McGrathNicol

RANSOMWARE ON THE RISE

Businesses are willing to pay double the cyber ransom in 2022, at a faster rate

Contents

A threat to Australian businesses

69% of businesses have now experienced a ransomware attack in the past five years.

In its second year, McGrathNicol Advisory in conjunction with YouGov, surveyed over 500 Australian business owners, partners, directors and C-Suite leaders to deliver a real-world barometer on changing attitudes towards cyber ransoms and associated board-level challenges. The study shows the true extent of ransomware attacks on Australian businesses and the willingness of leaders to make substantial payments to cybercrime groups.

The 2022 research found that almost seven in ten (69 percent) businesses have now experienced a ransomware attack in the past five years, which is a significant increase from 31 percent in 2021. Of those experiencing an attack, four in five (79 percent) businesses chose to pay the ransom and the average cyber ransom amount paid was $1.01 million which is consistent with the prior year.

However, the average amount that businesses would be willing to pay is considerably higher and has almost doubled to $1,288,608 compared to $682,123 in 2021. This shows that businesses are anticipating the financial fallout of a cyber breach far better than they were 12 months ago.

79%

of businesses who have experienced a ransomware attack chose to pay the ransom.

59%

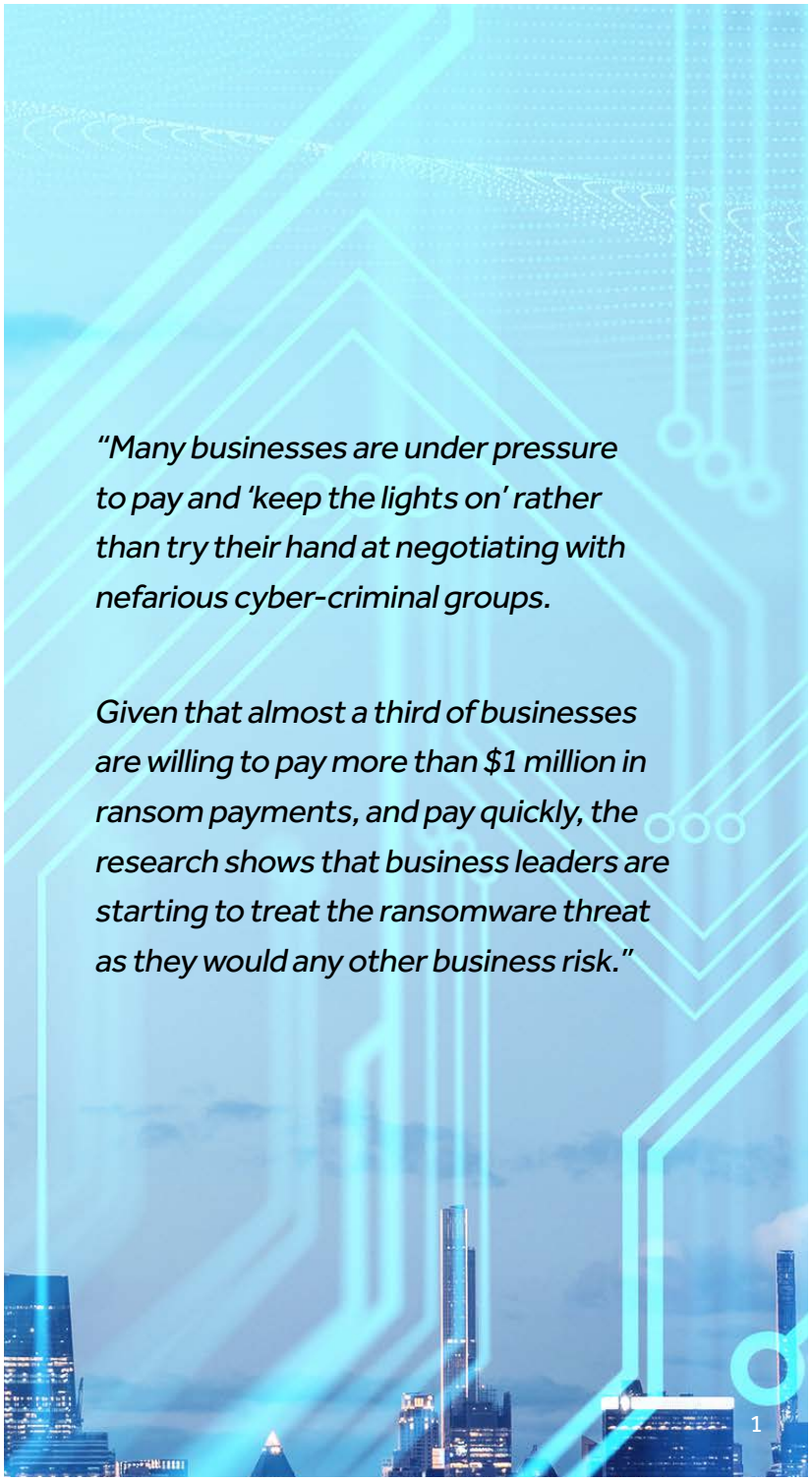
of businesses who paid a ransom chose to negotiate with cyber criminals, compared to 74% last year.

