intelligent inbox

You've got mail

The rise of email threats

EMAIL SECURITY SURVEY

Contents

An increase in threats	4
Identifying attacks	6
Employee education	8
Shifting attitudes	11

Introduction

This Summer, Intelligent Inbox sought industry wide insight on the current state of email security. Exploring the extent to which organisations are communicating and implementing best practices across workplaces.

This report includes a collation of views from high-level decision makers across industries, from system administrators through to CTOs and CISOs. Together, they share thoughts around key challenges impacting businesses where cybersecurity and email threats are concerned.

Perusing almost 300 responses, it is apparent there is an increased concern regarding the rise in email threats. This combined with a lack of employee education highlights how the susceptibility to threats is unmatched by efficient training. Cyberattacks are leveraging organizational changes such as migration to the cloud, contributing to the severity and frequency of attacks.

Key Findings

Exploring findings from our survey, our report evaluates the evolution of email threats, identifying common concerns surrounding email security or lack thereof.

87%

foresee an increase in email security threats over the next 12 months

PHISHING

methods are the most common type of email threat

EMPLOYEE EDUCATION

is key - building resilience to threats begins with adequate training.

An increase in threats

01 How do you see the number of email security threats evolving over the next 12 months?

When we asked this question, 87% opted for 'increase' and 'strong increase'. As email is the most popular form of communication among businesses and consumers, this revelation comes as no surprise. It's forecasted that in the next three years, the number of business and consumer emails sent per day will rise to 333 billion.

02 How much do you agree with the following?

"Email is where organisations are most vulnerable to cyber attacks"

Email-borne attacks are prevalent and a key concern for many organisations. Email remains the most popular infection vector for organisations and cyberattacks continue to exploit this.

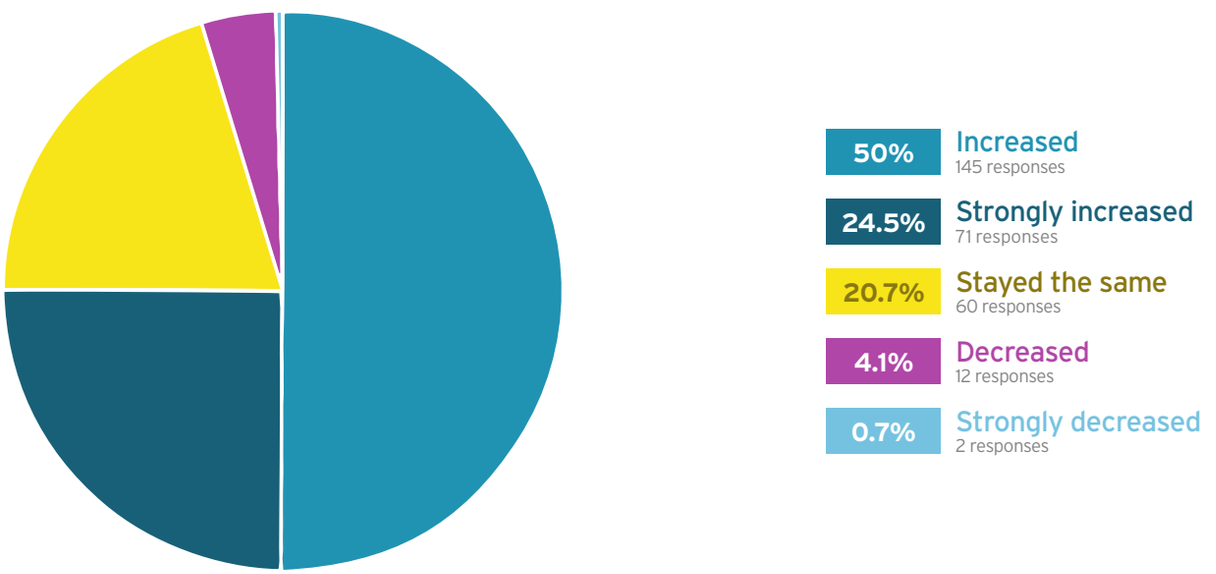
"91% of cyberattacks begin with email" **Cyber Defense Magazine**

Malicious programs continue to bypass advanced enterprise anti-virus and most email protection solutions without being detected.

