Click, breach, repeat

How people, culture, and leadership will shape the future of the cyber risk landscape in Australia and New Zealand

QBE

Foreword

Cyber was once seen as an emerging risk, a future concern for technical teams. But that future has arrived. Today, cyber risk is a shared challenge that extends to all areas of an organisation and every person with an internet connection.

It doesn't respect borders, and its impacts are often difficult to contain. As a result, cyber insurance has fast become a core consideration for organisations seeking to manage their risks, alongside more traditional lines of coverage. While the term "cyber risk" evokes images of hackers breaching firewalls or sophisticated malware infiltrating networks, the reality is more confronting. The single biggest factor in whether an organisation is breached, and how badly, is the behaviour of its own people.

In 2024, Australia recorded more than 87,000 cybercrime reports, equivalent to one every six minutes,[1] with phishing and ransomware dominating. Internationally, there was a 58% increase in attempts by threat actors to steal information.[2]

This research report - which features polling of over 1,700 Australians and New Zealanders - reveals key insights into consumer and employee attitudes and behaviours toward cyber awareness, and explores differences across countries, generations, and organisation sizes. It also makes clear through commentary from QBE's local and global cyber experts that attackers are watching, learning from our mistakes, and exploiting them faster than many organisations can respond.

The research tells us that younger workers represent both the biggest vulnerability and the greatest untapped opportunity when it comes to cyber resilience. Having grown up in the digital era, they're more likely than older generations to take shortcuts with basic security – delaying updates, reusing passwords, or clicking on phishing links. Organisations that invest in making security simple, engaging, and built into everyday workflows will not only reduce risk but also strengthen trust among their most demanding and digitally native employees.

At the organisational level, employees at larger organisations are less likely to make obvious missteps like phishing clicks, but show greater resistance to tools such as multi-factor authentication, especially compared with smaller businesses. These behavioural gaps create easy entry points for attackers, who increasingly rely on exploiting human error rather than sophisticated technical methods.

What happens after an incident is just as important as prevention. Older generations place the highest value on transparency and prevention over speed, while younger generations demand faster recovery. Trust, however, remains fragile. Even when customers continue doing business with a breached organisation, the financial, legal, and reputational fallout can be severe and long-lasting.

Our research makes one thing clear: human behaviour is now the critical battleground in cyber defence. Culture, processes, and leadership will shape whether Australian and New Zealand organisations can turn their people from their greatest vulnerability into their strongest line of defence, not just now, but in the decades ahead.

Serene Davis

Global Head of Cyber
QBE Insurance

Every click, ignored update, or unreported phishing attempt can form part of a chain of events that exposes a business to increased cyber risks.

1. Australian Government. Australian Signals Directorate. Annual Cyber Threat Report 2023-2024. Accessed on 18 August 2025.
2. Check Point. 2025 Cyber Security Report. Accessed on 18 August 2025.

Methodology

The survey data used in this report has been conducted using an online survey administered by Pure Profile. All figures, unless otherwise stated, are from Pure Profile. The total sample size was 1,764 adult Australian and New Zealanders. Fieldwork was undertaken in July 2025.

Disclaimer

Cyber risk is a human story[3]

41%

delay software updates

32%

believe multi-factor authentication is a hassle

86%

of employees confident in recognising cyber threats

61%

reuse

P@22words

241

days[5]

is the global average breach lifecycle (the mean time to identify and contain a breach)

36%

of workers believe their organisation is likely to be targeted by a cyber-attack over the next 12 months.

The top three industries being, Energy and Utilities, Government/ Public Sector and IT. In reality, healthcare sector breaches remain the costliest, averaging $7.42 million (USD). Breaches across this sector take the longest to identify and contain at 279 days.[4]

3. All data, unless otherwise specified, sourced from Pure Profile survey. See Methodology for more. 4. IBM. 2025 Cost of a Data Breach Report Accessed on 18 August 2025. 5. IBM. 2025 Cost of a Data Breach Report. Accessed on 18 August 2025.

