McGrathNicol

Ransomware: A Cost of Doing Business?

Australian businesses are still overwhelmingly paying cyber ransoms, and paying them quickly.

2023 Survey — In Partnership with YouGov Australia

Contents

Summary of 2023 findings

For the third year, McGrathNicol Advisory has created an authoritative barometer of the ransomware threat in Australia. Partnering with YouGov to survey over 500 Australian business owners, partners, directors and C-Suite leaders of businesses with more than 50 employees, this year's findings reveal that business leaders are still overwhelmingly paying ransoms, and paying them quickly.

73%
of surveyed businesses that suffered a cyber attack in the past five years paid a ransom

42%
fell victim to a single attack, 14% were targeted repeatedly

75%
paid the ransom within 48 hours

66%
negotiated prior to making a ransom payment

$1.03m vs **$1.32m**
estimated average cyber ransom that was paid
average ransom business leaders would willingly pay

60%
of business leaders say it should be mandatory to report ransomware attacks to the authorities
↓ from 70% in 2022

83%
say their view of a company would be negatively affected upon learning of a ransom payment
↓ from 91% in 2022, from 90% in 2021

88%
of business leaders believe their organisation is "prepared" for a ransomware attack
↑ from 78% in 2022

61%
of businesses have an incident response plan in place
↓ from 65% in 2022

30%
of all ransomware attacks used email phishing as the mode of entry

Australian businesses paying at all costs

73 percent of Australian businesses surveyed have suffered a cyber attack in the past five years and paid a ransom.

Following reports in 2021 and 2022, McGrathNicol Advisory continues to map the ransomware threat in Australia to better understand the attitudes and actions of businesses towards this pervasive cyber threat. Partnering with YouGov to survey over 500 Australian business owners, partners, directors and C-Suite leaders of businesses with 50+ employees, this year's findings reveal that executives are still paying ransoms at a high rate, with softening attitudes towards payments reporting.

Ransomware remains a significant threat to businesses.

The research shows that 56 percent of Australian businesses have suffered a ransomware attack in the past five years: 42 percent of medium and large businesses have fallen victim to a single attack, while 14 percent have been targeted repeatedly. The five-year ransomware average is down from a high of 69 percent in 2022, but remains well above the 31 percent recorded in 2021 when McGrathNicol started tracking these results. This suggests that while cyber criminals hit a ransomware peak last year, the threat remains as many groups have shifted to other forms of cyber extortion.

Businesses are choosing to pay ransoms at an alarmingly high rate.

Of those that did suffer an attack, close to three quarters (73 percent) chose to pay the ransom demand. This is incrementally down from a high of 79 percent in 2022 and 83 percent in 2021, but not enough to suggest that government pressure and regulatory scrutiny are having a significant impact on executives' decision to pay.

Businesses are also paying quickly.

Pointing to the speed at which these decisions are being made, 75 percent of Australian business leaders reported paying a ransom demand in less than 48 hours, and almost two in five (37 percent) reported making the payment within 24 hours. This is consistent with previous years, with 78 percent of companies surveyed in 2022 reporting that they paid within 48 hours, and 74 percent reporting the same in 2021. The figures show that many executives see a ransom payment as the lesser of two evils or simply 'a cost of doing business'.

"Businesses are still overwhelmingly paying ransoms, and paying them quickly, to avoid negative backlash from customers, partners and stakeholders. It's now being factored in as a cost of doing business."

"Executives are also becoming empathetic and less hard-nosed about reporting these attacks to authorities. But without greater collaboration and knowledge-sharing, our ability to prevent ransomware attacks is undermined."

Darren Hopkins
Partner, McGrathNicol Advisory

Negotiation is on the table

The average cyber ransom paid in 2023 was $1.03 million.

This figure reflects a three-year trend and is on par with $1.01 million in 2022 and $1.07 million in 2021. However, there is a significant discrepancy between how much businesses are paying and how much they would be *willing* to pay - $1.32 million. Despite government advice to the contrary, 70 percent of surveyed businesses (including those businesses yet to suffer an attack) say they would be willing to pay a ransom when faced with the high-pressure decision.

Further, many business leaders are choosing to negotiate prior to making a payment. In 2023, two in three business leaders (66 percent) chose to engage in dialogue and negotiate with their attacker before paying a ransom. This figure is up from 59 percent in 2021 but down from a high of 74 percent in 2022. Negotiation is seen by many as an opportunity to buy the organisation more time, learn about the adversary's usual tactics and tradecraft, and validate the threat including the information the criminals have purported to have stolen.

