Yet they don't appear to be concerned about email security challenges – perhaps indicating they are taking security more seriously than their global counterparts:

- Only 38% are concerned about increasingly sophisticated attacks
- 32% are concerned about insufficient security budget
- And as little as 14% are concerned about insufficient security staff
- 1 in 10 say they won't face any email security challenges

Over the past 12 months 6 in 10 companies are receiving an increased number of email-based threats. Interestingly 1 in 5 actually saw a decrease.

KEY FINDINGS IN SAUDI ARABIA

- 40% phishing attacks
- 38% internal threats or data leaks initiated by malicious insiders
- 34% business email compromise
- 30% spoofed email

92% of companies are the target of an email-related phishing attempt.

90% of companies have been the target of a ransomware attack but the kingdom is setting an example with the average downtime being only 5 days and 17% of respondents said they didn’t experience any.

94% of companies either have a cyber resilience strategy or are actively planning to roll one out.

68% experienced a Microsoft 365 outage during the past year.

99% of companies either have a system to monitor and protect against email-borne threats or are actively planning to roll one out.

This might be because respondents only experienced an average of 6 of 6 online brand spoofing attacks in the last year with a quarter saying they never experienced any.

Respondents said the main benefits of implementing AI and ML include:

- 98% feel that additional safeguards are needed for Microsoft 365
- 52% strongly agree.

Encouragingly, 44% of companies provide cyber awareness training to their employees on an ongoing basis, well above the global average of 23%

60% of respondents say their cyber resilience has been impaired by insufficient funding, with 54% citing missing out on new technology innovations as the biggest setback.

89% of companies are using or plan to use a brand protection service. But 1 in 10 either had no plans to implement one, only had plans beyond 12 months or didn’t know.

44% of companies were hit by a ransomware attack but the kingdom is setting an example with the average downtime being only 5 days and 17% of respondents said they didn’t experience any.

42% of respondents believe improvements are needed in all areas in their employee email security.

This regular training appears to be translating into some positive behaviours:

- Only 66% were concerned about personal email with 16% saying there is no risk at all
- 60% were concerned about employees oversharing company information on social media
- 62% were concerned about the use of collaboration tools

Respondents said the main benefits of implementing AI and ML include:

- Improvements in level of overall cybersecurity in their businesses - 38%
- Decrease in risk of cyberattacks impacting their business - 36%
- Core IT business leaders view it in relation to improving cybersecurity - 36%
- Decrease in feedback to determine the best course of action - 32%

94% of respondents say their cyber resilience has been impaired by insufficient funding, with 54% citing missing out on new technology innovations as the biggest setback.

This regular training appears to be translating into some positive behaviours:

- Only 66% were concerned about personal email with 16% saying there is no risk at all
- 60% were concerned about employees oversharing company information on social media
- 62% were concerned about the use of collaboration tools

Respondents said the main benefits of implementing AI and ML include: