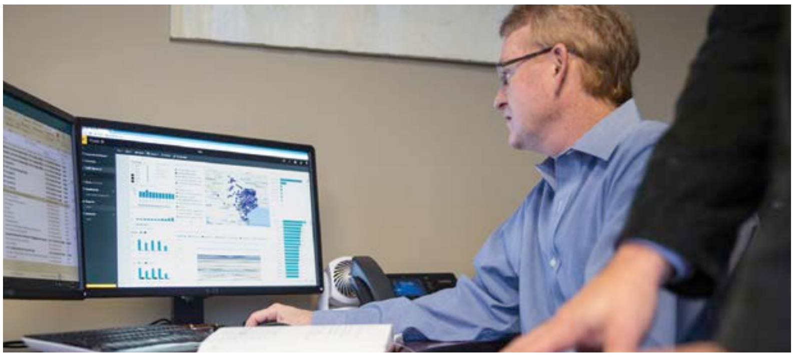
Who can you trust?

Even for the most security conscious organisations, supply chains are a potential weak link. It's very difficult to get third parties to meet your compliance standards and just about impossible to monitor what happens beyond your own networks. Hackers can get in at any point and head your way.

Certification is one way to build trust in the open and connected world of digital transformation. Are suppliers that connect to your cloud infrastructure STAR certified by the Cloud Security Alliance? Are they SOC 1, 2, or 3 compliant? These are simple proofs you can request to demonstrate that third-party organisations are taking your data security seriously.

Few organisations in Australia manage as much network complexity as Telstra. For example, it has 400,000 routers in operation from a range of different suppliers. Hancock says manufacturers can change 10,000 lines of configuration on each one so testing is incredibly complex. His team tests everything at the point when a device hits the network and then moves into continuous monitoring mode.

"We have a machine learning data analytics platform that processes 80 billion events a month for security alone," Hancock says. "It's pulling data from everywhere and telling us what we should prioritise. You have to look at everything that's available on your network. You need to know what's changed."



Borchi is concerned about supply chains, noting that health departments deal with thousands of suppliers that each bring their own risk. Sony, in one of the most high-profile data breaches of all time, was hacked through its credit card facilitator. In another major hack, retail giant Target had sensitive customer data exposed through a breach that got onto its network through air-conditioning sensors.

Microsoft takes a similarly cautious approach. It won't mandate any forced updates internally until they've been fully tested in a clean environment because the security team is concerned about introducing potential attacks.

"We have as much expertise as anybody with this because we have billions of Windows devices running globally," Johnson says. "We take those supply chain processes very seriously and we're pretty good at it because we have to be."

"IoT is growing at an astonishing velocity and creating a massive attack surface. It's moving at an incredible pace and the entire industry is now playing catch up to embed security."

Craig Hancock
CISO, Telstra

Chapter 2

When disaster strikes

Regulatory changes, both here in Australia and globally, will raise the profile of cybersecurity with board members and senior leadership teams. Yet many of these people are ill-informed or not engaged with the subject. You need to communicate risk and strategy in a way they understand. Cyber should also be part of your disaster recovery and business continuity planning. If disaster strikes, it's important to communicate quickly and clearly where possible to avoid reputational damage. You will be judged and remembered on how you respond.

Chapter 2 – When disaster strikes

Legislation and regulation

The Privacy Amendment (Notifiable Data Breaches) Act 2017, which amends the Privacy Act 1988, came into force on 22 February 2018. This has gained a lot of coverage in the Australian media. Yet Australian Information Security Association (AISA) Director, Helaine Leggat, says the amendment is 30 years too late.

In her opinion, the issue is not 'privacy' but the handling of personal information. When the Australian Privacy Act was passed 30 years ago, she says, even employee records were excluded from the protections afforded to other types of personal information.

Leggat points to Europe's General Data Protection Regulation (GDPR) as offering a higher level of protection, providing individual EU citizens with more control over their personal data. The European Commission has listed about a dozen countries that provide adequate protection. These include Argentina, Mexico, New Zealand, Switzerland and the United States but not Australia.

GDPR will apply to Australian organisations that have an establishment, offer goods and services or monitor the behaviour of individuals in the EU.