Three quarters of business leaders (74 percent) cite external risk factors as the motivation for paying, which is unsurprising given the front-page attacks and intense public scrutiny of breached organisations in 2022. The possibility of avoiding unknown consequences, for instance brand damage and potential harm to stakeholders, is seen by many as outweighing the cost of any potential ransom.

The growing 'legitimisation' of ransomware

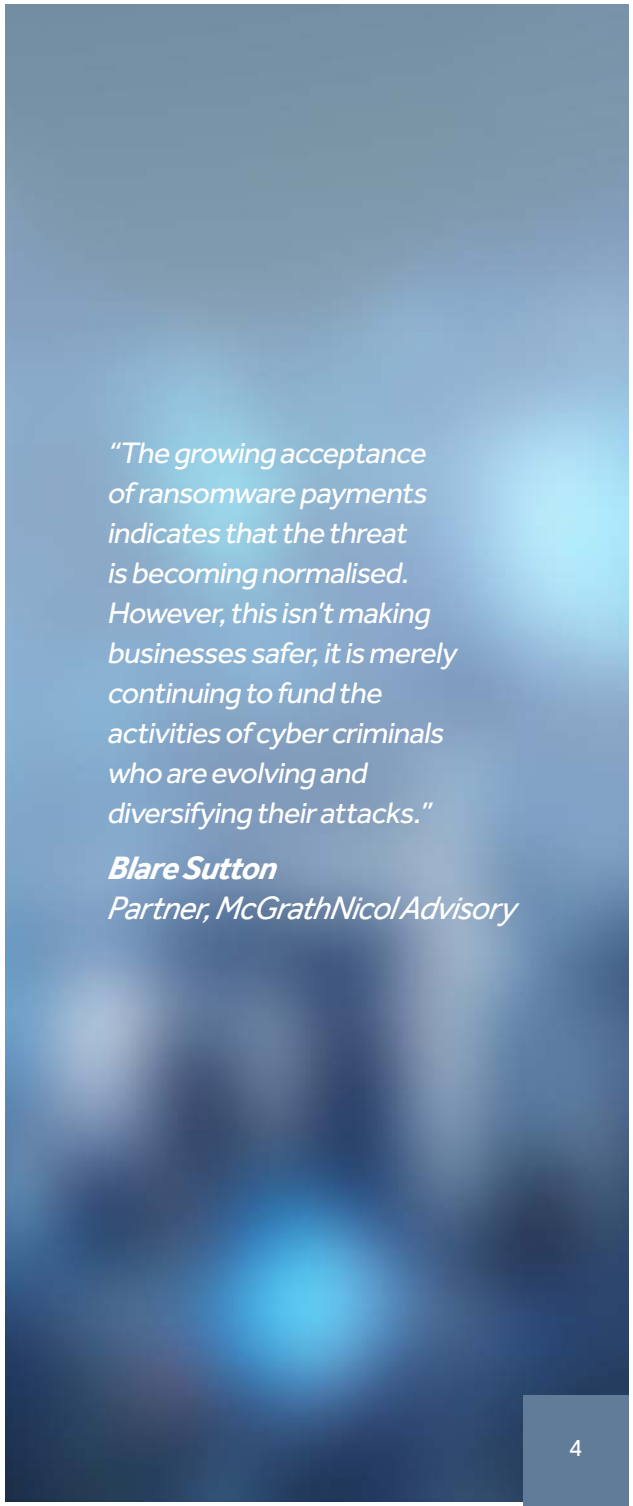
Research suggests a sentiment of 'legitimacy' towards ransomware payments across corporate Australia.

A consistently high volume of ransomware attacks over recent years has normalised the threat, leading to a softening of attitudes towards ransomware reporting. In 2022, 75 percent of surveyed executives believed that it should be mandatory for an Australian business to report a ransomware attack to the authorities, with almost three in five (56 percent) believing that it should be reported regardless of whether a ransom payment is made. However, this trend has reversed in 2023, with only 60 percent of surveyed executives saying they support mandatory reporting and less than half (46 percent) saying an attack should be reported even if a ransom hasn't been paid.

Executives' attitudes towards ransomware payments from businesses in their supply chain are easing too: 83 percent of executives say knowledge of a payment from a business they are associated with would negatively impact their perception of that business. This is down from 91 percent in 2022 and 90 percent in 2021.

When faced with external risk factors, pressures from multiple stakeholder groups, and legal and data privacy considerations, a payment is seen by many business leaders as the path of least resistance. But in many cases, a payment promotes and fuels the dark economy further, and leaves the organisation more vulnerable to multiple attacks. Without greater collaboration and knowledge-sharing between individual companies, regulators and the wider industry, our ability to prevent ransomware attacks is undermined.

A slight drop in ransomware attacks does not mean that the cyber threat is going away, but rather, that cyber criminals are diversifying their tactics for maximum impact.



