McGrathNicol

Ransomware: Rising Threats and Resilience

Average ransomware payment soars to $1.35 million, as Australian businesses increasingly willing to pay.

2024 Survey — In Partnership with YouGov Australia

Contents

Summary of 2024 findings

For the fourth year, McGrathNicol has created an authoritative barometer of the ransomware threat in Australia. We have partnered 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 the ransomware threat has become increasingly 'normalised', as the majority of businesses have now suffered an attack and chosen to pay a ransom.

69%

of surveyed businesses have experienced a ransomware attack in the past five years

42%

fell victim to a single attack, **26%** were targeted repeatedly

84%

of businesses that suffered a ransomware attack in the past five years paid a ransom

75%

paid the ransom within 48 hours

65%

negotiated prior to making a ransom payment

$1.35m vs **$1.42m**

estimated average cyber ransom that was paid

average ransom business leaders would be 'willing' to pay

79%

of business leaders say it should be mandatory to report ransomware attacks to the authorities

↑ from 60% in 2023

88%

say their view of a company would be negatively affected upon learning of a ransom payment

↑ from 83% in 2023

93%

of business leaders believe their organisation is 'prepared' for a ransomware attack

↑ from 88% in 2023

80%

of businesses have an incident response plan in place

↑ from 61% in 2023

44%

of businesses have experienced a malware attack or a Business Email Compromise attack (39%) in the past 12 months

Average ransomware payment soars to $1.35 million

The 2024 McGrathNicol Ransomware Survey provides a comprehensive view of the state of ransomware across Australian businesses of all sizes and sectors, from small and medium-sized businesses to large enterprises. The insights from our survey emphasise the critical importance of preparation, investment in cybersecurity, and a coordinated incident response. The findings reflect the true impact ransomware has on our economy, highlighting vulnerabilities and the significant progress organisations are making in addressing these threats.

In the past five years, 69% of businesses have experienced a ransomware attack, a notable increase from 56% in 2023. This sharp rise underscores the urgency for businesses to develop robust strategies for responding to ransomware incidents. Alarmingly, of those affected by ransomware in the past five years, 84% opted to pay the ransom with the average payment now soaring to $1.35 million (up from $1.03 million in 2023). The research shows that 83% of businesses, including those yet to experience an attack, would be 'willing' to pay a cyber ransom. These trends highlight the significant financial burden cyber attacks place on organisations. The survey aims to empower boards and executives to make more informed decisions when confronted with the ransomware reality.

Reporting changes may have desired effect

This year, the Federal Government has worked with businesses of all sizes to determine the best course of action when it comes to thwarting the threat of ransomware. Following extensive consultation, legislative changes have been designed to encourage greater collaboration and threat intelligence-sharing between businesses and government. A secondary objective is to quantify the sheer size of funds flowing from Australia to cyber threat actors and organised crime groups.

New legislation will require organisations with a turnover of $3 million or more to report any ransomware payments to the Australian Signals Directorate. Fines of up to 60 penalty units ($18,780) have been put forward for businesses and organisations that fail to report ransomware payments.

There has been overwhelming support for these changes. In fact, according to the McGrathNicol research, four in five (79%) respondents believe it should be mandatory for a business to report a ransomware attack to the authorities (a significant increase from 60% in 2023). Meanwhile, three in five (59%, up from 46% in 2023) argue that a ransomware attack should be reported regardless of whether a payment has been made. As online crime continues to wreak havoc on Australian businesses and consumers, more than three in five (62%) believe a cyber incident or data breach of any kind should be reported to the authorities.

Businesses weigh the hidden costs of an attack

The findings show how critical the first 48 hours after a ransomware attack really are. Three quarters of businesses chose to make a ransom payment within this timeframe, and frequently, this is because other hidden risks and costs to a business come into consideration.

