Over the past 12 months

When faced with a ransomware attack, 71% of companies paid the ransom, and 32% of those who paid failed to recover their data.

KEY FINDINGS IN SINGAPORE

45% said it was extremely likely.

84% are bracing for the fallout from an email-borne attack.

ALL respondents either have a system to monitor and protect against email-borne threats or are actively planning to roll one out.

Among Microsoft 365 security email users, 84% experienced an outage during the past year, 35% were severely impacted.

Organisations were affected by a lack of cyber resilience preparedness:

43% reputation

40% data loss

33% financial loss

32% reputation damage

39% data loss

40% financial loss

83% of companies were hurt by a ransomware attack.

Only 32% of companies currently have a cyber resilience strategy, but this number jumps to 57% when including those who are actively planning to put one in place.

97% of companies are receiving an increased number of email-based threats – the largest globally.

95% of respondents say their cyber resilience has been impaired by insufficient funding:

68% - missing out on improvements to existing cybersecurity solutions

63% - missing out on new technology innovations

93% feel that additional safeguards are needed for Microsoft 365.

97% of companies currently have a cyber resilience strategy, but this number jumps to 95% when including those who are actively planning to put one in place.

84% of companies are receiving an increased number of email-based threats – the largest globally.

82% offer it at least once a quarter.

When faced with a ransomware attack, 71% of companies paid the ransom, and 32% of those who paid failed to recover their data.

Singapore is the most concerned about employees making serious security mistakes in the following activities:

• Oversharing company information on social media - 89%

• Poor password hygiene - 89%

• Using cloud storage and other shadow IT - 89%

• Using personal email - 88%

• Inadvertent data leaks - 88%

• Browsing the web and online shopping - 86%

• Using collaboration tools - 81%

Only 32% of companies currently have a cyber resilience strategy, but this number jumps to 57% when including those who are actively planning to put one in place.

Singapore is the most concerned about employees making serious security mistakes in the following activities:

• Oversharing company information on social media - 89%

• Poor password hygiene - 89%

• Using cloud storage and other shadow IT - 89%

• Using personal email - 88%

• Inadvertent data leaks - 88%

• Browsing the web and online shopping - 86%

• Using collaboration tools - 81%

This is very likely because only 7% of companies provide least awareness training to employees as an ongoing action.

But reassuringly, 82% offer it at least once a quarter.

95% of respondents say their cyber resilience has been impaired by insufficient funding:

68% - missing out on improvements to existing cybersecurity solutions

63% - missing out on new technology innovations

93% feel that additional safeguards are needed for Microsoft 365.

97% of companies currently have a cyber resilience strategy, but this number jumps to 95% when including those who are actively planning to put one in place.

84% of companies are receiving an increased number of email-based threats – the largest globally.

82% offer it at least once a quarter.