mimecast

Confronting the NEW WAVE OF CYBERATTACKS

The State of Email Security 2022

KEY FINDINGS IN SOUTH AFRICA

Over the past 12 months

67% are bracing for the fallout from an email-borne attack

More than **3 out of 4** companies are receiving an increased number of email-based threats.

Email usage rose at **9** out of **10** companies, with **45%** saying it was significant.

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

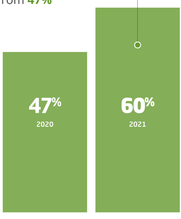
- **55%** increasingly sophisticated attacks
- **45%** weak email protections
- **41%** insufficient security budget

94% of companies have been the target of an email-related phishing attempt and **65%** experienced an increase.

89% of companies either have a cyber resilience strategy or are actively planning to put one in place.

But the goal posts for true cyber resilience have moved with only **33%** saying they currently have a strategy in place, compared to **41%** in 2021.

60% of companies were hurt by a ransomware attack, up from **47%**



South Africans experienced an average of nearly 11 days of downtime due to ransomware attacks.

1 in 10 suffered downtime for longer than 3 weeks.

South African organisations were affected by a lack of cyber resilience preparedness:

- **49%** - business disruption
- **48%** - data loss
- **42%** - impact to employee productivity
- **39%** - impacts to regulatory compliance

Interestingly, when faced with a ransomware attack, only **35%** of South African respondents paid the ransom, yet **43%** of those who paid failed to recover their data.

On average, **12%** of IT budgets are allocated for cyber resilience.

Whereas respondents believed **21%** should be allocated.

For **53%** of organisations, the budget was less than **10%**

97% of respondents say their cyber resilience has been impaired by insufficient funding:

62% - lack of investment in cybersecurity training for existing staff

59% - missing out on new technology innovations

Of all the countries surveyed, South African respondents expect the greatest change from government mandates for cyber resilience. They cited high levels of change in:

- Improvements in level of overall cybersecurity in their business - **46%**
- Care that business leaders show in relation to improving cybersecurity - **42%**
- Decrease in risk of cyberattacks impacting their business - **36%**
- Increase in financial cost to their business - **35%**
- Decrease in freedom to determine own best course of action - **30%**

93% feel that additional safeguards are needed for Microsoft 365.

54% strongly agree.

58% of companies have a system to monitor and protect against email-borne threats in internal-to-internal emails. This jumps to **97%** when including those actively planning to roll one out.

32%

Encouragingly, **32%** of companies provide cyber awareness training to their employees on an ongoing basis, but **1 in 5** only train once a year or less often.

Among Microsoft 365 security email users, 64% experienced an outage during the past year.

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

To counter brand spoofing, **86%** of companies are making use of DMARC or plan to do so over the next 12 months.

- **40%** were somewhat prepared or not prepared at all to detect and mitigate fraudulent web domains or website spoofing – the least confident of all countries.
- **62%** cited lack of technology as the reason for their lack of preparedness
- **98%** of companies are either using or plan to use a brand protection service this year

Confronting the NEW WAVE OF CYBERATTACKS

The State of Email Security 2022

GET THE REPORT