Cyber attacks have negative consequences for more than just the IT team. Over half (54%) of respondents say the attack their business experienced had a severe or significant impact on their finance operations, with more than 30% citing "a significant impact resulting in major disruptions and extended delays". Further, half of respondents (50%) say there was a severe or significant impact on their Human Resources function and nearly three in five explained that the breach had negatively impacted their Sales department (57%) and the wider supply chain (57%).

Of concern is the fact that more than four in five businesses would be willing to pay a cyber ransom if subjected to a successful ransomware attack (up from 70% in 2023). Over time, the estimated amount that businesses would be willing to hand over has also continued to increase, from $1.31 million in 2023 to $1.42 million in 2024. Specifically, more than a third of businesses (34%) would be willing to pay $1 million or more. As ransom payments become more frequent and 'normalised' in Australia, only one in ten businesses say they would not pay under any circumstances (down from 18% in 2023).

Other key findings

Encouragingly, businesses are becoming more proactive in their cybersecurity measures:

- 91% of businesses are now insured against ransomware attacks, with an average coverage amount of $1.47 million, a significant rise from 79% in 2023.
- 80% of businesses have an incident response plan in place (up from 61% in 2023), indicating that more organisations are taking the right steps to prepare for potential attacks.
- 77% of businesses now have a formal board notification protocol (compared to 64% in 2023), ensuring that leadership is informed and involved in addressing cyber risks.

Results

Prevalence of ransomware attacks in the past five years

- Overall, seven in ten (69%) respondents say their business has experienced a ransomware attack in the past five years. This is still substantially higher compared to 56% in 2023, and on par with 69% in 2022.
- One in two (50%) say their business has experienced one attack, while nearly one in five (18%) say their business has experienced multiple attacks. Furthermore, more than two in five (42%) say their business was breached in at least one instance, while one in four (26%) say their business was attacked but not breached at all.
- Respondents in businesses aged up to 10 years are more likely than those aged over 10 years to say their business has experienced a ransomware attack in the past five years (84% compared to over 10 years up to 20 years: 57%, over 20 years: 45%).
- Respondents in businesses with up to 999 employees are more likely than those in businesses with 1000+ employees to report that their business has been attacked and breached in the past five years (50-249: 43%, 250-999: 38% compared to 19%).

Prevalence of ransomware attacks in the past 12 months

- Overall, nearly three in five (56%) respondents say their business has experienced a ransomware attack in the past 12 months. Of those that have experienced an attack in the past 12 months, 89% decided to pay a cyber ransom.
- Respondents in businesses aged up to 10 years are more likely than those aged over 10 years to say their business has experienced a ransomware attack in the past 12 months (71% compared to over 10 years up to 20 years: 48%, over 20 years: 28%).
- Respondents in businesses with 50-999 employees are more likely than those in businesses with 1000+ employees to report that their business has experienced a ransomware attack in the past 12 months (50-249: 57%, 250-999: 54% compared to 31%).

Results

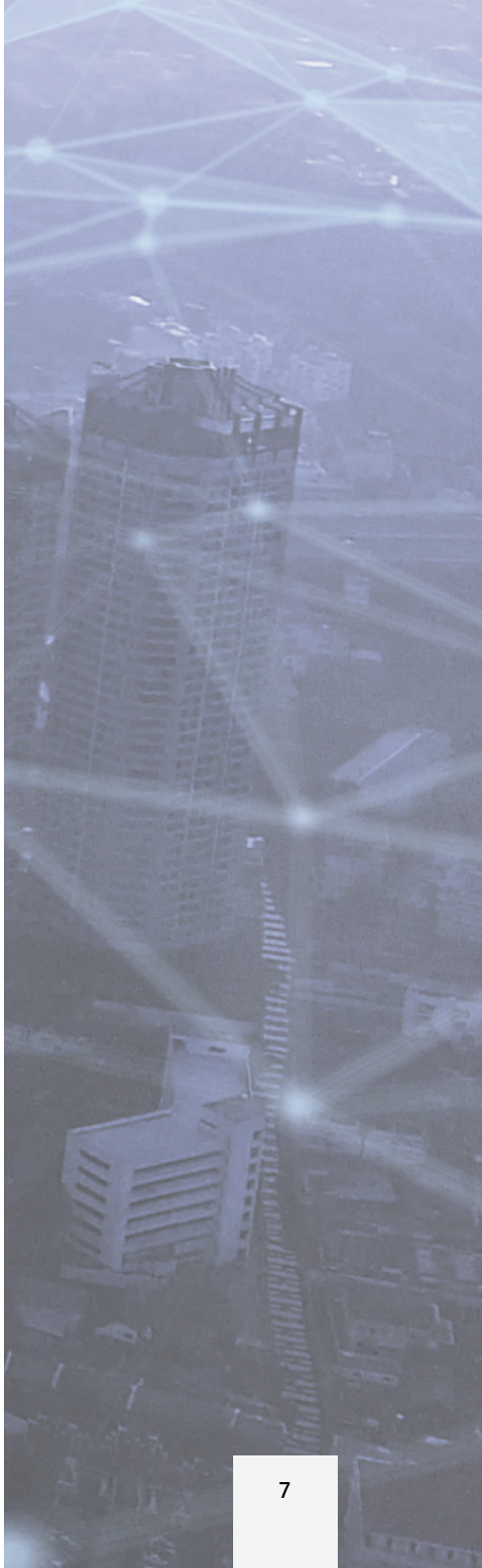
Other cyber attacks on businesses over the past 12 months

- Around two in five (44%) respondents say their business has experienced a malware attack in the past 12 months, while a similar proportion say their business has experienced a phishing attack (39%) or a Business Email Compromise (BEC) (39%) during this time.
- Just over a third (35%) say their business has experienced an attack exploiting unpatched vulnerabilities in the past 12 months, while one in five (19%) say their business hasn't experienced any of these cyber attacks during this period.
- Respondents in businesses aged up to 10 years are more likely than respondents in businesses over 10 years old to say their business has experienced a BEC (50% compared to over 10 years up to 20 years: 31%, over 20 years: 23%), phishing attack (49% compared to over 10 years up to 20 years: 27%, over 20 years: 31%) or an attack to exploit unpatched vulnerabilities (43% compared to over 10 years up to 20 years: 32%, over 20 years: 17%) in the past 12 months.

Group responsible for ransomware attack

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

- Nearly one in five (17%) say LockBit was responsible for the attack, while one in seven believe it was RansomHub. Around one in ten say Sandworm (9%), Dark Angels (8%), Whitewarlock (6%) or Black Basta (6%) were responsible for their business' ransomware attack.
- However, just over one in ten (12%) are unsure who was responsible for the attack.
- LockBit is more likely to have been responsible for attacking businesses with a higher annual turnover than those with a lower annual turnover ($50 million+: 27% compared to less than $10 million: 12%, $10 million to less than $50 million: 11%).



Results

Mode of entry

Among respondents whose business experienced an attack and was breached:

- Email fraud (24%, 30% in 2023) and malware or spyware (22%, 23% in 2023) were the most common modes of entry.
- These were followed by a man-in-the-middle attack (11%, 14% in 2023), text/phone fraud (phishing) (11%, 5% in 2023), a malicious insider providing access (8%, 5% in 2023), exploitation of a zero-day vulnerability (7%, 6% in 2023), weak or compromised credentials (7%, 10% in 2023) and exploitation of a common vulnerability (7%, 7% in 2023).

Form of ransom demand

Among respondents whose business experienced an attack and was breached:

- Nearly three in five (73%, 71% in 2023, 61% in 2022) say the cyber criminals demanded the ransom payment to be in cryptocurrency – inclusive of Bitcoin (49%, an increase from 33% in 2023 and 33% in 2022) or other forms of cryptocurrency (24%, 38% in 2023, 28% in 2022).
- One in four (26%, 29% in 2023) say the cyber criminals demanded the ransom to be paid via wire transfer.

