

# Confronting the NEW WAVE OF CYBERATTACKS

The State of Email Security 2022

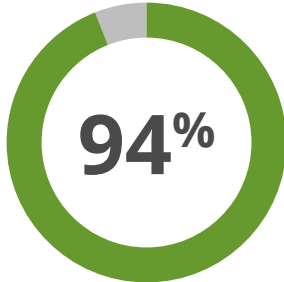
## KEY FINDINGS IN SAUDI ARABIA

Over the past 12 months

**92%** of companies are bracing for the fallout from an email-borne attack. With **14%** even saying it's inevitable.

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

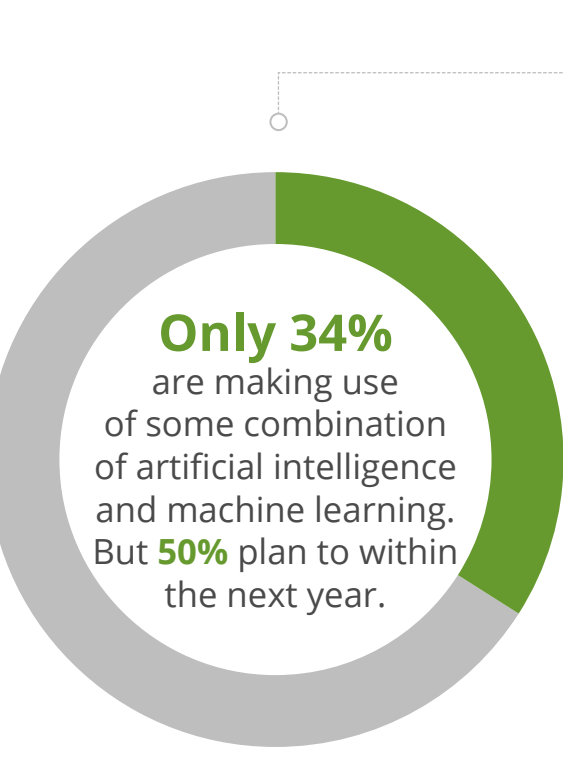
- Only **38%** are concerned about increasingly sophisticated attacks
- **32%** are concerned about insufficient security budget
- And as little as **14%** are concerned about insufficient security staff
- **1 in 10** say they won't face any email security challenges



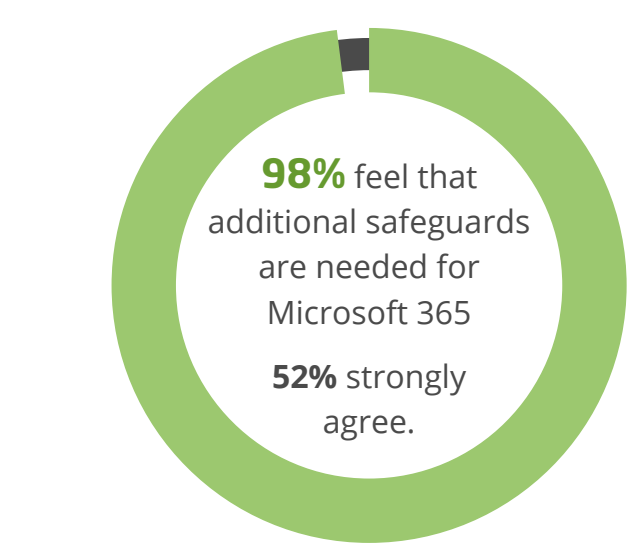
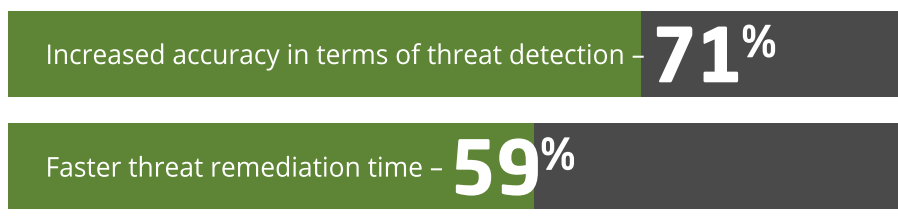
of companies either have a cyber resilience strategy or are actively planning to put one in place.

KSA respondents expect **high** levels of changes in their organisation from government mandates for cyber resilience:

- Improvements in level of overall cybersecurity in their business - **38%**
- Decrease in risk of cyberattacks impacting their business - **36%**
- Care that business leaders show in relation to improving cybersecurity - **36%**
- Decrease in freedom to determine own best course of action - **32%**



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



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

**92%** of companies are either 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.

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

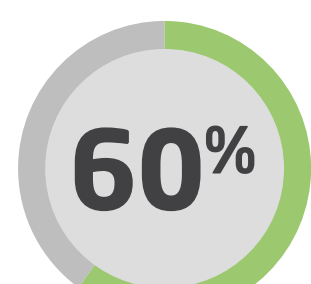
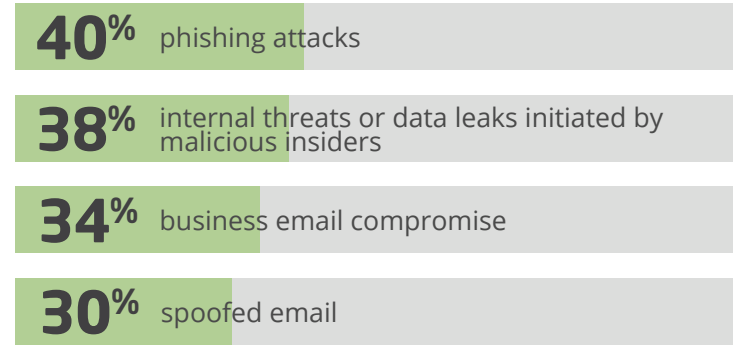
**6 in 10** companies are receiving an increased number of email-based threats. Interestingly **1 in 5** actually saw a decrease.

Email usage rose at more than **8 out of 10** companies, with **46%** saying it was significant.

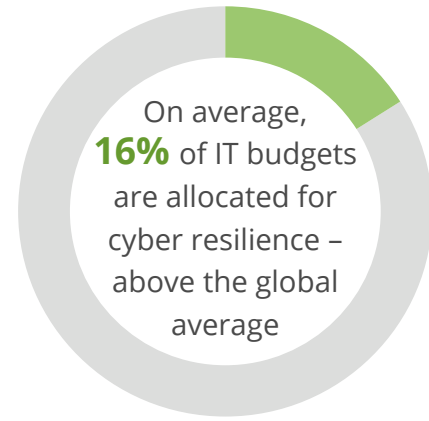
**90%**

of companies have been the target of an email-related phishing attempt.

But interestingly saw a **decrease** in several email-related attacks:



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 say they didn't experience any.

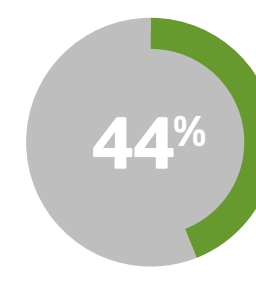


But respondents believe **19%** should be allocated.



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.

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



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

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

- **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

**42%** were only somewhat prepared or not prepared at all to deal with attacks that spoof their email domains.



# Confronting the NEW WAVE OF CYBERATTACKS

The State of Email Security 2022

GET THE REPORT

