

2023

Key SOES findings

in UAE over the last 12 months

Email

Email usage continues to rise at **9 of 10** companies



3 out of 4 have experienced an increase in email-based threats

Collaboration Tools



4 out of 5 say collaboration tools are posing significant new security risks

Cyber Awareness

64% believe their company is at risk due to inadvertent data leaks by careless or negligent employees.

100% of companies provide some form of cyber awareness training to their workforce

1 out of 3 train their staff on an ongoing basis – the highest globally

Cyber Defences

100% either have a system to monitor and protect against email-borne threats or are actively planning to roll one out

94% think they need stronger protections than those that come with their MS 365 and Google Workspace applications

ALL are using DMARC or plan to use it to thwart email spoofing and encouragingly **40%** have already deployed it

Cyberattacks

70% say cyberattacks are growing increasingly sophisticated - the second highest globally

2 out of 3 companies were harmed by a ransomware attack

Budget

60% of respondents say their companies need to spend more on cybersecurity, but only by **5%** more

Cyber Insurance

Encouragingly **66%** would not see cyber insurance as a substitute for developing a comprehensive cyber preparedness program

AI and Machine Learning

ALL respondents are either using or plan to use AI and machine learning to bolster their cybersecurity.

The biggest benefit of AI was reduced human error across the company (e.g. as a result of contextual email warning banners) **54%**