Results

Cyber ransom payments

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

- More than four in five (84%) decided to pay the cyber ransom, an increase from last year (73% in 2023, 79% in 2022).
- Overall, the estimated average amount of cyber ransom paid was $1.35 million, an increase from $1.03 million in 2023 and $1.01 million in 2022.
- Those in businesses earning $50 million+ estimated that they paid more on average than their counterparts in businesses earning less ($1.8 million compared to less than $10 million: $1.1 million, $10 million to less than $50 million: $1.1 million)

Timeframe and negotiation for ransom payment

Among respondents in businesses that were attacked and paid a ransom:

- One in five (21%) made payment within 24 hours (down from 37% in 2023 and 44% in 2022), while more than half (53%) did so within 24 to less than 48 hours (up from 38% in 2023 and 34% in 2022). Almost one in four (24%) did so in 48 hours or longer (23% in 2023, 20% in 2022).
- Two in three (65%) negotiated prior to making payment (66% in 2023, 59% in 2022), while one in three (33%) did not negotiate (32% in 2023, 39% in 2022).
- Those in businesses earning $50 million+ annually were around three times as likely as those in businesses earning less to report that the ransom was paid within 24 hours without negotiation (17% compared to less than $10 million: 5%, $10 million to less than $50 million: 6%).

Results

Willingness to pay a ransom

- More than four in five (83%) respondents say the business would be willing to pay a cyber ransom if it was subjected to a ransomware attack (up from 70% in 2023, 69% in 2022), although almost one in six (14%) say the business would only do so if there was no other choice (15% in 2023, 7% in 2022).
- One in ten (10%) say the business would not pay under any circumstance (18% in 2023, 14% in 2022), while 7% are unsure whether the business would pay (12% in 2023, 18% in 2022).
- Overall, the estimated average cyber ransom amount that businesses would be willing to pay is $1.42 million ($1.31 million in 2023. $1.29 million in 2022).
- Specifically, one in three business (34%) would be willing to pay $1 million or more (23% in 2023, 30% in 2022), while one in four (23%) would be willing to pay between $500,000 and $999,999 (up from 12% in 2023, 14% in 2022).
- The estimated average cyber ransom amount that businesses would be willing to pay is highest among businesses earning $50 million+ ($1.9 million compared to less than $10 million: $1.17 million, $10 million to less than $50 million: $1.17 million).
- Those in older businesses aged over 10 years are more likely than those in businesses aged up to 10 years to say their business wouldn't pay a ransom under any circumstance(over 20 years: 20% and over 10 years up to 20 years: 14% compared to up to 10 years: 4%), as are those in businesses with 1,000+ employees (20%) compared to those with up to 50-999 employees (50-249: 10%, 250-999: 9%).
- In contrast, those in businesses aged up to 10 years are more likely than those in businesses aged 10 years or older to say their business would pay an amount (81% compared to over 10 years up to 20 years: 65%, over 20 years: 44%), as are those in businesses with 50-249 employees (71%) compared to those in businesses with 250+ employees (250-999: 60%, 1,000+: 52%).

Results

Length of attack assessment

Among respondents whose business experienced an attack:

- On average, the estimated time taken to assess all required information about the attack and accurately report it to relevant stakeholders was 23.37 hours (20.24 hours in 2023, 20.82 hours in 2022).
- More specifically, one in five (19%) say it took the business up to 6 hours to do so (30% in 2023, 21% in 2022), three in ten (29%) say this process took 7 to 12 hours (35% in 2023, 25% in 2022), a similar proportion say it took 13 to 24 hours (28%, 15% in 2023, 38% in 2022), while one in five (21%, 17% in 2023, 13% in 2022) say it took the business 2 days or more.
- The estimated average is notably higher among those unaware of the consequences of ransomware (34.09 hours) compared to those who are aware of them (21.47 hours) and among businesses with 250-999 employees relative to businesses with 50-249 employees (31.21 hours compared to 22.74 hours).