"Personal information is only one kind of information that the law affords protection, mandating that it be handled in a particular way, notably in relation to security," Leggat says. "Handling PI and complying with international privacy laws is a complex global issue."

Companies that do not meet the requirements could face reputational, business and legal sanctions as well as incurring hefty fines and facing class action lawsuits, so it's important to understand your obligations regardless of where your organisation is based.

"We need to find an equivalent for complying with Australian law but operating in an international environment. This is where international standards come into play," Leggat says.

The biggest GDPR concern for many Australian CISOs is the 72-hour breach notification rule because it's often difficult to assess what's happened during those first three days. Under Australian legislation, organisations must notify 'as soon as practicable' once aware there are reasonable grounds to believe there's been an eligible data breach.

Despite her support for GDPR, Leggat usually prefers to view privacy as risk-based rather than compliance-based. She says organisations should be allowed to self-regulate according to industry sector, services, risk appetite, budget and organisational maturity.

"Some people are looking for minimal compliance and I respect that," she says. "You need to build a solution designed for what you can realistically manage and then grow in maturity."

"We need to find an equivalent [to GDPR] for complying with Australian law but operating in an international environment. This is where international standards come into play."

Helaine Leggat
Director, Australian Information Security Association

Chapter 2 – When disaster strikes

Perception versus reality

Despite lots of commentary suggesting cybersecurity is now a board-level discussion, there are still plenty of Australian company directors who aren't adequately informed. This is why AISA has formed a strategic partnership with the Australian Institute of Company Directors. Almost half of those surveyed by law firm MinterEllison are only briefed on cybersecurity once a year, with 13 per cent admitting they never get an update.

"I've spoken to board members over the years who admit to switching off when cyber comes up because they don't understand the conversation," Borchi says. "Risks and strategies need to be explained in a meaningful way to prevent this from happening."

Whether or not they would be excited by the prospect of a cybersecurity briefing, it's clear many company directors also have inflated expectations of the security measures their organisations have put in place. While 59 per cent of board members believe their cybersecurity practices are very effective, according to Association of Corporate Counsel Australia research, only 18 per cent of IT security professionals would agree with this assessment.

Regulators take a dim view of failure and hand out heavy fines. The potential damage to corporate reputation is even more costly. British telco TalkTalk Group was hit with a record fine of £400,000 in 2016, according to a Financial Times report, for failing to adequately protect customer data following the theft of almost 157,000 records. In August 2017, it received another £100,000 fine after another 21,000 accounts were compromised.

When consumer credit rating company Equifax was hit by a data breach last year, it exposed the personal identifiable information of more than 145 million Americans. That's almost half the population and it quickly escalated into a situation CNN Money described as a public relations catastrophe.

Bloomberg reported that three Equifax executives sold shares worth $US1.8 million before the breach was disclosed, then a site set up for consumers to check if they'd been affected was criticised for forcing people to waive the right to join class action lawsuits. A bunch of lawsuits followed after that language was forcibly removed from the terms and conditions. Equifax CEO and Chairman, Richard Smith, stepped down in the eye of the storm as reported by The New York Times.

Closer to home, iTnews says 50,000 government and 40,000 private sector workers were caught up in one of Australia's largest ever data breaches. This hit the Australian Electoral Commission, the Department of Finance and the National Disability Insurance Agency as well as AGL, AMP and Rabobank. The Australian Cyber Security Centre first became aware of the breach in October 2017 although the government has described the data as historical.

"We have a machine learning data analytics platform that processes 80 billion events a month for security alone. It's pulling data from everywhere and telling us what we should prioritise."

Craig Hancock
CISO, Telstra

Chapter 2 – When disaster strikes

Perception versus reality

When there is an incident, our panel agreed it's important to get out in front of the problem from a communications perspective. This means responding quickly and clearly because social media will come down hard on smokescreens and unjustified claims. Herein lies a major problem because it can be difficult to provide factual information in the immediate aftermath of a cyberattack. This is because you probably won't have all the answers even if you do want to be transparent.

Despite the ever-growing list of costly, high-profile breaches, Johnson is surprised to find most Microsoft customers she talks to around the world still don't have a cyber-recovery plan. She's advocating very strongly for them to create a plan modelled on disaster recovery initiatives.