44%

of business leaders would pay a ransom within 24 hours to minimise potential damage.

$1.28m

the amount most business leaders would be willing to pay, which is almost double compared with 2021.



"Many businesses are under pressure to pay and 'keep the lights on' rather than try their hand at negotiating with nefarious cyber-criminal groups.

Given that almost a third of businesses are willing to pay more than $1 million in ransom payments, and pay quickly, the research shows that business leaders are starting to treat the ransomware threat as they would any other business risk."

"Building muscle memory around response and recovery is important, but it is only one part of the process of building overall cyber resilience. Organisations really need to understand the current and evolving threat landscape.

They need to make decisions about their own risk profile and risk appetite, and then use that information to build a program of continuous improvement geared towards building cyber into business-as-usual practices.

Cyber isn't a new agenda item—it is and should be an established component by now."

Are businesses well-prepared?

Businesses are over-confident in their abilities to respond to a ransomware attack, but the reality is that many are still very unprepared.

Almost four in five (78 percent) businesses believe that their organisation is 'well prepared' to respond to a cyber-attack, with half (51 percent) reporting that they are 'very prepared'. However, this is at odds with other details in the research, which found that 13 percent of businesses said it took them two days or longer to inform all relevant stakeholders, whilst three in ten (28 percent) are unsure whether an attack would be reported to all stakeholders. Alarmingly, one in five (20 percent) large businesses with more than 1000+ employees admit that they did not report the attack to all relevant stakeholders.

75%

of all ransomware attacks were due to an original phishing email or credential compromise.

65%

of business leaders say that their business has an incident response plan for a cyber attack.

75%

of businesses believe that it should be mandatory to report a ransomware attack to the authorities.

18%

of businesses are unaware that paying a ransom funds criminal organisations.

Key findings

1. **The timeframe for ransom payments has shortened**
   44 percent of businesses attacked paid a cyber ransom within 24 hours (up from 23 percent in 2021).

2. **Negotiation is also less likely to have taken place**
   Of those business leaders who have paid a cyber ransom, three in five (59 percent) chose to negotiate with cyber criminals to lessen the financial and operational damage to their business, compared to three in four (74 percent) last year.

3. **Residual uncertainty over consequences of ransom payment**
   Close to one in five Australian organisations are unaware that paying a ransom funds criminal organisations.

4. **Email fraud is the most common mode of entry**
   75 percent of all ransomware attacks can be attributed to an original phishing email or credential compromise, while the remaining 25 percent are a result of vulnerabilities exploitation and malicious access.

What this means for your business

Ransomware continues to rise and Australia has become a lucrative target market for cybercriminals. McGrathNicol's annual ransomware survey reveals the extent of these attacks and also the willingness of Australian executives to pay a ransom to prevent further damage to their customers and their brand.

Cyber awareness is a non-negotiable for business executives. Businesses should treat a ransomware threat as they would any other high stakes, significant business risk. Well-prepared businesses are those who invest in cyber resilience plans, build muscle memory around response and recovery to detect early and mitigate risk. These organisations understand their cyber risk profile, and use that information to build cyber consciousness into business-as-usual practices.

An organisation that experiences a ransomware attack does not need to go it alone. Our experts work with clients to proactively manage cyber risk and respond to cyber incidents. View our experts on page 13.