Estimated length of attack assessment

Among respondents in businesses not yet attacked and/or not breached:

- In case of an attack, on average, the predicted estimated time taken to assess all required information about the attack and accurately report it to relevant stakeholders is 18.96 hours on par with 17.82 hours in 2023 (16.52 hours in 2022), but notably lower compared to the average actual estimated time taken of 23.37 hours among businesses attacked.
- Specifically, in case of a successful attack, more than one in four (27%) predict that it would take the business up to 6 hours (27% in 2023, 24% in 2022), one in six (16%) predict that it would take the business 7 to 12 hours (19% in 2023, 15% in 2022), while nearly one in four (23%) predict that it would take the business 13 to 24 hours (13% in 2023, 19% in 2022).
- Interestingly, one in five (20%) are unsure how long it would take (12% in 2023, 9% in 2022), while 5% are unsure if it would be reported to relevant stakeholders (18% in 2023, 28% in 2022).
- The average figure is nearly twice as high among businesses with 250-999 employees than among businesses with 50-249 employees (30.96 hours compared to 17.52 hours) and among businesses earning $50 million or more than among businesses earning $10 million to less than $50 million (23.23 hours compared to 13.65 hours).

Results

Insured against ransomware

- Nine in ten (91%) respondents say their business is currently insured against a ransomware attack (79% in 2023, 91% in 2022).
- More than two in five (42%) say the insurance cover amount is less than $1 million (42% in 2023, 39% in 2022), one in four (25%) say the cover amount is between $1 million and $1,999,999 (14% in 2023, 20% in 2022), while one in seven (15%) say the cover amount is $2 million or more (14% in 2023, 11% in 2022).
- One in ten (9%) are insured but unsure of the cover amount (9% in 2023, 20% in 2022).
- Overall, the estimated average insurance cover amount among those who are insured is $1.47 million ($1.37 million in 2023, $1.31 million in 2022).
- This figure is higher among businesses earning $50 million+ compared to businesses earning less than $10 million or $10 million to less than $50 million ($1.74 million compared to $1.34 million and $1.31 million respectively), as well as businesses with 1,000+ employees compared to businesses with 50-249 employees ($2.08 million compared to $1.45 million).

Insured or re-insured against future attacks

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

- Nine in ten (89%) say their business was able to get insured or re-insured against future attacks after the attack (81% in 2023, 83% in 2022). Only 8% say their business wasn't able to get insured or re-insured (13% in 2023, 11% in 2022), while only 3% say their business didn't seek to get insured or re-insured (6% in 2023, 6% in 2022).
- Interestingly, those in businesses that decided to pay the ransom are more likely than peers in businesses that didn't to say the business was able to get insured or re-insured (92% compared to 74%), as are those in businesses aged up to 10 years relative to peers in businesses aged over 20 years (92% compared to 80%).

Results

Preparedness for cyber attacks

- Compared to previous years, more respondents believe their business is prepared in responding to a cyber attack (93%, 88% in 2023, 78% in 2022), inclusive of nearly one in two (48%, 35% in 2023, 51% in 2022) who believe their business is very prepared.
- Just three in ten (28%) respondents who don't/are unsure if their business has an incident response plan say their business is very prepared in responding to a cyber attack.
- Those in larger businesses with 250+ employees are more likely to say that their business is very prepared in responding to a cyber attack than those with 50-249 employees (250-999: 58%, 1,000 or more: 70% compared to 50-249: 47%).
- Those in newer companies aged up to 10 years are more likely than those in older companies aged over 10 years to believe their business is very prepared in responding to a cyber attack (56% compared to over 10 years, up to 20 years: 39%, over 20 years: 40%).

Prevalence of incident response plans

- Four in five (80%) respondents say their business has an incident response plan for a cyber attack, an increase compared to previous years (61% in 2023, 65% in 2022). Nearly one in seven say their business doesn't have an incident response plan for a cyber attack (13%, 21% in 2023, 15% in 2022), while just under one in ten are unsure if they do (8%, 18% in 2023, 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 (97% compared to 79%), including very prepared (53% compared to 28%).
- Perhaps unsurprisingly, an incident response plan is more likely to be present among businesses that have experienced a ransomware attack in the past five years compared to businesses that haven't (88% compared to 63%).