Glynn says cyber incidents should be viewed like any other business risk, noting that they can cause mayhem and should be managed accordingly. "Incident response needs to be part of disaster recovery and business continuity planning so that people can practise," he says. "You don't want to get this wrong in the heat of the moment."

Taking the pragmatic view that data breach is going to happen at some stage, Glynn says organisations will increasingly be judged on how they respond. This is why it's crucial to have an incident response program that covers how it will be communicated to staff, customers, partners, the media and other stakeholders.

"I've spoken to board members over the years who admit to switching off when cyber comes up because they don't understand the conversation. Risks and strategies need to be explained in a meaningful way to prevent this from happening."

John Borchi
CISO, Queensland Health

Chapter 3

People and partnerships

Finding enough trained people is a challenge for every cybersecurity team but, with a little creativity, there’s a world of transferrable skills to tap into. A background in accountancy builds great attention to detail, psychology develops understanding of human behaviour and military service teaches investigative skills. Taking a macro view, we all stand to benefit from building stronger links between the public and private sector. There’s also an opportunity for peer groups like telcos and utilities to share learnings and build greater industry resilience.

Chapter 3 – People and partnerships

Back to school

The cybersecurity industry struggles to hire people. In a global Intel Security survey that asked respondents whether there was a shortage of cybersecurity professionals in their country, Australia ranked second behind Mexico. As a nation, we need 500 more cyber graduates per year just to meet existing demand. And that demand is sure to grow. Given this background, how do you attract and retain the right talent?

The Department of Human Services found its hiring plans were shaped partly by a market reality – there simply weren't enough trained security experts in Canberra to meet its requirements. Yet the team has more than tripled in size during the past year.

"We knew it was going to be impossible to find enough skilled people, so we made a conscious decision to hire straight from school and train them internally," Devine says. "We've supplemented this strategy by hiring some more experienced people who are contracted to split time evenly between doing their job and mentoring three juniors.

"It will probably be two years before we know if this strategy is going to work. We know people will leave because these roles are in high demand but we did the maths and we'll be ahead if we can keep one in three of those going through training."

Hancock says Telstra hires about 50 university and TAFE graduates every year. Many of these new hires end up working in its security team. Yet although it has the luxury of a large cyber team and significant budgets, he says problems are often caused by the broader technology team.

"We need to embed security skills into the network teams so that they build security in rather than waiting for us to run tests and fix problems," he says. "There are rooms full of books about how to stop SQL injections but you have to get people to read them.

"We now have security professionals embedded in our development teams. It's not perfect but it's a better approach. Ideally you've got to educate the whole company but that's really hard."

DHS has also started to rotate security professionals through development teams to reduce the likelihood that security flaws are missed when designing new applications.

At Queensland Health, there's been a deliberate shift in the types of people being hired for cybersecurity roles. Where the industry tradition has been to hire somebody with a technology background, this department has also been thinking outside of the box in terms of hiring cyber talent.

"Our cybersecurity training, communications and awareness program is run by business and marketing graduates. You want people who communicate well and can present the information clearly," Borchi says. "There's no way to get people straight off the street with the right mix of attitude and background but I'm leaning more towards business than technology people."

Borchi says people who don't come from a technology background often dismiss cybersecurity, thinking they can't explain it if they don't understand it. He tells them that they're exactly what he needs: "If they have the communication skills, we need them to understand cyber so they can explain it to others."

AISA plays an important role in improving industry education around cybersecurity and cyberlaw in partnership with state and federal government as well as schools, TAFEs and universities. It's represented on the advisory board of Box Hill Institute and contributes to the development of course content.

Chapter 3 – People and partnerships

Strength through diversity

Microsoft runs a military transition program in the US that includes a 12-week cybersecurity boot camp. Johnson says these people already have investigative skills so it's a natural transition to teach them cyber forensics. Locally, DHS has implemented a similar program, which is no surprise given that Devine is a former Australian Navy Commander with 20 years' military experience.

"Some of our best hires have been people coming out of the Australian Defence Force," she says. "These people are strategic thinkers, they have built-in loyalty and they bring a host of other skills that are hard to measure in aptitude tests. They've already been through a lot of that to get into Defence in the first place."