Results

Prevalence of ransomware attacks in the past 5 years

- Overall, seven in ten (69%) respondents surveyed say that their business has experienced a ransomware attack in the past 5 years, a significant increase from 31% in 2021.
- More than half (52%) say that their business has experienced one attack, while one in six (17%) say that their business has experienced multiple attacks. Furthermore, almost half (48%) say that their business was attacked and breached in at least one instance, while more than one in five (22%) say that their business was attacked but not breached in any instance.
- Those in businesses with 250-999 employees are more likely than those in businesses with 50-249 employees or 1,000+ employees to say that their business has experienced a ransomware attack in the past 5 years (84% compared to 68% and 72% respectively).
- Interestingly, those in businesses with 250-999 employees are more likely than those in businesses with 50-249 employees or 1,000+ employees to say that their business has experienced one attack (74% compared to 51% and 58% respectively) or was attacked but not breached in any instance (41% compared to 21% and 13% respectively).
- Those in businesses with 1,000+ employees are more likely than those in businesses with 250-999 employees to say that their business was attacked and breached in at least one instance (59% compared to 44%), while those in businesses with 50-249 employees are more likely than those in businesses 250-999 employees to say that their business has experienced multiple attacks (18% compared to 11%).

Results

Cyber ransom payments

Among respondents in businesses attacked:

- Four in five (79%) decided to pay the cyber ransom (83% in 2021). One in four (25%) paid less than $500,000, more than one in five (22%) paid between $500,000 and $999,999, while three in ten (29%) paid at least $1 million.
- Overall, the estimated average amount of cyber ransom paid among those who can recall the amount was $1.01 million, on par with $1.07 million in 2021. This estimated average is highest among those in businesses with 1,000+ employees* ($1.58 million, compared to those in businesses with 50-249 employees: $1.01 million or 250-999 employees: $0.92 million).

Willingness to pay a ransom

- Seven in ten (69%) respondents say that the business would be willing to pay a cyber ransom if it was subjected to a ransomware attack (down from 80% in 2021), although 7% say that the business would only do so if there was no other choice (down from 12% in 2021).
- One in seven (14%) say that the business would not pay under any circumstance (14% in 2021), while almost one in five (18%) are unsure whether the business would pay, up from 6% in 2021.
- However, it appears that the amount that businesses would be willing to pay has increased notably, with three in ten (30%) saying that the business would be willing to pay $1,000,000 or more, up from 16% in 2021, and one in seven (14%) saying that the business would be willing to pay between $500,000 and $999,999, up from 6% in 2021.
- Overall, the estimated average cyber ransom amount that businesses would be willing to pay among those that would be willing to pay is $1,288,608, almost doubling from $682,123 in 2021.
- Those in businesses with 1,000+ employees are the most likely to say that the business would only pay if there was no other choice (27%), compared to only 7% of those in businesses with 50-249 employees and 9% of those in businesses with 250-999 employees.
- Those in businesses with 50-249 employees are the most likely to say that the business wouldn't pay under any circumstance or be unsure whether the business would pay (14% and 19% respectively), compared to those in businesses with 250-999 employees (6% and 5% respectively) or 1,000+ employees (3% and 6% respectively).
- Unsurprisingly, those in businesses that made a ransom payment are more likely than those in businesses that didn't to be willing to pay (96% compared to 52%).

Results

Drivers of paying a ransom

Among respondents who would pay a ransom:

- Almost seven in ten (68%) cite risk drivers behind their willingness to pay (69% in 2021), which include minimising potential harm to stakeholders (42%, up from 34% in 2021), reducing brand damage (34%, 28% in 2021) and not having sensitive information leaked on the dark web (23%, 27% in 2021).
- Almost two in three (65%) cite operational drivers behind their willingness to pay (up from 54% in 2021), which include getting back to normal operations faster (47%, up from 31% in 2021) and re-establishing control and access to critical infrastructure and systems (40%, 35% in 2021).
- More than two in five (43%) would pay as insurance would cover a large percentage of the payment, up from 34% in 2021.
- Those in businesses with 50-249 employees are the most likely to be willing to pay as insurance would cover a large percentage of the payment (44%), compared to those in businesses with 250-999 employees and 1,000+ employees (34% and 29% respectively).
- Those in businesses with 50-249 employees are more likely than those in businesses with 250-999 employees to cite re-establishing control and access to critical infrastructure and systems (40% compared to 30%), while those in businesses with 250-999 employees are more likely than those in businesses with 1,000+ employees to cite reducing brand damage (40% compared to 23%).

