Over the past 12 months

When faced with a ransomware attack, 62% of companies paid the ransom, yet 30% of them failed to recover their data.

3 out of 4 companies received an increased number of email-based threats.

Australia saw a higher than average increase across all email-related attacks:

- 59% - misuse of their brand via spoofed email
- 58% - email-related phishing
- 50% - business email compromise
- Half - internal threats or data leaks
- 51% - spoofed web domains/sites

To counter brand spoofing, 90% of companies are making use of DMARC or plan to do so over the next 12 months.

77% of companies were hurt by a ransomware attack, up from 64% in 2020.

49% of respondents said the main benefits of implementing AI and ML include:

- Improved accuracy in detecting threats
- Reduced costs associated with cybersecurity
- Increased productivity

Yet 1 in 10 have no plans to use it.

Respondents said the main barriers to implementing AI and ML include:

- Lack of data
- Cost of implementation
- Talent and skills shortage

Among Microsoft 365 email users, 80% experienced an outage during the past year and 51% were severely impacted.

Only 23% of companies provide cyber awareness training to their employees or an ongoing test, but 85% of employees were at least aware of a threat.

99% of companies either have a cyber incident response plan or are currently working on one.

The goal posts for true cyber resilience have moved with only 34% saying they currently have a strategy in place, compared to 51% in 2021.

With more than 1 in 10 saying it’s inevitable and 4 in 10 saying it’s extremely likely.

More than 8 out of 10 respondents believe this company is at risk due to a lack of protection or data leaks by careless or negligent employees.

89% of companies say being the target of a ransomware attack is extremely likely.

Australians are more concerned about their email security challenges compared to other regions:

- 57% - email spoofing
- 47% - unauthorised access
- 46% - data loss or data theft
- 45% - unsolicited email or spam

Australians and 11% felt threatened.

90% of companies said their cyber resilience has been impaired by insufficient funding.

89% of companies are either using or plan to use a third-party protection service this year.

On average, 14% of IT budgets are allocated for cyber resilience.

Australians said 18% should be allocated.

Among Microsoft 365 email users, 80% experienced an outage during the past year and 33% were severely impacted.

98% of companies either have a cyber incident response plan or are currently working on one.

Australians are more concerned about various email security challenges, compared to most other countries:

- More than 8 out of 10 respondents believe their company is at risk due to a lack of protection or data leaks by careless or negligent employees.

More than 8 out of 10 respondents believe this company is at risk due to a lack of protection or data leaks by careless or negligent employees.