Human behaviour in cyber risk

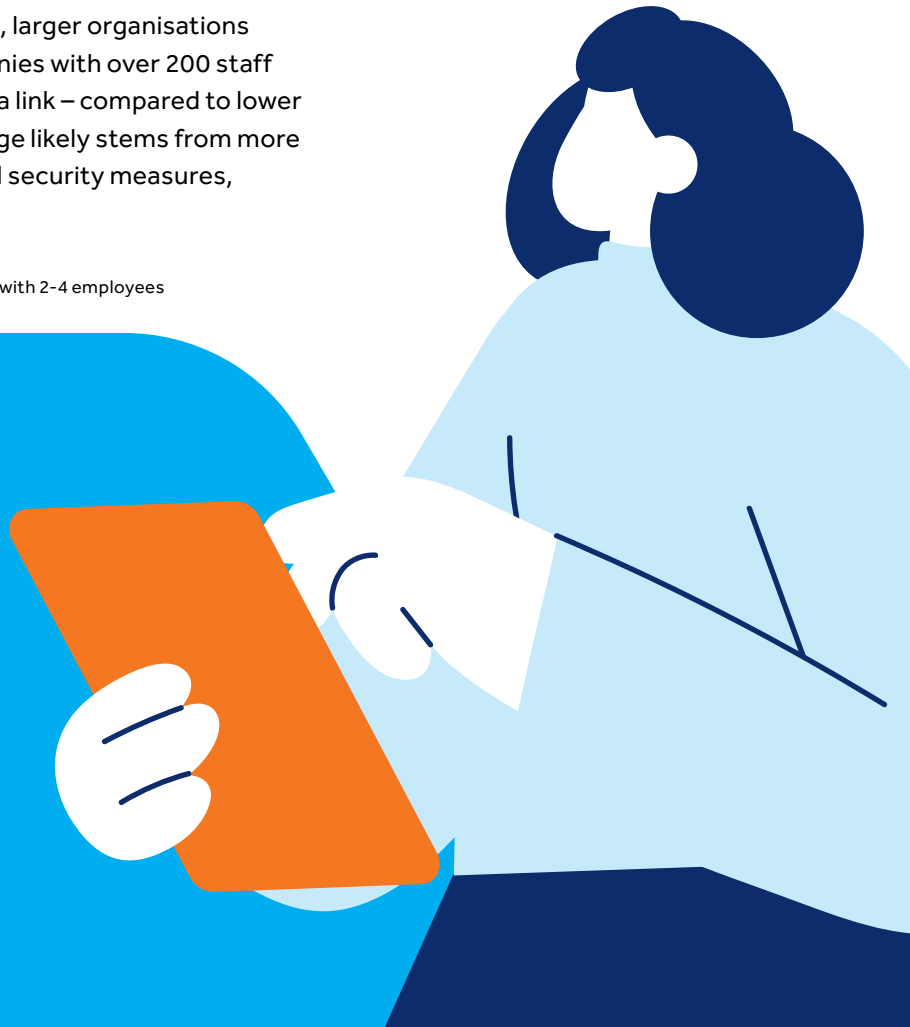
For years, cybersecurity conversations have been centred on technology: firewalls, encryption, and tools designed to prevent and block potential attacks.

Yet QBE research shows that in many breaches, the decisive factor isn't the sophistication of the attacker's tools and methods, it's the behaviour and actions of the people inside the organisation.

The data is stark. More than one in three workers (35%) admit to clicking a phishing link at some point in their career, which is a key entry point for attackers.

When comparing results by organisation size, larger organisations fare better, with 65% of employees in companies with over 200 staff reporting that they've never clicked on such a link – compared to lower figures for micro-SMEs[6] (51%). This advantage likely stems from more formalised training programs and automated security measures, but it's no guarantee of safety.

6. For the purposes of this report. Micro-SME's are businesses with 2-4 employees



"The most sophisticated threat actors still rely on something simple: human error. They don't need to invent new exploits when the basics work."

Ben Richardson
Cyber Product Lead, QBE Australia

Generational differences are even more telling. Gen Z and Millennials are more likely to juggle multiple devices (phones, tablets, laptops, gaming consoles), and have a larger online surface area. This constant connectivity makes them less tolerant of friction in their workflows, which can lead to riskier digital behaviours. They are also significantly more likely to delay critical updates (46% versus 33% for Baby Boomers), reuse passwords across work and personal accounts, and fall for phishing attempts, as they seek workarounds that can compromise security.

These patterns create low-cost, low-effort opportunities for attackers, who increasingly prioritise human error over technical exploits. Once inside, attackers can escalate privileges, move laterally, and extract data with minimal resistance. At the same time, as Baby Boomers approach retirement age, organisations will need to rethink the digital backbone of their workplaces and customer interactions to effectively manage cyber risk – considering not just infrastructure, but also network security and a culture that supports how different generations interact with the online world.