Timeframe and negotiation for ransom payment

- The timeframe for payment appears to have shortened, with negotiation being less likely to have taken place. More than two in five (44%) did so within 24 hours (up from 23% in 2021), one in three (34%) did so within 24 to less than 48 hours (down from 51% in 2021), while one in five (20%) did so in 48 hours or longer (24% in 2021).
- Three in five (59%) negotiated prior to making payment (down from 74% in 2021), while two in five (39%) did not (up from 24% in 2021).
- Those in businesses with 1,000+ employees* are more likely than those in businesses with 50-249 employees or 250-999 employees to have negotiated prior to making payment (79%, compared to 58% and 60% respectively) and to have done so within 24 hours (55%, compared to 22% and 36% respectively).

Results

Mode of entry

Among respondents in businesses attacked and breached:

- The most common mode of entry was email fraud (phishing) (21%), followed closely by malware or spyware (20%). These are followed by text/phone fraud (phishing) (12%), exploitation of a common vulnerability (11%), weak or compromised credentials (11%), and man-in-the- middle-attack (11%).
- Less common modes of entry are exploitation of a zero-day vulnerability (7%) and a malicious insider providing access (7%).
- Those in businesses with 1,000+ employees* are the most likely to have been breached via email fraud (phishing) (37%, compared to those in businesses with 50-249 employees: 21% or 250-999 employees: 20%) or malware or spyware (37%, compared to those in businesses with 50-249 employees: 20% or 250-999 employees: 14%).

Form of ransom demand

- Three in five (61%) say that the cyber criminals demanded the ransom payment in cryptocurrency, including 33% that cite Bitcoin and 28% that cite another cryptocurrency. Almost four in ten (38%) say that the cyber criminals demanded the ransom payment via wire transfer.
- Compared to those in businesses with 250-999 employees or 1,000+ employees*, those in businesses with 50-249 employees are less likely to say that the cyber criminals demanded the ransom payment in cryptocurrency (59%, compared to 78% and 89% respectively) and more likely to say that the cyber criminals demanded the ransom payment via wire transfer (40% compared to 21% and 11% respectively).

Preparedness for cyber attacks

- Almost four in five (78%) respondents believe that their business is prepared in responding to a cyber attack, including half (51%) who believe that their business is very prepared.
- Only 7% believe that their business is unprepared, while 15% are unsure whether their business is prepared.
- Those in larger businesses are more likely than those in small businesses to say that they are prepared (1,000+ employees: 95%, 250-999 employees: 97% respectively, compared to 50-249 employees: 77%).
- Those in businesses with 50-249 employees are the most likely to be unsure whether their business is prepared (16%), compared to only
- 1% among those in businesses with 250-999 employees and 3% among those in businesses with 1,000+ employees.
- Those in businesses with 50-249 employees are also more likely than those in businesses with 250-999 employees to believe that their business is prepared (8% compared to 1%).

Results

Prevalence of incident response plans

- Almost two in three (65%) respondents say that their business has an incident response plan for a cyber attack, 15% say that their business doesn't, while one in five (20%) are unsure whether their business has one.
- Those in larger businesses are more likely than those in small businesses to say that their business has an incident response plan for a cyber attack (1,000+ employees: 80%, 250-999 employees: 74% respectively, compared to 50-249 employees: 64%).
- Those in businesses with 250-999 employees are the most likely to say that their business doesn't have an incident response plan (24%), compared to 15% among those in businesses with 50-249 employees and 6% among those in businesses with 1,000+ employees.
- Those in businesses with 250-999 employees are the least likely to be unsure whether their business has an incident response plan (2%), compared to 21% among those in businesses with 50-249 employees and 14% among those in businesses with 1,000+ employees.