"The growing acceptance of ransomware payments indicates that the threat is becoming normalised. However, this isn't making businesses safer, it is merely continuing to fund the activities of cyber criminals who are evolving and diversifying their attacks."

Blare Sutton
Partner, McGrathNicol Advisory

Complacency reduces preparation

Businesses are overconfident in their ability to respond to an attack.

Almost nine in ten (88 percent) surveyed Australian executives believe their organisation is "prepared" for a ransomware attack which is a significant uptick from 78 percent in 2022. This confidence seems overstated, with only three in five (61 percent) organisations having a cyber incident response plan in place. A further 18 percent of business leaders are unsure whether one exists within their organisation.

What should a cyber incident response plan include?

As best practice, a cyber incident response plan should include details on roles and responsibilities in the event of an attack; whether the organisation will weigh up paying a cyber ransom and negotiate, or whether this step is to be avoided completely; communications plans for both internal and external stakeholders; recovery steps; and the details of a dedicated responsible person to engage with third-party investigators during the incident and alert relevant authorities. Importantly, the incident response plan must be reviewed on a quarterly basis and regular practice drills are also highly recommended.

These steps will provide assurance to the executive team and a greater level of preparedness, rather than panic, in the case of a successful ransomware attack.

Businesses never have to face these cyber threats alone.

Organisations like the Australian Cyber Security Centre and the Office of the Australian Information Commissioner can offer practical advice, information and cyber assessment tools to determine next steps in case of a breach or successful attack. At McGrathNicol, we work closely with these government organisations and the wider industry to share intelligence and contribute to strengthening Australia's overall cyber security resilience.

Other key findings

1. Cyber criminals are finding new ways to exploit Australian businesses.

The five-year ransomware average is down from a high of 69 percent in 2022, but remains well above the 31 percent recorded in 2021 when McGrathNicol started tracking these results. The findings suggest that cyber criminals hit a ransomware peak last year and have diversified to other forms of cyber extortion in 2023.

2. Cyber insurance continues to provide peace of mind.

Four in five (80 percent) surveyed businesses believe their cyber insurance policy is good value, with 64 percent saying that their policy protection provides peace of mind. More than two in five (44 percent) executives attribute this positive perception to the role of a cyber insurance payout in protecting their business financially.

3. Email phishing remains the most common mode of entry.

Email fraud or 'business email compromise' was leveraged in 30 percent of all ransomware attacks in 2023 (on par with 21 percent in 2022).

Results

Prevalence of ransomware attacks in the past 5 years

- Overall, nearly three in five (56%) respondents say their business has experienced a ransomware attack in the past five years. Although this is lower compared to 69% in 2022, this is still substantially higher compared to 31% in 2021.
- More than two in five (42%) say their business has experienced one attack, while one in seven (14%) say their business has experienced multiple attacks. Furthermore, three in ten (29%) say their business was breached in at least one instance, while a similar proportion (27%) say their business was not breached at all.
- Respondents in businesses aged over 10 up to 20 years are more likely than those in businesses aged up to 10 years to have experienced an attack in the past five years (68% compared to 52%).
- Respondents in businesses with 1,000 or more employees are around twice as likely as those in smaller businesses to say their business has experienced multiple attacks (28% compared to 50-249 employees: 13%, 250-999 employees: 16%).

Cyber ransom payments

Among respondents in businesses attacked:

- Nearly three in four (73%) decided to pay the cyber ransom, although this is trending downwards from 79% in 2022 and 83% in 2021.
- Overall, the estimated average amount of cyber ransom paid was $1.03 million, on par with $1.01 million in 2022 and $1.07million in 2021.
- This estimated average is notably higher among those in businesses earning $50 million+ ($1.40 million), around twice as high as those in businesses earning less than $10 million ($699k).

Results

Willingness to pay a ransom

- Seven in ten (70%) respondents say the business would be willing to pay a cyber ransom if it was subjected to a ransomware attack (on par with 69% in 2022, but down from 80% in 2021), although almost one in six (15%) say the business would only do so if there was no other choice (up from 7% in 2022, on par with 12% in 2021).
- Almost one in five (18%) say the business would not pay under any circumstance (14% in 2022 and 2021), while one in eight (12%) are unsure whether the business would pay (down from 18% in 2022, up from 6% in 2021).
- Overall, the estimated average cyber ransom amount that businesses would be willing to pay is $1.32 million (on par with $1.29 million in 2021 and almost doubling from $682k in 2021).
- Specifically, almost one in four (23%) would be willing to pay $1 million or more (down from 30% in 2022 and up from 16% in 2021), while one in eight (12%) would be willing to pay between $500,000 and $999,999 (on par with 14% in 2022, up from 6% in 2021).
- The estimated average cyber ransom amount that businesses would be willing to pay is highest among businesses earning $50 million+ ($1.85 million compared to less than $10 million: $1.10 million, $10 million to less than $50 million: $1.15 million).
- Likewise, the estimated average cyber ransom amount that businesses would be willing to pay is highest among businesses aged over 20 years ($1.92 million compared to up to 10 years: $819k, over 10 up to 20 years: $1.27 million).

