mimecast

Middle East Findings

The State of Email Security 2020

Key findings over the previous 12 months

67% have been impacted by ransomware in the past 12 months

74% believe weak passwords pose a risk of a serious security mistake

53% saw phishing attacks increase

48% say they experienced data loss due to lack of cyber resilience preparedness

56% experienced an increase in impersonation fraud in the last year

79% have experienced downtime from an attack

31% do not provide awareness training on a frequent basis

68% believe their organisation's volume of web or email spoofing will remain the same or increase in the coming year

79% of respondents' organisations were hit by an attack spread from an infected user to other employees

Email attacks, and why they aren't decreasing

67% of organisations believe it's inevitable or likely they will suffer from an email-borne attack in the coming year

62% of respondents had seen impersonation fraud increase or stay the same

62% of respondents stated phishing remained flat or increased

67% of businesses were impacted by ransomware. **They faced 2 days of downtime**.

Of the organisations who fell victim to an email-born attack:

48% experienced data loss

31% had impact to employee productivity

25% saw business interruption/downtime

On average

6/10

organisations have a security system to protect internal and outbound emails:

43% don't yet monitor and protect against email-borne attacks or data leaks in internal emails.

32% don't yet monitor and protect against email-borne attacks like malware and malicious links in outbound email.

36% don't yet monitor and protect against data leaks or exfiltration in outbound email.

35% don't yet have automated detection and removal of malicious or unwanted emails that have already landed in employees' inboxes.

How Security Awareness Training closes the understanding gap

74% believe poor password hygiene poses a risk

71% say inadvertent data leaks are a high risk

79% were hit by malicious activity spread from employee to employee

37% offer training monthly

9% are only trained once per year

100% offer some training at varying frequencies and formats:

- **68%** group training sessions
- **50%** emailed or printed tips
- **49%** online tests
- **60%** 1:1 training

38% of training was developed in-house. Just 18% use training videos. Only 17% use a single third-party provider.

The new mandate: online brand protection

53% anticipate an increase in web or email spoofing and brand exploitation

7 the average number of web or email spoofing attacks organisations were made aware of

- **74%** concerned about a web domain, brand exploitation, or site spoofing attack
- **76%** concerned about an attack that directly spoofs their email domain

99% of respondents were aware of DMARC

37% already use DMARC

99% have a dedicated budget for online brand protection strategies

Who holds the Budget? **47%** CIO **41%** CISO **41%** CFO **14%** CMO **12%** LEGAL / COMPLAINCE

* It's much more likely for CFOs to hold the budget in ME than many other regions surveyed

Is cyber resilience improving?

82% of respondents either have a cyber resilience strategy or actively rolling one out

18% still only planning to implement a cyber resilience strategy

96% use Office 365 as their email provider

Only about **40%** strongly agree Office 365 provides world-class security

73% experienced an Office 365 outage in the last 12 months

78% already added or are currently adding additional layers of continuity and cyber resilience

A lack of cyber resilience preparedness is leading to:

- **48%** Data loss
- **31%** Negative impact to employee productivity
- **25%** Business downtime

What's included in their cyber resilience strategies?

- **72%** Email security
- **63%** Network security
- **68%** Web security
- **69%** Data backup/recovery

2/5 included penetration testing for key systems and regularly testing incident response processes

1/2 included brand exploitation protection for email-spoofing and website-domain spoofing

Download the full report

Get it now

mimecast.com/state-of-email-security

mimecast