03 Over the past 3 years, how has the volume of email attacks, or threats to your organisation changed?

In a recent PSA, the FBI voiced concerns surrounding the rise of reported complaints involving Business Email Compromise (BEC) and Email Account Compromise (EAC) threats. Cyberattacks targeting organisations and individuals continue to increase, reportedly costing organisations a loss reaching $12B. This does not seem to be slowing down, as confirmed by 75% of respondents, who note an increased volume of attacks within the past three years.

Throughout 2020 email will remain the primary method of advanced cyberattacks on organisations. Email threats are most successful when sent as attachments and PDF formats, appearing to be legitimate. Organisations should prioritise safeguarding communication channels and ensure gateway security protect against such malicious attachments and URLs.



Identifying attacks

Building resilience against threats aligns with increasing awareness. Encouraging comprehensive reporting methods can be a starting point. Organisations should ensure employees are aware of how to identify malicious threats despite their legitimate appearance.

04 What types of email threats have been attempted on your company over the past 12 months?

Phishing

Phishing attacks appear to be the most prominent of cyberattacks with 75% percent of respondents experiencing these email threats within the past 12 months. Email security techniques apply blacklists and reputation analysis to sift through potential threats. Using brand impersonation, cybercriminals continue to bypass email security often appearing as reputable senders.

05 Which departments in your organisation have experienced the most attacks?

Departmental threats

It comes as no surprise that 57% of finance departments have experienced the most attacks. Their high-level access to valuable information and sensitive data with monetary value makes them vulnerable and attractive. Role-specific email security solution training should be effected in departments with a higher susceptibility to threats combating the frequency of attacks these departments experience.

56.9%	Finance 165 responses	40.3%	CEO office 117 responses	32.4%	Customer support 94 responses
31%	IT 90 responses	27.2%	HR 79 response	16.6%	Other 48 response

Employee Education

06 How often do your staff receive cyber security training (eg how to spot phishing emails)?

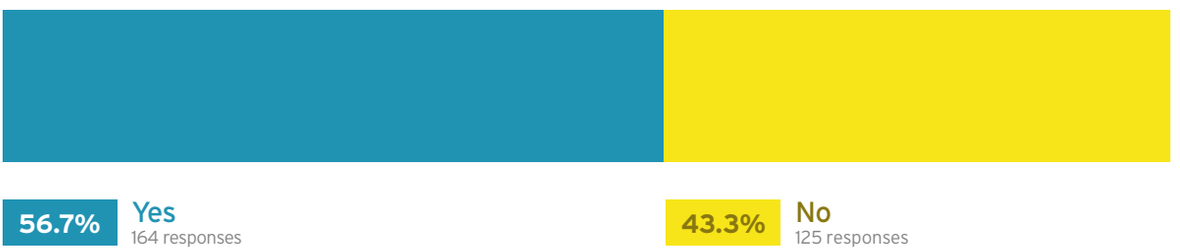
Efficient Employee Education

29% of respondents indicated training occurs annually, a following quarter opting for 'other' elaborated further within their comments; noting how training only occurred following a security breach. Organisations appear to deploy training ineffectively, with reactionary responses rather than anticipated methods. With a wider number of respondents expressing the same it is apparent that training should be a top priority, as attacks have become so iniquitous and effective.