Results

Drivers of paying a ransom

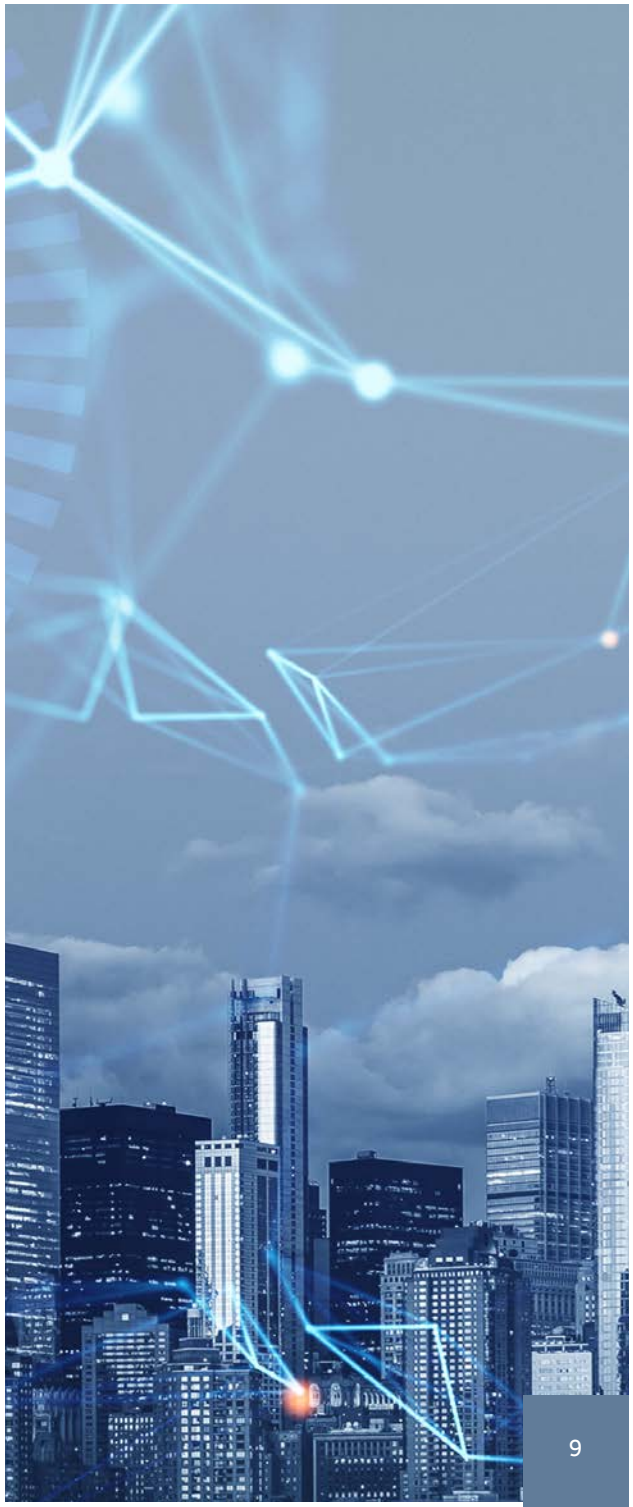
Among respondents who would pay a ransom:

- Almost three in four (74%) cite risk drivers behind their willingness to pay (68% in 2022, 69% in 2021), which include minimising potential harm to stakeholders (44%, 42% in 2022, up from 34% in 2021), reducing brand damage (39%, 34% in 2022, up from 28% in 2021) and not having sensitive information leaked on the dark web (27%, 23% in 2022, 27% in 2021).
- More than three in five (63%) cite operational drivers behind their willingness to pay (65% in 2022, up from 54% in 2021), which include getting back to normal operations faster (44%, 47% in 2022, up from 31% in 2021) and re-establishing control and access to critical infrastructure and systems (36%, 40% in 2022, 35% in 2021).
- Almost two in five (38%) would pay as insurance would cover a large percentage of the payment (43% in 2022, 34% in 2021).
- Operational drivers are more pertinent among businesses with 1,000+ employees compared to smaller businesses (82% compared to 50-249 employees: 62%, 250-999 employees: 67%), while on the other hand, risk drivers are more pertinent among smaller businesses compared to businesses with 1,000+ employees (50-249 employees: 74%, 250-999 employees: 72% compared to 59%).