Length of attack assessments

- One in five (21%) say that it took the business up to 6 hours to assess all required information about the attack and accurately report it to relevant stakeholders, one in four (25%) say that it took the business 7 to 12 hours, while almost two in five (38%) say that it took the business 13 to 24 hours. Some 13% say that it took the business 2 days or longer to do so.
- Those in businesses with 50-249 employees are the most likely to say that this process was completed within a day (84%), compared to 72% among those in businesses with 250-999 employees and 70% among those in businesses with 1,000+ employees*. Those in businesses with 250-999 employees are the most likely to say that this process was completed in 4 to 7 days (18%), compared to 4% among those in businesses with 50-249 employees and 2% among those in businesses with 1,000+ employees*.
- Alarmingly, one in five (20%) of those in businesses with 1,000+ employees* admit that the attack wasn't reported to relevant stakeholders, compared to only 1% of those in businesses with 50-249 employees or 250-999 employees.
- On average, the estimated time taken to assess all required information about the attack and accurately report it to relevant stakeholders among those who can recall the time taken was 20.8 hours.
- This figure is highest among those in businesses with 250-999 employees (35.5 hours), compared to 19.8 hours among those in businesses with 50-249 employees and 15.6 hours among those in businesses with 1,000+ employees*. This figure is also almost twice as high in businesses that made the ransom payment as in businesses that didn't (22.8 compared to 12.4).

Results

Notifying the board of directors

- Four in five (80%) respondents say that the board of directors would be notified in case their business was subjected to a ransomware attack, including seven in ten (71%) who say that there is a notification protocol in place and one in ten (9%) who say that there is another method in place.
- Only 4% say that the board of directors wouldn't be notified, while one in six (16%) are unsure whether the board of directors would be notified.
- Those in larger businesses are more likely than those in small businesses to say that the board of directors would be notified (1,000+ employees: 94%, 250-999 employees: 96% respectively, compared to 50-249 employees: 79%).
- Those in businesses with 50-249 employees are the most likely to be unsure whether the board of directors would be notified (17%), compared to only 2% among those in businesses with 250-999 employees and 5% among those in businesses with 1,000+ employees.

Insured against ransomware

- Nine in ten (91%) respondents say that their business is currently insured against a ransomware attack, up from 84% in 2021.
- Two in five (39%) say that the insurance cover amount is less than $1 million (up from 30% in 2021), one in five (20%) say that the cover amount is between $1 million and $1,999,999 (19% in 2021), while 11% say that the cover amount is $2 million or more (down from 20% in 2021). One in five (20%) are insured but unsure of the cover amount (15% in 2021).
- Overall, the estimated average insurance cover amount among those who are insured and can recall the amount is $1.31 million ($1.87 million in 2021).
- Interestingly, those in businesses with 50-249 employees are more likely than those in businesses with 1,000+ employees to say that their business is currently insured (91% compared to 81%), although the estimated average cover amount is higher in businesses in the latter group than in businesses in the former group ($1.83 million compared to $1.32 million).

Insured or re-insured against future attacks

- More than four in five (83%) say that their business was able to get insured or re-insured against future attacks after the attack. Only 11% say that their business wasn't able to get insured or re-insured, while 6% say that their business didn't seek to get insured or re-insured.
- Those in businesses with 1,000+ employees are the most likely to say that their business was able to get insured or re-insured (100%), compared to 84% among those in businesses with 50-249 employees and 73% among those in businesses with 250-999 employees.
- Those in businesses with 250-999 employees are more likely than those in businesses with 50-249 employees to say that their business wasn't able to get insured or re-insured (26% compared to 10%)
- Those in businesses that made the ransom payment are more likely than those in businesses that didn't to say that their business was able to get insured or re-insured (87% compared to 70%). One in four (24%) of those in businesses that didn't make the ransom payment say that their business didn't seek to get insured or re-insured.

Results

Perceived value of insurance policy

Among respondents in businesses insured:

- Almost nine in ten (87%) believe that the insurance policy is good value. Only 7% believe otherwise, while only 5% are unsure whether it is good value.
- Those in businesses with 250-999 employees are the most likely to believe that the insurance policy is good value (96%), compared to those in businesses with 50-249 employees (87%) or 1,000+ employees (87%).

Reasons for policy being good value

- The most common reasons for the perception of good value are that the insurer helps in accessing advice and support that will better protect the business (55%), that the protection provides peace of mind (54%) and that the insurer has helped/will help in responding to a ransomware attack (52%). Two in five (39%) also believe that the payout has helped/will help protect the business.
- Those in businesses with 50-249 employees are more likely than those in 250-999 employees to cite that the insurer helps in accessing advice and support that will better protect the business (56% compared to 40%).
- Those in businesses with 50-249 employees and 1,000+ employees* are more likely than those in 250-999 employees to cite that the insurer has helped/will help in responding to a ransomware attack (53% and 56% respectively, compared to 39%).

