mimecast

Confronting the NEW WAVE OF CYBERATTACKS

The State of Email Security 2022

KEY FINDINGS IN AUSTRALIA

Over the past 12 months

3 out of 4 companies received an increased number of email-based threats.

Email usage rose at **8** out of **10** companies

89% of companies are bracing for the fallout from an email-borne attack.

With more than **1 in 10** saying it's inevitable and **4 in 10** saying it's extremely likely.

More than 8 out of 10 respondents believe their company is at risk due to inadvertent data leaks by careless or negligent employees.

Australians are more concerned about various email security challenges, compared to most other countries:

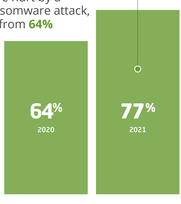
- **57%** increasingly sophisticated attacks – the highest of any country
- **47%** security naive employees
- **46%** insufficient staff – again by far the most concerned country globally
- **45%** weak email protections

Australia saw a higher than average INCREASE across all email-related attacks:

- **59%** - misuse of their brand via spoofed email
- **58%** - email-related phishing
- **50%** - business email compromise
- **Half** - internal threats or data leaks
- **51%** - spoofed web domains/sites

98% of companies have been the target of an email-related phishing attempt.

77% of companies were hurt by a ransomware attack, up from **64%**



When faced with a ransomware attack, **62%** of companies paid the ransom, yet **30%** of them failed to recover their data.

49% are making use of some combination of artificial intelligence and machine learning. Yet **1 in 10** have no plans to use it.

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

- **65%** Increased accuracy in terms of threat detection
- **65%** Reduced human error within cybersecurity team
- **57%** Threat prevention

On average, **14%** of IT budgets are allocated for cyber resilience.

Australians said 18% should be allocated.

93% of respondents say their cyber resilience has been impaired by insufficient funding:

52% - lack of investment in cybersecurity training for existing staff

51% - missing out on improvements to existing cybersecurity solutions

Among Microsoft 365 email users, 80% experienced an outage during the past year and 33% were severely impacted.

95% of companies either have a cyber resilience strategy or are actively planning to put one in place.

Only 23% of companies provide cyber awareness training to their employees on an ongoing basis, but 85% offer it at least once a quarter.

The goal posts for true cyber resilience have moved with only 34% saying they currently have a strategy in place, compared to 51% in 2021.

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

100% of companies are either using or plan to use a brand protection service this year.

To counter brand spoofing, **90%** of companies are making use of DMARC or plan to do so over the next 12 months.

Confronting the NEW WAVE OF CYBERATTACKS

The State of Email Security 2022

GET THE REPORT