The DHS cybersecurity team also includes an eclectic mix of psychologists, lawyers and politics graduates. When she was putting together a team to improve awareness and education, Devine turned to somebody with a major in communications, not cyber.

"That's working really well. Even the branding of the security operations centre has grown exponentially because we have somebody who can tell the story properly," she says. "Sure you need some people to do the technical stuff but there has to be that blend. I'd say we have a fairly even split between technical and non-technical people."

AISA has 3,000 individual members. Leggat says a lack of agreed terminology, and the understanding of security capabilities on either side of the recruitment process, is a widespread problem. How can jobseekers and employers align their understanding of the requirements when there are no formally recognised criteria?

"The matchmaking part of the hiring process is often missing," she says. "We're working to help solve this problem."

Given the squeeze on talent, both in terms of capacity and capability, what role will managed service providers and other outsourcers play in closing the cybersecurity skills gap? For most attendees, the risk associated with putting security in the hands of a third-party outweighs the benefits.

elevenM's Glynn says outsourcing makes a lot more sense for small and medium-sized businesses (SMBs). "If I was talking to a start-up or an SMB that didn't have decades of in-house security experience, I would be pushing them towards the cloud," he says. "Generally, the control in that environment is more than adequate and much better than these organisations could achieve by trying to do it themselves."

DHS outsources some cyber work but Devine wants to keep it in-house wherever possible. She says this is an important part of building culture within the security operations centre.

"Some of our best hires have been people coming out of the Australian Defence Force. These people are strategic thinkers, they have built-in loyalty and they bring a host of other skills that are hard to measure in aptitude tests."

Narelle Devine
CISO, Department of Human Services

Chapter 3 – People and partnerships

Partners in crime prevention

The heads of information security within Australia's largest companies and government departments are very well connected. Devine says she talks to other prominent CISOs every day, challenging the common perception that they don't share information with each other.

While it's reassuring to know some of these security experts have each other on speed dial, our panel says there's much room for improvement in how government and business works together to improve cybersecurity. A new opportunity for greater collaboration will present midway through 2018 when the Australian Cyber Security Centre moves to a new purpose-built facility. This will have different levels of classification that make it more accessible to industry.

While the cybersecurity strategies of Australian state and federal governments call for partnerships with the private sector and academia, Leggat says information sharing is fraught with risk. This is because the relevant legislation is often surveillance focused, falling under national intelligence and law enforcement.

"Access alone may be criminal, sharing protected information carries higher risk," she says. "On the academic side, Australia is bound by international agreements and restrictions on dual-use technologies. Sharing some information comes with a jail term."

When it comes to intelligence sharing organisations, Johnson says the Financial Services – Information Sharing and Analysis Centre (FS-ISAC) is the best in the world. She sees opportunities for other industries to follow suit. In the telco industry, for example, it would be incredibly powerful if Telstra shared information with the likes of AT&T, BT, Comcast and Verizon to create global threat visibility.

> "Security is a team sport and everybody needs to be part of the solution. They should participate in their own rescue and security should be a celebrated part of organisational culture."

Ann Johnson
Vice President, Strategic, Enterprise & Cybersecurity, Microsoft

Final thoughts

Cybersecurity can no longer be treated as an afterthought. Effective protection strategies combine technical expertise with broad organisational management and security teams need to be part of the first conversation. For their part, those teams can't afford to be seen as a potential roadblock – they need to work closely with application development to help achieve goals securely without unnecessary disruption.

Projects will continue to fail because of security breaches within organisations that don't make these changes. "At its best, security is a team sport, and everybody needs to be part of the solution," Johnson says. "They should participate in their own rescue and security should be a celebrated part of organisational culture."

Security teams must continue to build systems for all users and promote a culture of continuous education. When it comes to cybersecurity, we must never stop learning.

Contributors

John Borchi CISO, Queensland Health
Narelle Devine CISO, Department of Human Services
Steve Glynn Principal, elevenM Consulting
Craig Hancock CISO, Telstra
Ann Johnson Vice President, Strategic, Enterprise and Cybersecurity, Microsoft
Helaine Leggat Director, Australian Information Security Association