Timeframe and negotiation for ransom payment

Among respondents who were attacked and paid a ransom:

- Almost two in five (37%) made payment within 24 hours (44% in 2022, 23% in 2021), while a similar proportion (38%) did so within 24 to less than 48 hours(34% in 2022, 51% in 2021). Almost one in four (23%) did so in 48 hours or longer (20% in 2022, 24% in 2021).
- Two in three (66%) negotiated prior to making payment (59% in 2022, 74% in 2021), while one in three (32%) did not negotiate (39% in 2022, 24% in 2021).
- Those in businesses with 50-249 employees are more likely than peers in businesses with 250-999 employees to have made payment within 24 hours with negotiation (28% compared to 9%), as are those in businesses aged up to 10 years compared to peers in businesses aged over 20 years (38% compared to 4%).
- On the other hand, those in businesses with 250-999 employees are more likely than peers in businesses with 50-249 employees to have made payment within 24 hours without negotiation (19% compared to 9%) or within 24 to less than 48 hours with negotiation (37% compared to 23%).



Results

Mode of entry

Among respondents in businesses attacked and breached:

- The most common mode of entry was email fraud (phishing) (30%, 21% in 2022), followed by malware or spyware (23%, 20% in 2022).
- These are followed by man-in-the-middle attack (14%, 11% in 2022),weak or compromised credentials (10%, 11% in 2022),exploitation of a common vulnerability (7%, 11% in 2022) or a zero-day vulnerability (6%, 7% in 2022), as well as malicious insider providing access (5%, 7% in 2022) and text/phone fraud (phishing) (5%, down from 12% in 2022).

Form of ransom demand

- Seven in ten (71%, 61% in 2022) say the cyber criminals demanded the ransom payment in cryptocurrency, including Bitcoin (33%, 33% in 2022) or another cryptocurrency (38%, 28% in 2022).
- Three in ten (29%, 38% in 2022) say the cyber criminals demanded the ransom payment via wire transfer.

Preparedness for cyber attacks

- Almost nine in ten (88%) respondents believe their business is prepared in responding to a cyber attack, up from 78% in 2022. However, only around one in three (35%) believe their business is very prepared, down from 51% in 2022.
- Those who are insured against ransomware are more likely than those who aren't to believe their business is prepared (91% compared to 75%), including very prepared (40% compared to 15%).
- Those in businesses with 1,000+ employees are the most likely to believe their business is very prepared (66% compared to 50-249 employees: 34%, 250-999: 39%).
- Likewise, those in businesses earning $50 million+ are the most likely to believe their business is very prepared (45% compared to less than $10 million: 29%, $10 million to less than $50 million: 27%).

Results

Prevalence of incident response plans

- Three in five (61%) respondents say their business has an incident response plan for a cyber attack (65% in 2022). However, one in five (21%) say their business doesn't (up from 15% in 2022), while a similar proportion (18%) are unsure whether their business has one (20% in 2022).
- Those in businesses with an incident response plan are more likely than those in businesses without one to believe their business is prepared in responding to a cyber attack (95% compared to 69%), including very prepared (46% compared to 15%).
- Perhaps unsurprisingly, an incident response plan is more likely to be present among businesses that have experienced a ransomware attack in the past 5 years compared to businesses that haven't (84% compared to 32%), as well as among businesses that are insured against ransomware compared to businesses that aren't (74% compared to 11%).
- An incident response plan is also more common among businesses with 1,000 or more employees compared to smaller businesses (87% compared to 50-249 employees: 60%, 250-999 employees: 61%) and among businesses aged over 20 years compared to businesses aged up to 10 years (77% compared to 49%).
- Almost two in five (37%) respondents in businesses earning $50 million are unsure whether their business has one, compared to 9% in businesses earning less than $10 million and 4% in businesses earning $10 million to less than $50 million.

Length of attack assessments

- On average, the estimated time taken to assess all required information about the attack and accurately report it to relevant stakeholders was 20.24 hours (on par with 20.80 hours in 2022).
- Specifically, three in ten (30%) say it took the business up to 6 hours to do so (up from 21% in 2022), more than one in three (35%) say this process took 7 to 12 hours (up from 25% in 2022), almost one in six (15%) say this process took 13 to 24 hours (down from 38% in 2022), while another one in six (17%) say it took the business 2 days or longer (13% in 2022).
- The estimated average is notably higher among businesses with 1,000+ employees (29.35 hours) compared to businesses with 250-999 employees (20.97 hours).