28.7%	Annually 83 responses	9.7%	Weekly 28 responses
17.3%	Quarterly 50 responses	5.5%	Daily 16 responses
15.2%	Monthly 44 responses	25.6%	Other 74 responses
10.7%	Twice a year 31 responses		

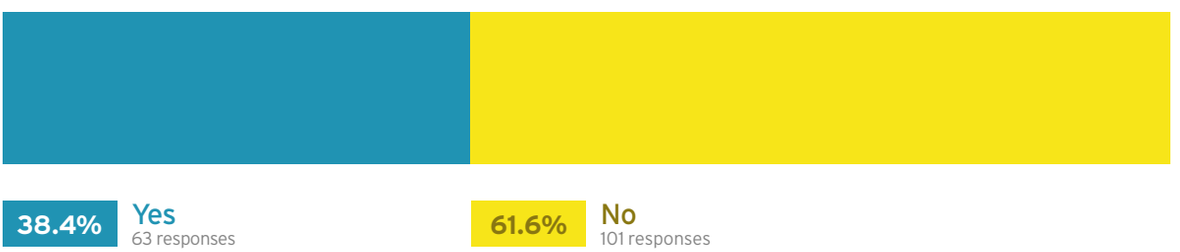
07 Has your organisation ever experienced a scenario where an employee has not adhered to your security policies?

57% of employees have experienced scenarios where colleagues have not adhered to security policies. Defining this during the on-boarding process can help counteract the vulnerability to potential threats. Peer to peer file sharing often opens doors to malware and viruses. Other strategies such as reporting suspicious emails and URLs, identifying language often used in phishing emails, and of course fighting off curiosity to open suspicious emails should be part of employee education.



08 If so, was this employee using work arounds in order to do so?

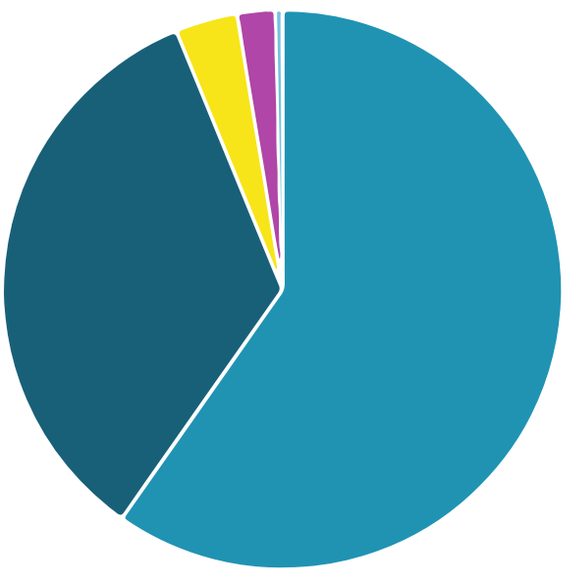
Ensuring employees are aware of company-wide approved platforms and formats would be the first step as they expose a particular weak point where cybersecurity is concerned. It's been recommended that employees who fall prey to phishing emails be subject to disciplinary procedures. This resolves nothing in the long run, as its speculative and still not known why people are attracted to click on phishing emails. It may possibly be narrowed down to something as simplistic as human curiosity, or due to other distinguishing factors such as their role, or personal email habits.

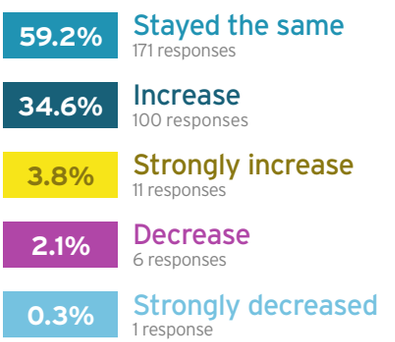


09 How do you see your budget for email security changing over the next 12 months?

There was a strong correlation among respondents who received training annually and those who expected to see their budget on email security stay the same. Organisations seem unwilling to invest further in email protection, with only 34% expecting an increase in security spend.

Organisations, whilst spending largely on network security solutions tend to neglect email security, despite the fact that between 75% and 90% of targeted cyber-attacks start with an email.