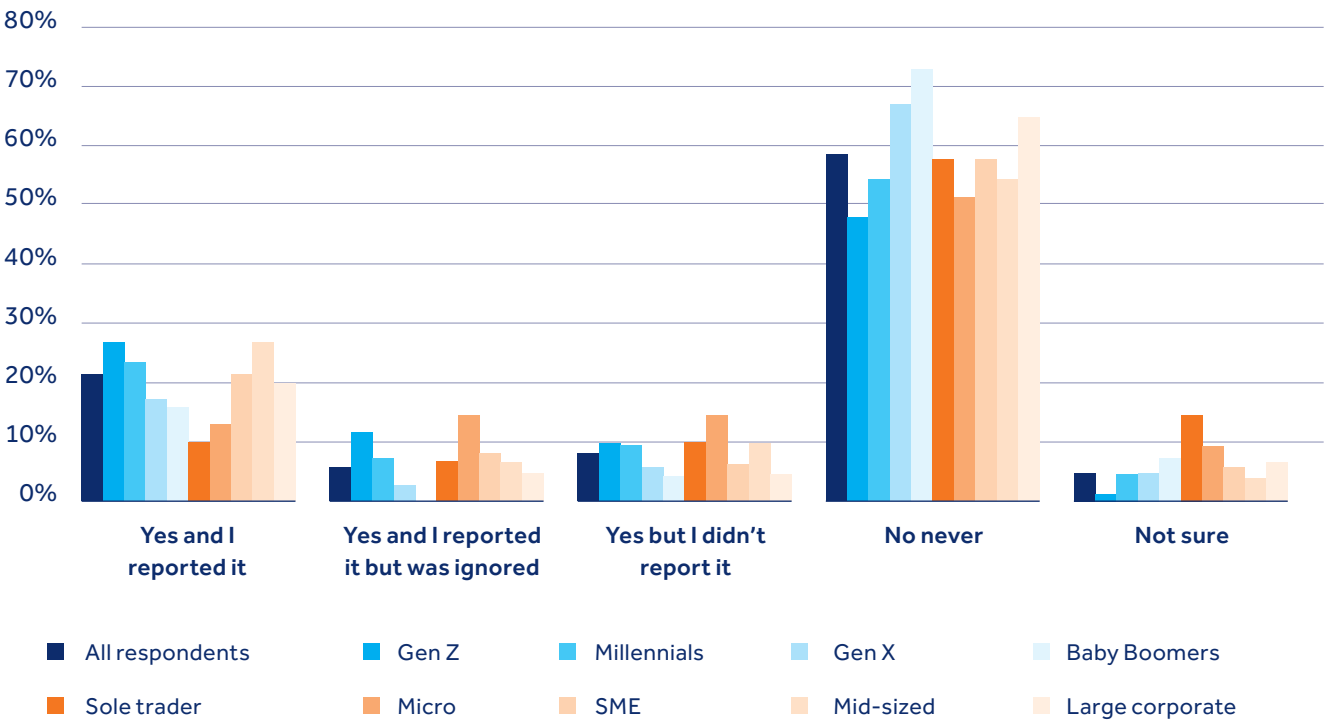
The survey data also reveals a striking blind spot. When asked *"Have you ever clicked a suspicious link or made a cyber mistake at work?"*, almost 60% of employees declared *"No, never."* However, due to the sheer volume of cybercrime incidents, we know many mistakes go unnoticed, with attackers often delaying actions including selling stolen data to other groups who exploit it months later.

This is reinforced by the fact that 86% of workers said they were confident in spotting cyber threats. Confidence can be valuable, but overconfidence creates risk. It only takes one misstep to compromise an organisation, and attackers know it.

For businesses, this highlights a simple truth — training alone won't close the gap. Security must be designed with the assumption that errors will occur, and be backed by strong access and segregation controls (enforced multi-factor authentication), the consistent deployment of minimum baseline configurations (including anti-malware controls and patching policies in place), with clear escalation pathways and business continuity planning.

Key survey insight

Have you ever clicked on a suspicious link or made a cyber mistake at work?



"Human error is the number one factor in most cyber incidents, often starting with social engineering. With AI-driven deepfakes and more sophisticated phishing campaigns, attackers are better than ever at manipulating people. That's why we underwrite not just to technical controls like multi-factor authentication, but also to training and awareness, because people remain the first barrier."

Desiree Spain

Global Head of Cyber Underwriting Management, QBE

Cracks in the culture

Cyber incidents rarely begin with the first line of malicious code. More often, they stem from cracks in the organisation's culture, governance or leadership.

Weak oversight, unclear accountability, and a reluctance to confront uncomfortable truths often create the conditions that make a cyber breach inevitable.

QBE's research reveals a gap between how employees view cyber responsibility and how organisations actually manage it. When asked who they would blame if a breach occurred, 31% of workers pointed to their IT department, far outpacing executives (13%), third-party providers (5%) and even hackers or cyber criminals (26%).

This disconnect matters. In an effective cybersecurity culture, responsibility is shared and understood across the organisation, from the front desk to the boardroom. But in too many businesses, cyber remains siloed as "an IT problem", leaving executives unprepared to lead during a crisis and employees unsure where they stand.

"If your leadership team isn't asking the right questions about cyber, the business is already vulnerable."

Serene Davis
Global Head of Cyber, QBE

Psychological safety plays a critical role here, as cybercriminals often use confusion, greed and fear as levers to trick a person into providing access or data. Impacted employees are often less likely to report a suspicious email link they've clicked or a misconfiguration they've noticed. In QBE's research, 35% of workers admitted to clicking on a phishing link. Of those, some reported it immediately, others hesitated, and 8% didn't report it at all. That's not just a security lapse, it's a cultural failure. In an environment where mistakes are punished rather than addressed constructively, threats can remain hidden until they've escalated beyond control.

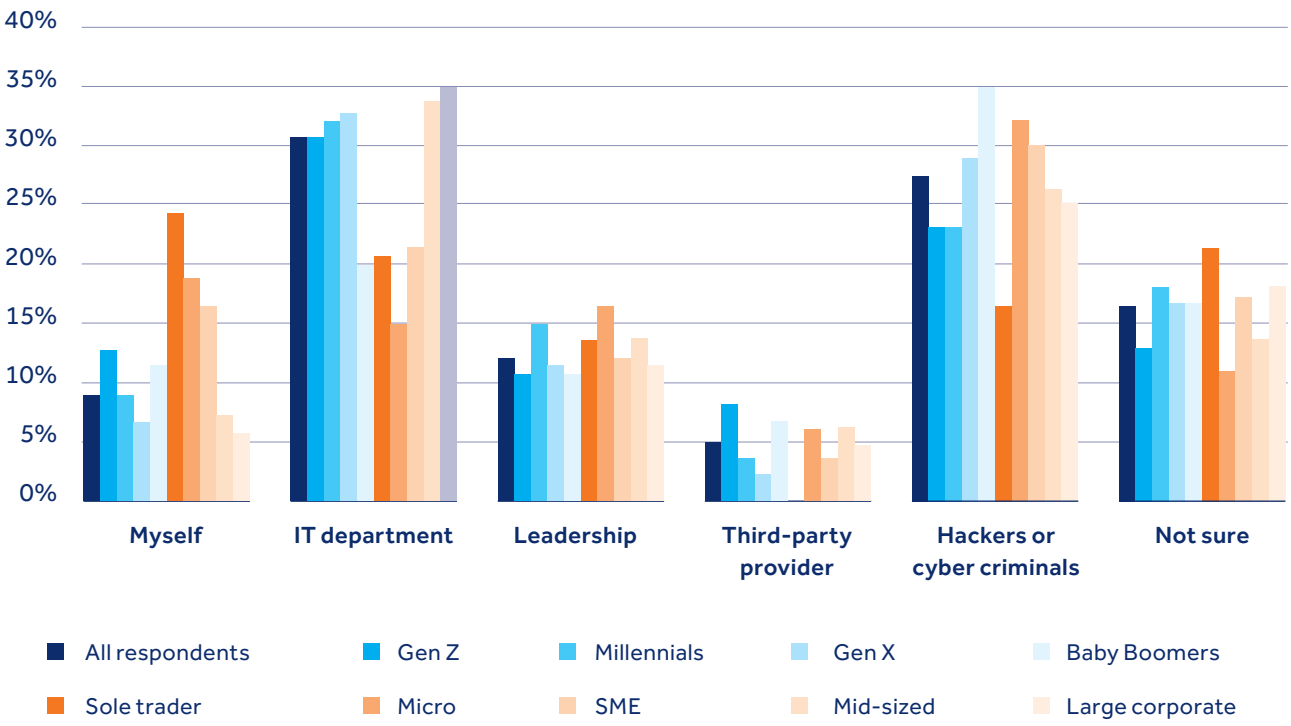
Industry, size, and structure all shape an organisation's cultural readiness for cybersecurity. Larger organisations often have clearer processes and better phishing avoidance rates, but also face more resistance to protective measures, with 35% of employees (in organisations of more than 200 employees) finding multi-factor authentication a hassle, compared to 21% for micro-SMEs. Their large complex structures can also slow down response times, despite having more formal governance in place.