Reasons for policy being poor value

Among the minority of respondents in businesses insured and don't believe that or are unsure whether the policy is good value:

- The most common reason for this view is that the policy has too many stipulations attached and that they don't feel confident the insurer will accept a claim (59%).
- This is followed by the premiums being too high (31%), the policy not providing adequate financial protection (28%) and the insurer not providing adequate advice and support that will better protect the business (21%).

Results

Awareness and attitude to paying a ransom

- More than four in five (82%) respondents claim to be aware that paying a ransom finances criminal organisations (up from 66% in 2021), with three in five (59%) also saying that it is a key factor in their decision of to pay or not to pay, up from 36% in 2021, and one in four (24%) saying that it is not (down from 30% in 2021).
- Only one in five (18%) are unaware that paying a ransom finances criminal organisations (down from 34% in 2021), with 7% saying that it is now a key factor in their decision of to pay or not to pay and 11% saying that it is not (down from 17% and 16% respectively 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 almost two in three (65%) respondents, up from 54% in 2021.
- Interestingly, compared to those in businesses that didn't make a ransom payment, those in businesses that did are more likely to be unaware of the consequences and say that it is not a key factor in the decision-making (16% compared to 2%) and less likely to be unaware of the consequences and say that it is now a key factor in the decision-making (3% compared to 23%).
- Compared to those in businesses with 50-249 employees or 1,000+ employees, those in businesses with 250-999 employees are more likely to be aware of the consequences and say that it is not a key factor in the decision-making (40% compared to 23% and 22% respectively) and less likely to be aware of the consequences and say that it is a key factor in the decision-making (41% compared to 60% and 59% respectively).

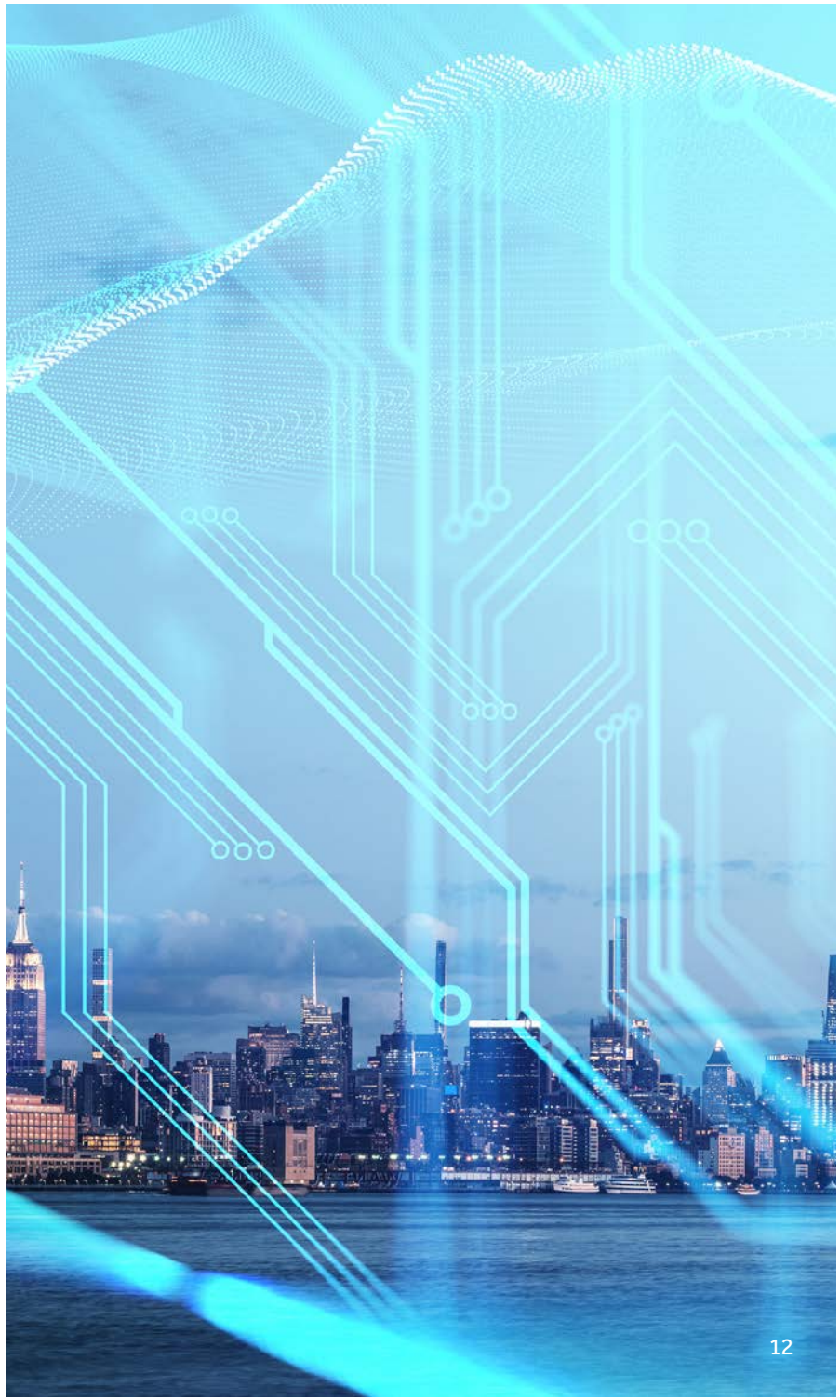
Reporting ransomware attacks to authorities