Results

Notifying the board of directors

- Three in four (76%) respondents say the board of directors would be notified in case their business was subjected to a ransomware attack (80% in 2022), including almost two thirds (64%) who say there is a notification protocol (down from 71% in 2022) and one in eight (12%) who cite another method (9% in 2022). However, almost one in six (15%) are unsure whether this would be the case (16% in 2022).
- Those in businesses that have experienced a ransomware attack in the past 5 years are more likely than peers in businesses that haven't to say the board of directors would be notified (95% compared to 53%), as are those in businesses that are insured against ransomware compared to peers in businesses that aren't (90% compared to 26%) and those in businesses that have an incident response plan compared to peers in businesses that don't (99% compared to 61%).
- Those in businesses with 1,000+ employees are more likely than peers in smaller businesses to say the board of directors would be notified (97% compared to 50-249 employees: 76%, 250-999 employees: 74%).
- Likewise, those in businesses aged over 10 years are more likely than peers in businesses aged up to 10 years to say the board of directors would be notified (over 20 years: 94%, over 10 up to 20 years: 85% compared to 60%).
- Interestingly, those in businesses earning $50 million or more are less likely than peers in businesses earning less to say the board of directors would be notified (57% compared to less than $10 million: 88%, $10 million to less than $10 million: 85%), with more than one third (36%) of those in businesses earning $50 million or more being unsure whether this would be the case.

Results

Insured against ransomware

- Four in five (79%) respondents say their business is currently insured against a ransomware attack. However, this is down from 91% in 2022, although this is on par with 84% in 2021.
- More than two in five (42%) say the insurance cover amount is less than $1 million (39% in 2022, 30% in 2021), one in seven (14%) say the cover amount is between $1 million and $1,999,999 (20% in 2022, 19% in 2021), while the same proportion (14%) say the cover amount is $2 million or more (11% in 2022, 20% in 2021).
- One in ten (9%) are insured but unsure of the cover amount (20% in 2022, 15% in 2021).
- Overall, the estimated average insurance cover amount among those who are insured is $1.37 million (on par with $1.31 million in 2022, but lower than $1.87 million in 2021).
- This figure is higher among businesses earning $50 million+ compared to businesses earning less than $10 million ($1.71 million compared to $1.11 million), as well as businesses aged over 20 years compared to businesses aged up to 10 years ($1.65 million compared to $1.14 million).

Insured or re-insured against future attacks

Among respondents whose business experienced an attack in the past five years:

- Four in five (81%) say their business was able to get insured or re-insured against future attacks after the attack (83% in 2022).
- Only 13% say their business wasn't able to get insured or re-insured (11% in 2022), while 6% say their business didn't seek to get insured or re-insured (6% in 2022).
- Interestingly, those in businesses with 1,000+ employees are the most likely to say their business didn't seek to get insured or re-insured (14% compared to 50-249 employees: 6%, 250-999 employees: 1%.

Results

Perceived value of insurance policy

Among respondents in businesses insured:

- Four in five (80%) believe their business cyber insurance policy is good value (87% in 2022). Only one in ten (10%) believe otherwise, while another one in ten (10%) are unsure if it is good value (7% and 5% respectively in 2022).

Reasons for policy being good value

- The most common reasons for the perception of good value are that the protection provides peace of mind (63%, up from 54% in 2022), followed by that the insurer helps in accessing adviceand support that will better protect the business (50%, 55% in 2022) or has helped/will help in responding to a ransomware attack (50%, 52% in 2022).
- More than two in five (44%) also attribute this perception to the role of the payout in helping to protect the business (39% in 2022).
- Those in businesses with fewer than 1,000 employees are more likely than peers in businesses with 1,000+ employees to cite the peace of mind as a factor (50-249 employees: 63%, 250-999 employees: 64%, compared to 49%), as are those in businesses aged over 20 yearscompared to peers in businesses aged over 10 up to 20 years (71% compared to 51%).
- Those in businesses earning $50 million+ are the most likely to value the insurer's help in responding to a ransomware attack(68% compared to less than $10 million: 41%, $10 million to less than $50 million: 46%) or in providing advice and support that will better protect the business (73% compared to less than $10 million: 43%, $10 million to less than $50 million: 39%).