Shifting Attitudes

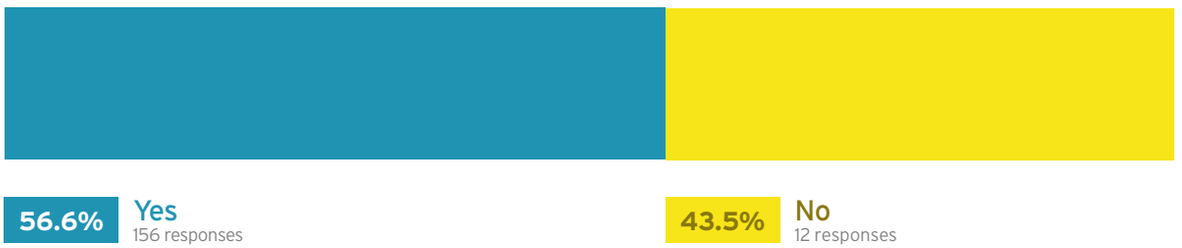
Many organisations migrating to cloud platforms need systems that increase functionality, productivity and agility. Integrating social technologies into daily work, is becoming the norm. Fast and responsive communications are required. These encourage employees to work remotely and collaborate efficiently internally or externally.

10 Have you considered or implemented non-email communication methods (eg Slack or Yammer) as a way of reducing email threats?

36% of respondents have either implemented or considered other forms of non-email communications, varying from Slack, to Yammer, and for frequent users of Office365, Microsoft Teams. Employees are increasingly becoming more reliant on fast-paced and real-time methods of communication in comparison to traditional methods. The business benefit is apparent, as without any latency colleagues can exchange information and share insight on projects.

A McKinsey report with a decade of research on the business uses of social technologies, confirms that messaged based platforms are gaining traction.

11 Does your organisation use Microsoft Office365?



Many organisations migrating to cloud platforms need systems that increase functionality, productivity and agility. Integrating social technologies into daily work, is becoming the norm. Fast and responsive communications are required. These encourage employees to work remotely and collaborate efficiently internally or externally.

"30 % of our interactions in the past year have been through smart machines."
Gartner

The way we communicate is changing and these transformational changes in technology are impacting organisations globally. Communications that can be tracked, referred to and contained on one platform yield a higher quality of information exchange. Enabling and delivering modern capabilities to collaborate, and exchange information in real-time should be a top priority for organisations. Not only will this encourage smarter work processes it will reduce the amount of threats permeating organisations, as reduction of its use minimizes the opportunities for cyberattacks.

Conclusion

The findings reveal that whilst organisations are aware of the volume of email attacks increasing over the past few years, not many are prepared to prioritise a budget that counteracts this.

The frequency of training is a key factor in the lack of awareness among employees unable to identify and prevent security threats. Devising training methods that are frequent, interactive and engaging may result in a reduction in threats. End-user training is imperative to prevent future attacks. Role-specific cybersecurity training giving focus to departmental functions, will provide context and clarity, helping employees easily identify potential threats.

Looking ahead, the inevitable increase of email communications sent daily among businesses and consumers will lead to wider threats. There is a requirement for larger investment to provide sufficient security measures that safeguard networks and implement strategies. This can only result in beneficial business factors. Integrating internal communication functions such as Slack, Yammer and Office365 Microsoft Teams would contribute to a reduction of threats.

The security measures a company takes are subjective, organisations need to decipher which safeguards meet companywide requirements dependent on what cyberattacks they have experienced. In any case, raising awareness among employees should be the first port of call, this can be done by different training methods including awareness training and simulated attacks.

Applying strategic integrated security solutions that consider end users, cloud systems and protect against potential across attacks would be an effective method to diffuse the increasing number of email threats.

A long-term solution should involve encouraging a shift in working culture, introducing more collaborative tools and a variety of file sharing methods. Exploring workarounds that encourage peer-to-peer communications and increase employee collaborative tools that minimize exposure to phishing, malware and cyberattacks.