- Three in four (75%) respondents believe that it should be mandatory for a business to report a ransomware attack to the authorities (up from 67% in 2021), with almost three in five (56%) believing that it should be reported regardless of whether a payment is made (up from 43% in 2021) and more than two in five (45%) believing that it should be reported only when a payment is made (up from 24% in 2021).
- More than half (52%) believe a cyber incident or data breach of any kind should be reported to the authorities (54% in 2021).
- Those in businesses that made a ransom payment are more likely than those in businesses that didn't to believe that a ransomware attack should be reported only when a payment is made (51% compared to 33%).
- Those in businesses with 50-249 employees are more likely than those in businesses with 1,000+ employees to believe that a ransomware attack should be reported regardless of whether a payment is made (57% compared to 41%).

Results

Cyber attacks since start of Russia-Ukraine conflict

- More than three in four (77%) respondents say that they have seen more or about the same number of cyber attacks or attempted attacks on their business since the start of the Russia-Ukraine conflict. Half (49%) say that they have seen more, including around one in four each who have seen a lot more or a little more (26% and 23% respectively).
- Only 6% say that they have seen fewer cyber attacks or attempted attacks, while almost one in five (18%) are unsure whether there has been more, about the same or fewer cyber attacks or attempted attacks.
- Those in larger businesses are more likely than those in small businesses to say that they have seen more cyber attacks or attempted attacks (1,000+ employees: 72%, 250-999 employees: 63% respectively, compared to 50-249 employees: 47%).
- Interestingly, those in businesses with 1,000+ employees are almost three times as likely as those in businesses with 50-249 employees to say that they have seen fewer cyber attacks or attempted attacks (14% compared to 5%).
- Those in businesses with 50-249 employees are the most likely to be unsure whether there has been more, about the same or fewer cyber attacks or attempted attacks (19%), compared to only 3% among those in businesses with 250-999 employees and 6% among those in businesses with 1,000+ employees.
- Those in businesses that made a ransom payment are nearly four times as likely as those in businesses that didn't to say that they have seen a lot more cyber attacks or attempted attacks (42% compared to 11%).



Meet the Partners

Darren Hopkins
Partner, Brisbane
M +61 416 151 419
E dhopkins

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.

Joss Howard
Partner, Sydney
M +61 460 972 700
E jhoward

Joss specialises in technical, information security and cyber resilience. She advises global businesses across sectors including aerospace, defence, finance, government, healthcare, leisure and retail, transport, telecommunication and utilities.

Jamie Norton
Partner, Canberra
M +61 438 643 170
E jnorton

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

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.

Trent Whitbourn
Partner, Sydney
M +61 407 578 086
E twhitbourn

Trent is a forensic and technology specialist in digital forensics, cyber security and information risk, end-to-end electronic discovery and data analytics. He has worked across different jurisdictions, Government projects and local and US regulators.

This study was conducted online between 9 September and 21 September 2022 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 516 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.