In contrast, SMEs may benefit from flatter hierarchies that enable faster escalation, but they can often lack comprehensive training and defined frameworks to prevent errors. Additionally, SMEs tend to rely more heavily on outsourced technology providers, which can limit their ability to act swiftly and decisively in a crisis. Across both large organisations and SMEs, broader lateral access with less segregation of duties increases risk exposure, especially when staff hold wide-ranging authorities without clear constraints or established protocols.

Culture and leadership ultimately determine whether an organisation responds to cyber threats reactively or proactively. Leaders set the tone as to whether cybersecurity is an afterthought or a standing agenda item at every executive meeting. Governance frameworks only work if they are understood, implemented, and enforced at every level.

Key survey insight

If your organisation suffered a cyber breach, who would you assume is responsible?



"A ransomware attack isn't just a cyber incident, it is often a full-scale business crisis. Importantly, it's not an IT issue, it's an executive responsibility."

Dominic Keller

Global Head of Cyber Services, QBE

Inside the breach response room

It starts with a ping

A junior analyst notices an unfamiliar login at **2:13 am**, on a Sunday. The IP traces back to Eastern Europe. At first glance, it could be a false alarm, another one of the hundreds they see daily. But then another alert hits. And another.

By **2:18 am**, the threat is confirmed, and the breach response team begins to assemble. The first hour is the "golden hour" of a cyber response, a tightrope walk between moving fast enough to contain damage and slow enough to avoid catastrophic missteps. Decisions made here can cost millions, save millions, or, in the worst cases, decide whether the business survives.

"Cyberattacks happen at the most inconvenient times, weekends, nights, holidays, basically when the A-team is off duty."

Dominic Keller

Global Head of Cyber Services, QBE

Hour 1

Detection and escalation

The “golden hour” is when malicious activity is essentially confirmed. The breach commander, often a senior security leader, alerts the executive sponsor, usually the CIO or CISO. Legal counsel is engaged to begin assessing the individual, contractual, and regulatory notice obligations.

In these early moments, people instinctively rely on familiar communication channels - email, messaging apps, internal systems - without realising those very tools may already be compromised. The moment it dawns on the room that their usual ways of coordinating can’t be trusted is often tense and disorienting. New, secure lines of communication must be established, adding pressure to an already high-stakes situation.

Hour 2–6

Containment and control

IT scrambles to isolate affected systems. Forensic investigators begin tracing the intrusion path. In the background, discussions take place of whether to take critical systems offline, a decision that will stop the attackers, but can also impair or cease revenue generating operations. Media statements are written, and HR assesses employee impacts.

This is where unprepared leadership can buckle. Without prior rehearsals, every decision becomes a debate. In a prepared organisation, this phase focuses on action and accountability: systems are segmented, backups are validated, and communication protocols activate automatically. In an unprepared one, containment can drag on for days while attackers stay a step ahead.

Day 1–3

Communication and fallout

This is where the breach reaches the public domain and customers want to know if their data has been stolen, and industry regulators might request detailed incident timelines. Inconsistent messaging or delayed disclosure can inflict more damage than the breach itself. Therefore, measures adopted ahead of time can minimise the uncertainty around the safety of customer data.

At the same time, ransom negotiations may be underway behind closed doors. In 2024, the average ransom payment hit $2.73 million (USD), though a growing number of organisations are refusing to pay.[7] But ransoms can complicate the crisis, opening a new layer of risk, triggering complex compliance and sanctions obligations. In jurisdictions like Australia, new laws now require mandatory notification of ransom payments, increasing regulatory scrutiny at the worst possible moment.

7. IBM. 13% Of Organizations Reported Breaches Of AI Models Or Applications, 97% Of Which Reported Lacking Proper AI Access Controls. Accessed on 18 August 2025.