Reasons for policy being poor value

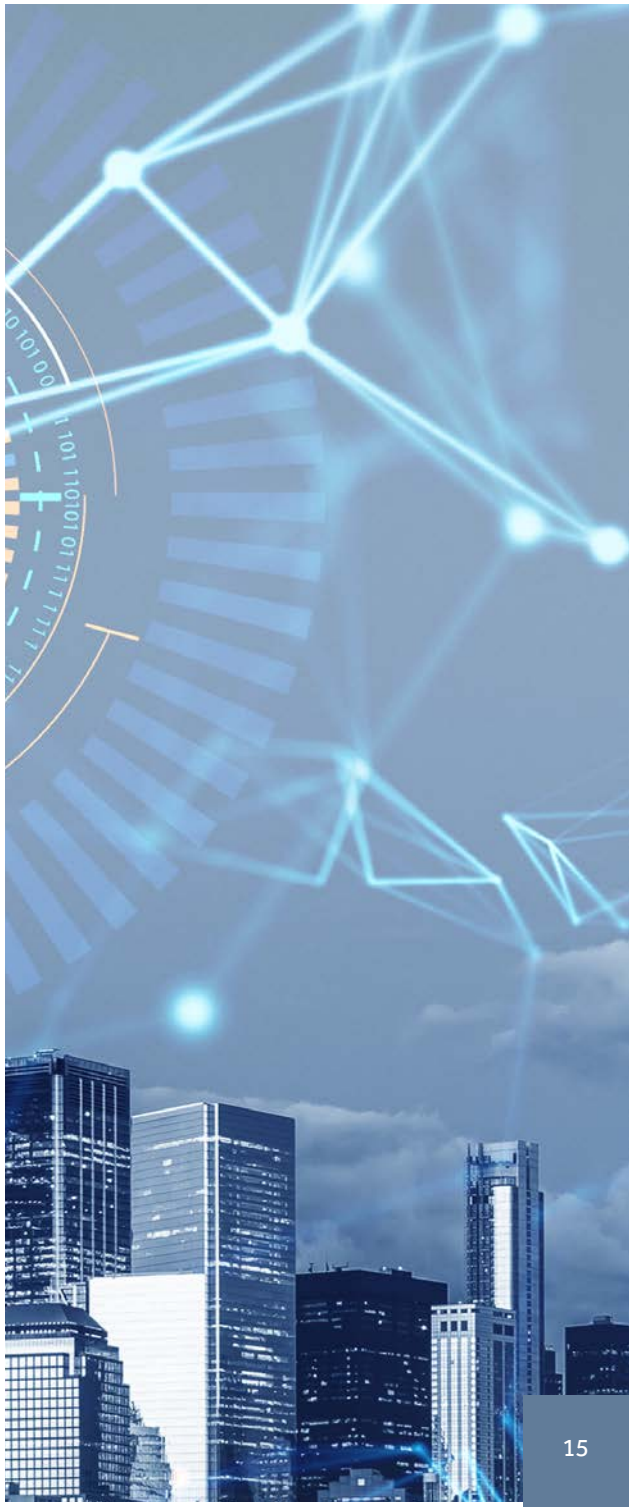
Among those respondents whose businesses are insured and who don't believe, or are unsure whether, their policy is good value:

- The most common reasons for this view include: the premiums are too high (40%, 31% in 2022), and the policy has too many stipulations attached which means they don't feel confident the insurer will accept a claim (38%, down from 59% in 2022).
- These are followed by a view that the policy does not provide adequate financial protection (29%, 28% in 2022) and that the insurer does not provide adequate advice and support that will better protect the business (28%, 21% in 2022).

Results

Awareness and attitude to paying a ransom

- Although seven in ten (70%) respondents claim to be aware that paying a ransom finances criminal organisations, this is down from 82% in 2022 (66% in 2021), with almost half (47%) also saying that it is a key factor in their decision of to pay or not to pay (down from 59% in 2022, up from 36% in 2021), and almost one in four (23%) saying that it is not (24% in 2022, down from 30% in 2021).
- Three in ten (30%) are unaware that paying a ransom finances criminal organisations(up from 18% in 2022, on par with 34% in 2021), with one in eight (13%) saying that it is now a key factor in their decision of to pay or not to pay (up from 7% in 2022, 17% in 2021) and almost one in five (18%) saying that it is not (up from 11% in 2022, 16% in 2021).
- Overall, the consequences of paying a ransom act as a key factor in the decision of to pay or not to pay for three in five (59%) respondents (65% in 2022, 54% in 2021).
- Those in businesses that experienced a ransomware attack in the past 5 years are more likely than peers in businesses that didn't to claim to be aware (79% compared to 58%), as are those in businesses that are insured against ransomware compared to peers in businesses that aren't (74% compared to 55%) and those in businesses that have an incident response plan compared to peers in businesses that don't (79% compared to 58%).
- Likewise, those in businesses with 1,000+ employees are more likely than peers in businesses with 50-249 employees to claim to be aware (84% compared to 69%), as are those in businesses aged over 20 years compared to peers in businesses aged up to 10 years (78% compared to 64%).