Results

Notifying the board of directors

- More than nine in ten (92%) respondents say the board of directors would be notified in case their business was subjected to a ransomware attack (up from 76% in 2023, 80% in 2022), including three in four (77%) who say there is a notification protocol (64% in 2023, 71% in 2022) and one in seven (15%) who cite another method (12% in 2023, 9% in 2022). Just 4% are unsure whether this would be the case, a decrease compared to previous years (15% in 2023, 16% in 2022).
- Those in businesses that have experienced a ransomware attack in the past five years are more likely than peers in businesses that haven't to say the board of directors would be notified (97% compared to 81%) and those in businesses that have an incident response plan compared to peers in businesses that don't (96% compared to 73%).
- Those in businesses with 250-999 employees are more likely than those in businesses with 50-249 employees to say that the board of directors would be notified and that there is a notification protocol in place (90% compared to 76%).
- On the other hand, those in businesses with 50-249 employees are more likely than those in businesses with 250-999 employees to say that while the board of directors would be notified, they don't have a notification protocol in place or that this would occur via another method (16% compared to 8%).
- Those in newer businesses aged up to 10 years are more likely than those in businesses aged over 10 years up to 20 years to say the board of directors would be notified and there's a notification protocol in place (82% compared to 67%).
- While those in businesses aged over 10 years up to 20 years are more likely than those in businesses aged up to 10 years to say the board of directors would be notified, but there's no notification protocol in place or it would occur via another method (21% compared to 13%).

Results

Drivers of paying a ransom

Among respondents who would pay a ransom:

- Three in four (74%, 63% in 2023, 65% in 2022) cite operational drivers for their willingness to pay a ransom, an increase compared to previous years – specifically re-establishing control and access to critical infrastructure and systems (48%, up from 36% in 2023 and 40% in 2022) and getting back to normal operations faster (46%, 44% in 2023, 47% in 2022).
- A similar proportion (73%, 74% in 2023, 68% in 2022) cite risk drivers for their willingness to pay a ransom – specifically minimising potential harm to stakeholders and others (47%, 44% in 2023, 42% in 2022), reducing brand damage (38%, 39% in 2023, 34% in 2022) and not having sensitive information leaked on the dark web (21%, 27% in 2023, 23% in 2022).
- While more than half (52%, 38% in 2023, 43% in 2022) would pay as insurance would cover a large percentage of the payment, an increase compared to previous years.
- Risk drivers are more pertinent among those in new companies aged up to 10 years are more likely than those in old companies aged over 20 years (78% compared to 62%), in addition to companies earning $50 million or more annually (78%) compared to companies earning less than $10 million annually (64%).
- Minimising the potential for harm to stakeholders and others is more likely to be cited as a driver among those in businesses that have experienced a ransomware attack in the last five years (51%) compared to those in businesses that haven't (34%).
- While getting back to normal business operations faster is more likely to be cited as a driver among those in businesses who haven't experienced a ransomware attack in the last five years (58%) compared to those in businesses that have (42%).

Results

Awareness and attitude to paying a ransom

- Four in five (81%, 70% in 2023, 82% in 2022) respondents claim to be aware that paying a ransom finances criminal organisations, with almost half (46%, 47% in 2023, 59% in 2022) saying that it is a key factor in deciding whether to pay, and a third (34%, up from 23% in 2023 and 24% in 2022) saying it isn't.
- One in five (19%, 30% in 2023, 18% in 2022) respondents aren't aware that paying a ransom finances criminal organisations – of these, one in seven (13%, on par with 13% in 2023, 7% in 2022) say that it is now a key factor in deciding whether to pay, and 6% (down from 18% in 2023, 11% in 2022) saying it isn't.
- 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 (60%) respondents (59% in 2023, 65% in 2022).
- Those in businesses earning less than $10 million annually are more likely than those in businesses earning $10 million or more annually to admit they weren't aware that paying a ransom finances criminal organisations, but that it's not a key factor in their decision to pay or not (13% compared to $10 million to less than $50 million: 3%, $50 million or more: 4%).
- Those in businesses aged up to 20 years are more likely than those in businesses aged over 20 years to say that while they're aware that paying a ransom finances criminal organisations, this isn't a key factor in their decision to pay or not (up to 10 years: 36%, over 10 years, up to 20 years: 41% compared to over 20 years: 22%).

