mimecast

2023 Key SOES findings

in Singapore over the last 12 months

Email

Email usage continues to rise at **84%** of companies

78% have experienced an increase in email-based threats

Collaboration Tools

●●○

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

72% expect to be harmed in 2023 by a collaboration-tool-based attack.

Cyber Awareness

●●●●●
●●●●○

9 out of 10 believe their company is at risk due to inadvertent data leaks by careless or negligent employees

Respondents were also concerned about employees making serious security mistakes in the following activities:

81% using cloud storage and other shadow IT

81% poor password hygiene

70% using collaboration tools

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

100

Cyber Defences

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

99

98% think they need stronger protections than those that come with their MS 365 and Google Workspace applications

98

Cyberattacks

61% say cyberattacks are growing increasingly sophisticated

63% were harmed by a ransomware attack

99

Nearly all (99%) have been targeted by email-based phishing attacks

Budget

67% say their companies need to spend more on cybersecurity

Cyber Insurance

Respondents are divided on the value of cyber insurance policies

46% see them as worthwhile additions

54% don't see it as a comprehensive safety net

AI and Machine Learning

97% are either using or plan to use AI and machine learning to bolster their cybersecurity

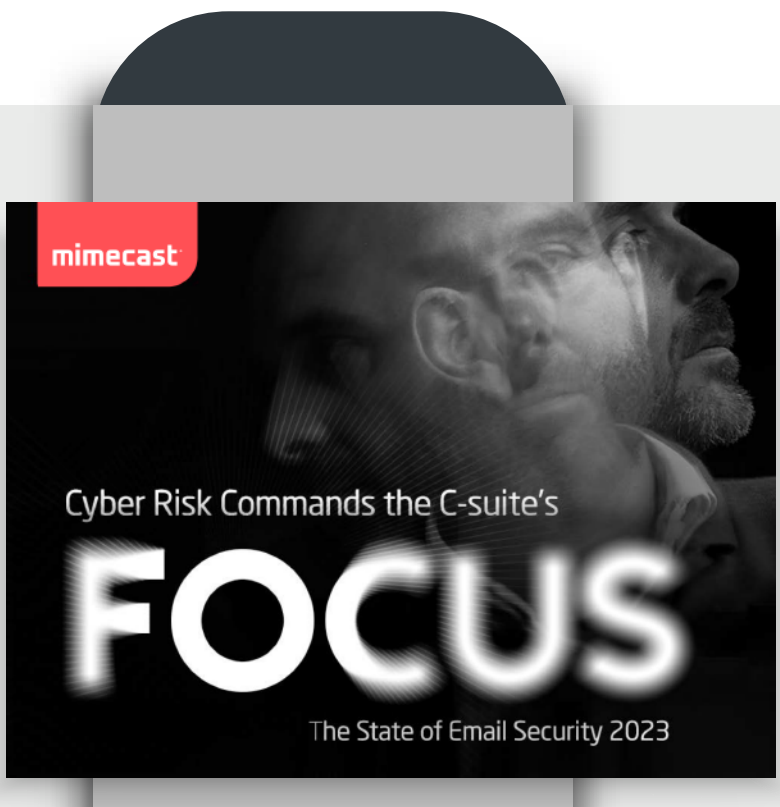
the three main benefits are:

55% improved ability to block threats

54% faster remediation when an attack has occurred

48% reduced workload for the cybersecurity team

93% agree that AI systems that provide real-time, contextual warnings to email and collaboration tool users would be a huge boon



The State of Email Security Report 2023

READ IT NOW