Results

Reporting ransomware attacks to authorities

- Although three in five (60%) respondents believe it should be mandatory for a business to report a ransomware attack to the authorities, this is down from 75% in 2022 (and down from 67% in 2021).
- Less than half (46%) believe a ransomware attack should be reported regardless of whether a payment is made (down from 56% in 2022, on par with 43% in 2021), while one in three (32%) believe it should be reported only when a payment is made (down from 45% in 2022, up from 24% in 2021). Three in five (61%) believe a cyber incident or data breach of any kind should be reported to the authorities (up from 52% in 2022, on par with 54% in 2021).
- Those in businesses that experienced a ransomware attack in the past 5 years are more likely than peers in businesses that didn't to believe it should be mandatory for a business to report a ransomware attack to the authorities (67% compared to 50%), as are those in businesses that are insured against ransomware compared to peers in businesses that aren't (68% compared to 27%).
- Likewise, those in businesses that have an incident response plan are more likely than peers in businesses that don't to believe it should be mandatory for a business to report a ransomware attack to the authorities (71% compared to 46%).
- Those in businesses with 1,000+ employees are more likely than peers in smaller businesses to believe a cyber incident or data breach of any kind should be reported to the authorities (73% compared to 50-249 employees: 61%, 250-999 employees: 57%).
- Those in businesses aged over 20 years are more likely than peers in businesses aged up to 10 years to believe a cyber incident or data breach of any kind (70% compared to 54%) or a ransomware attack (70% compared to 50%) should be reported to the authorities.

Results

Impact and knowledge of ransomware payment

- More than four in five (83%) respondents say knowledge of a ransomware payment from a business in their supply chain/a business they are associated with would impact their perception of that business (down from 91% in 2022 and 90% in 2021).
- More than one in three (35%) say paying a ransom means the business does not have safeguards in place (down from 44% in 2022, on par with 31% in 2021), while a similar proportion (37%) say they wouldn't want company data to be at risk (33% in 2022, 36% in 2021). More than two in five (44%) also say their business would not associate with businesses funding criminal activity (40% in 2022, 38% in 2021).
- Those in businesses that experienced a ransomware attack in the past 5 years are more likely than peers in businesses that didn't to say their perception would be impacted (95% compared to 67%), as are those in businesses that are insured against ransomware compared to peers in businesses that aren't (93% compared to 44%).
- Interestingly, those in businesses earning $50 million+ are less likely than peers in businesses earning less to say their perception would be impacted (69% compared to less than $10 million: 93%, $10 million to less than $50 million: 85%), as are those in businesses aged up to 10 years compared to more established businesses (71% compared to over 10 up to 20 years: 90%, over 20 years: 94%).

Contacts

Darren Hopkins
Partner, Brisbane
M +61 416 151 419
E dhopkins@mcgrathnicol.com

Darren advises businesses on both proactive and reactive uses of technology in cybersecurity, privacy, digital forensics and technology-led investigations. He regularly works with boards, executives and senior business leaders.

Tony Barnes
Partner, Brisbane
M +61 448 068 548
E tbarnes@mcgrathnicol.com

Tony is an internationally experienced technology strategy and cybersecurity advisor, with more than 25 years of experience as a senior executive and non-executive director in critical industries, technology, software and cybersecurity.

Brendan Payne
Partner, Perth
M +61 403 153 162
E bpayne@mcgrathnicol.com

Brendan is a forensic technology and cyber specialist with more than 16 years of experience specialising in digital forensics, cyber incident response, cyber risk and governance, eDiscovery and technology-led investigations.

Joss Howard
Partner, Sydney
M +61 460 972 700
E jhoward@mcgrathnicol.com

Joss advises Boards and senior management on effective information and cyber security strategies, helping to set the 'tone from the top'. Built over a 25 year career leading and implementing security programs, she is an expert in risk assessment and cyber resiliency.

Jamie Norton
Partner, Canberra
M +61 438 643 170
E jnorton@mcgrathnicol.com

Jamie specialises in cybersecurity strategy, program development, governance, risk, and operations. He has 20 years experience in managing security resilience for State and Federal Government agencies and commercial organisations.

Blare Sutton
Partner, Melbourne
M +61 417 252 739
E bsutton@mcgrathnicol.com

Blare is a highly regarded forensic expert with more than 20 years of experience in technology and cyber. He manages highly sensitive engagements involving internal and external actors, law enforcement, financial institutions and civil remedies.

This study was conducted online between 19 September and 3 October 2023 by YouGov. The study was conducted via online survey as an ad-hoc study, targeting owners/partners, board members, and C-suites in Australian businesses with 50+ employees. The sample is comprised of 502 respondents. The findings have been weighted by business size and location, and the sample is representative of approximately 60,000 Australian medium and large businesses with 50+ employees.


mcgrathnicol.com