Week 1 and beyond

Recovery and reflection

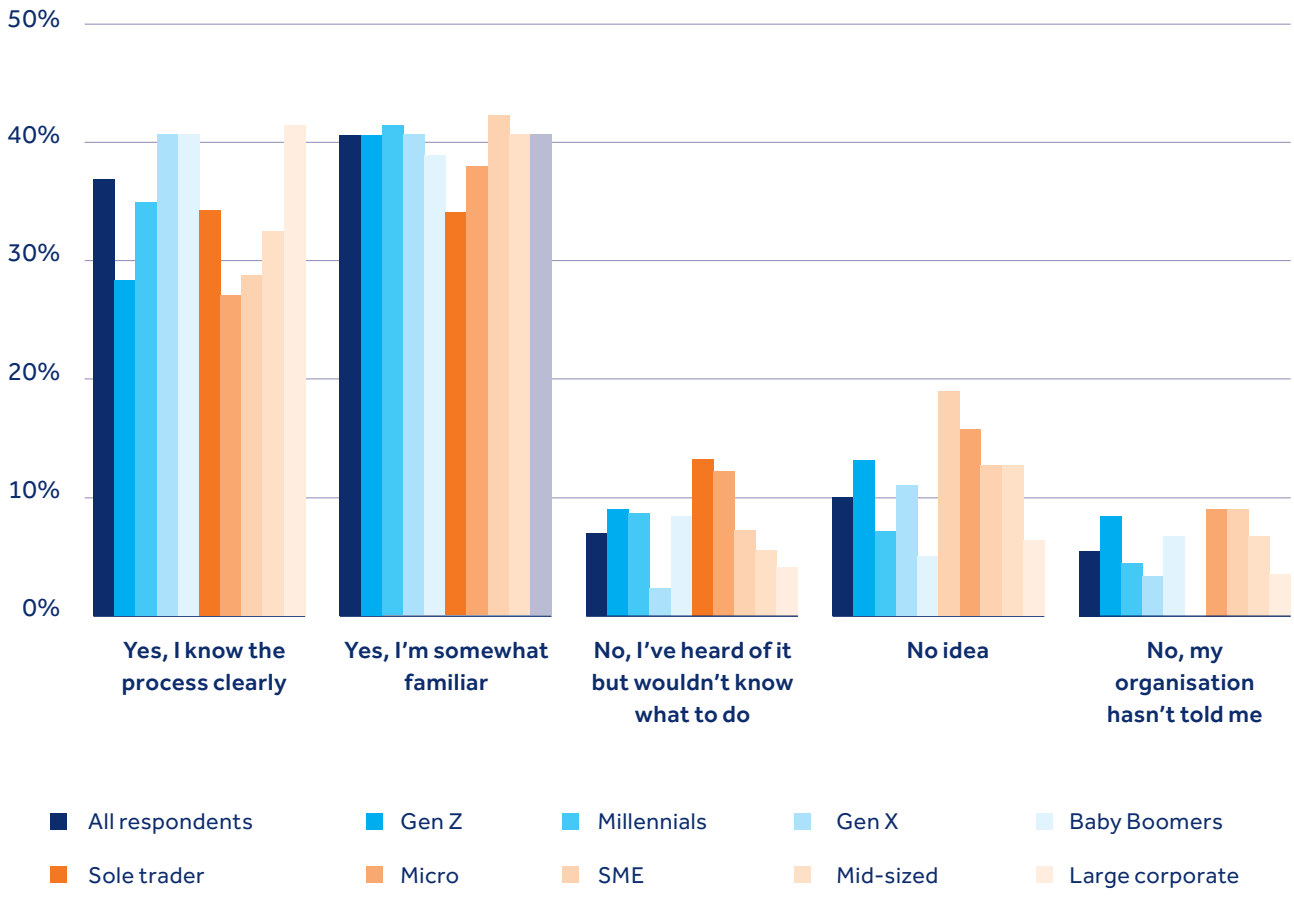
Whether the ransom was paid or not, this is where systems come back online, and post-incident reviews are conducted that may reveal missed warnings, outdated playbooks, or critical dependencies on third-party vendors. Recovery can stretch over several months. This timeline is influenced by many factors, including the type of incident, its impact on operations, and critically, the organisation's level of preparedness.

Our research shows that in many Australian and New Zealand organisations, cultural and structural gaps during this phase can magnify the long-term impacts. Gen Z and Millennials, are generally more forgiving of human error. While Baby Boomers are more prevention-focused, and will judge the response based on whether it prevents future incidents. Larger organisations typically manage containment better due to established protocols and resources. However, SMEs often communicate faster, which can help preserve trust, even when technical recovery takes longer.

Cyber incidents present opportunities for theories to confront reality. They are how leadership proves, or disproves, its readiness. One truth will become painfully clear: in cybersecurity, the moment of attack is not the time to figure out who's in charge.

Key survey insight

Would you know what to do, or who to contact, if you spotted a cyber threat or breach in your workplace?



13%

of Gen Z who have witnessed a cyber incident at work feel that the incident was handled poorly compared to **Boomers (0%)**, **Millennials (8%)** and **Gen X (4%)**

Rebuilding trust after a breach

When a cyber incident occurs, customers, regulators, and the public want to know two things: What happened? And what's being done about it? Reputation is as critical to resilience as technology, and how leaders communicate and demonstrate accountability can determine whether trust is restored or permanently eroded.

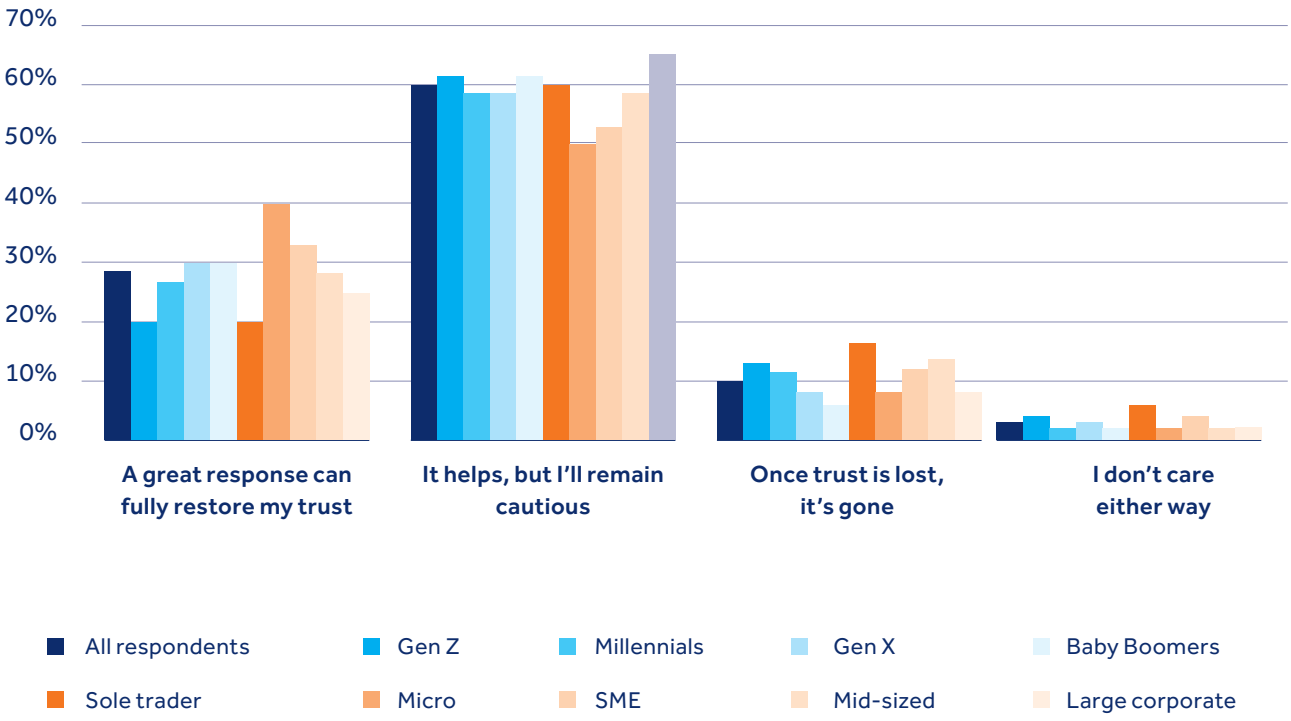
Our research makes clear that transparency has become the defining factor. 34% of Australians and New Zealanders say that openness is the single most important factor following a breach. This is followed closely by the expectation that the organisation takes steps to prevent recurrences (31%). By contrast, only 11% view speed of recovery as a priority. Generational differences are evident with younger cohorts such as Gen Z and Millennials placing more value on rapid recovery, while Baby Boomers and Gen X focus more on long-term prevention and assurance. Regional differences are equally important. Australians are more likely than New Zealanders to demand compensation (17% vs 13%) suggesting that while technical recovery is critical, communication and customer engagement strategies must be tailored to the market and demographic groups.

The willingness of consumers to forgive is also conditional. 40% of Australians say they would give a breached company another chance, compared with 47% in New Zealand. Baby Boomers are the most forgiving (50%), while Gen Z (37%) and Millennials (39%) are less inclined to offer a second chance. This reflects generational expectations where younger consumers raised in a digital-first environment, see cyber resilience as a baseline obligation rather than an added safeguard.

Cyber trust is both vital and fragile. Organisations that communicate transparently, take accountability, and demonstrate meaningful change are best placed to preserve customer confidence and protect brand equity. In today's environment, reputation is not restored through speed of recovery alone, it is earned through openness, leadership, and a demonstrable commitment to doing better.