Results

Reporting ransomware attacks to authorities

- Four in five (79%) respondents believe it should be mandatory for a business to report a ransomware attack to the authorities (60% in 2023, 75% in 2022).
- More than three in five (62%, 61% in 2023, 52% in 2022) believe a cyber incident or data breach of any kind should be reported to the authorities.
- Three in five (59%, 46% in 2023, 56% in 2022) believe a ransomware attack should be reported regardless of whether a payment is made, while one in two (51%, 32% in 2023, 45% in 2022) believe it should only be reported when a payment is made.
- Those in businesses that experienced a ransomware attack in the past five 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 (85% compared to 65%), as are those in businesses with an incident response plan (83%) compared to those in businesses that don't/are unsure if they do (63%).
- Those in businesses with 50-999 employees are more likely than those in businesses with 1000+ employees to believe that it should be mandatory for a business to report a ransomware attack only where a ransom payment is made (50-249: 52%, 250-999: 48% compared to 31%), as are those in newer businesses aged up to 10 years (60%) compared to those in businesses aged over 10 years (over 10 years up to 20 years: 39%, over 20 years: 45%).
- Those in businesses aged up to 20 years are more likely than those in businesses aged over 20 years to say that while they're aware that paying a ransom finances criminal organisations, this isn't a key factor in their decision to pay or not (up to 10 years: 36%, over 10 years, up to 20 years: 41% compared to over 20 years: 22%).

Results

Impact of knowledge of a ransomware payment

- Nearly nine in ten (88%, 83% in 2023, 91% in 2022) respondents say that 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:
  - One in two (50%, 44% in 2023, 40% in 2022) say their business will not associate with businesses funding criminal activity, while a similar proportion (47%, 35% in 2023, 44% in 2022) say paying a ransom means the business doesn't have safeguards in place.
  - Two in five (40%, 37% in 2023, 33% in 2022) say they wouldn't want their company data to be at risk.
- Those in businesses that experienced a ransomware attack in the past five years are more likely than peers in businesses that didn't to say their perception would be impacted (94% compared to 76%) – specifically that their business will not associate with other businesses funding criminal activity (55% compared to 39%), and that paying a ransom means they do not have safeguards in place (54% compared to 31%).
- While those in businesses who have paid a cyber ransom are more likely than those in businesses who haven't to say their perception would be impacted (96% compared to 84%) – particularly that paying a ransom means they do not have safeguards in place (59% compared to 30%).
- Those in older businesses aged over 20 years are more likely than those in businesses aged up to 20 years to say that their perception would be impacted because they don't want their company data to be at risk (61% compared to up to 10 years: 35%, over 10 years up to 20 years: 32%).

Contacts

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

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

Sara Deady
Partner, Sydney
M +61 420 941 295
E sdeady@mcgrathnicol.com

Matt Grant
Partner, Sydney
M +61 439 205 873
E mgrant@mcgrathnicol.com

Melinda Hogan
Partner, Clients & Markets, Melbourne
M +61 408 313 647
E mhogan@mcgrathnicol.com

Alex Morkos
Partner, Sydney
M +61 400 090 074
E amorkos@mcgrathnicol.com

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

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

Mark Wroniak
Partner, Sydney
M +61 417 860 736
E mwroniak@mcgrathnicol.com

The 2024 McGrathNicol Ransomware Survey was conducted online between 19 September and 30 September 2024 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 500 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