Key survey insight

To what extent does the quality of a company's response to a cyber breach influence your trust?



Only 11%

of cyber-impacted customers say they would never trust a breached business again, but a poor response could cause further reputational damage and drive away return customers.

The importance of cyber insurance

Cyber resilience requires more than technical defences and incident response teams. It demands a holistic approach that connects risk management, governance, employee behaviour, and financial protection.

Today, customers expect nothing less, with eight out of ten people wanting the organisations they deal with to have cyber insurance in place. That expectation makes cyber coverage not just a safety net, but a marker of trust and credibility in the market. QBE's role is to not only support organisations with coverage when an incident occurs, but to also better prepare them to withstand and recover from the growing scale of cyber threats.

Preparedness and protection

Insurance is only one part of the solution. While financial cover is critical, it often doesn't fully account for the real impact, especially the cashflow strain from business interruption, or the significant costs of legal counsel, IT forensics, and remediation.

The most resilient organisations are those that invest in prevention and preparation well before an incident occurs. That's why QBE provides value-added services alongside our cyber insurance, including threat intelligence briefings, access to specialist response teams, policy and governance templates, and executive-level tabletop exercises.

As Mr Keller notes, "Executives who haven't sat through a cyber breach simulation are often shocked by how many critical business decisions are required in a pressured situation. These exercises expose the chaos that follows a breach, surfacing gaps in planning and revealing the cultural cracks and coordination failures that only become visible under pressure."

Global insights, local expertise

As a global insurer, QBE combines international threat intelligence with a deep understanding of the local regulatory and risk landscapes, ensuring guidance that is both globally informed and locally relevant. Whether helping Australian organisations meet increasingly stringent reporting obligations or supporting New Zealand businesses to understand evolving threat trends, our approach is consistent and expert-led.

As Ms Spain explains, "QBE's strength is its global reach and consistency. We see cyber claims and threat trends across every market, and that intelligence translates directly into the guidance and coverage we provide in Australia and New Zealand. Customers know they're getting the same comprehensive product as clients in the US or Europe, backed by a global insurer with the expertise and capital to pay claims."

Support for industries and organisations of all sizes

Our research shows that large organisations and small-to-medium enterprises face significant yet unique challenges. Larger companies often benefit from stronger phishing avoidance and more established IT infrastructure, yet they encounter greater resistance to measures like multi-factor authentication. Smaller businesses may be more agile but may lack the resources to invest in specialist cyber expertise.

QBE's approach is designed to support both ends of this spectrum, tailoring solutions to organisational size, sector, and maturity. As Mr Richardson notes, "Cyber risk doesn't discriminate by size. Our role is to scale support so every organisation can access the same expertise, services, and resilience planning."

Building long-term resilience

Ultimately, cyber insurance must be more than a financial backstop. QBE's goal is to embed cyber resilience into the fabric of an organisation, reducing the likelihood of incidents, limiting their impact, and protecting customer trust when an incident occurs.

In today's environment, where attackers exploit human error as readily as technical weaknesses, resilience requires a partnership between organisations, their people, and the specialists who support them. According to Ms Davis, "Resilience is a cultural shift, it goes beyond incident response plans to embedding cyber awareness across HR, finance, communications and leadership, so every part of the business knows its role in a crisis. QBE helps organisations rehearse these scenarios so they can knock down silos and build confidence that spans the entire enterprise."

QBE's cyber insurance solutions are built to deliver that partnership, ensuring businesses can withstand today's threats, while also adapting to tomorrow's.

QBE's local and global cyber team

This report was developed with insights from QBE's cyber experts across Australia, New Zealand and globally.

Their combined expertise in underwriting, threat intelligence and cyber services helped shape the findings and recommendations. Our teams work closely with broker partners and customers to strengthen cyber resilience. To learn more about how QBE's Cyber Insurance solutions can work for you or your customers, visit our website: **qbe.com/cyber**

Local contacts:

Ben Richardson
Cyber Product Lead, Australia
ben.richardson@qbe.com

Miro Dordevich
Cyber Product Lead, New Zealand
miro.dordevich@qbe.com

Our global cyber contributors to this report include:

Serene Davis
Global Head of Cyber

Dominic Keller
Global Head of Cyber Services

Desiree Spain
Global Head of Cyber Underwriting Management

Claire Kidwell-Smith
Global Head of Cyber Operations

Devon DeFreitas
Lead Global Client Solutions, Cyber Services

Jack Tolliday
Senior Lead - Cyber Services and Threat Intelligence