Barracuda®

The Email Threat:

Key Concerns of EMEA IT Stakeholders and the Vital Role of Staff Training

White Paper

Introduction

Email is the ubiquitous, indispensable business IT system. Organisations rely on it to collaborate inside the organisation and with partners and suppliers, send and receive invoices, and engage with customers. Although newer web-based communication and collaboration systems have emerged in recent years, email remains the gold standard for IT: fast, convenient, simple to use, cost effective and auditable.

There's just one problem: email was built for a different time, one in which cyber-threats were few and far between. Email today is the number one threat vector facing organisations. Business Email Compromise (BEC), ransomware, banking trojans, phishing, social engineering, information-stealing malware, spam — the list of email-borne threats seems to grow every year. These are compounded by the risk of accidental disclosure of sensitive information via email. Out of 3325 data security reports filed with the UK's Information Commissioner's Office (ICO) in the 2017-18 financial year, the most common type of distinct incident was emails sent to the wrong person.

This gets to the heart of the challenge for IT security managers. Email is the number one threat vector precisely because it allows malicious third parties to directly target what has long been regarded as the organisation's weakest link: its employees. The following research was therefore designed not only to shine a light on the scale and impact of the email security challenge facing IT security practitioners but also to reveal more detail on this crucial human factor.

We found that email threats are increasing, costs are going up and the impact on IT and staff productivity is escalating. But while respondents believe that new tools like AI can help mitigate these threats, the vast majority also believe that end-user training and awareness programmes are a vital pre-requisite to improving email security.

Europe is said to suffer the highest economic impact of cybercrime in the world. New EU-wide legislation enacted in May, the GDPR and NIS Directive, will mandate strict new rules around cybersecurity and data protection. It's time for organisations to better understand where they're most exposed and what they can do to minimise damage.

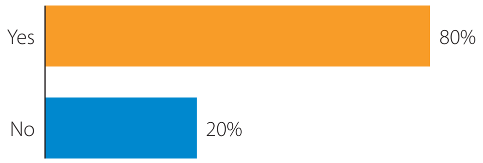
Methodology

The survey includes responses from executives, individual contributors and team managers serving in IT-security roles in 145 EMEA organisations. Companies surveyed include small, mid-sized and enterprise businesses in technology, financial services, education, healthcare, manufacturing, government, telecommunication, retail and other industries. This is part of a wider global study detailing the current state of email security.

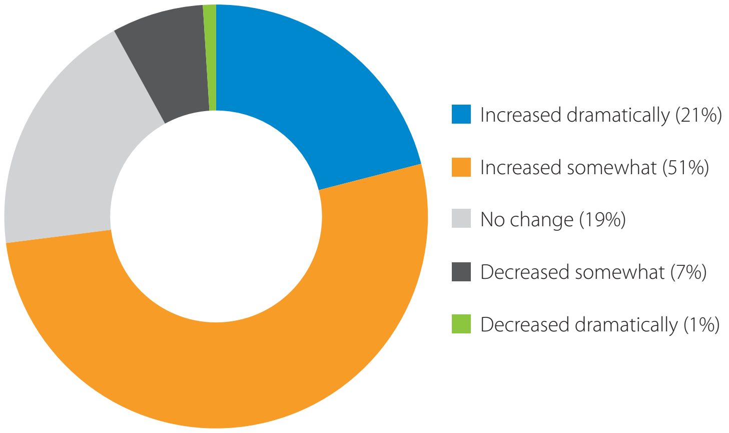
Email threats are everywhere

What's very clear from the outset is that email security threats show no signs of slowing down. Some 80% of respondents claimed their organisation faced one in the past year and 73% said the frequency of attacks had increased over this time.

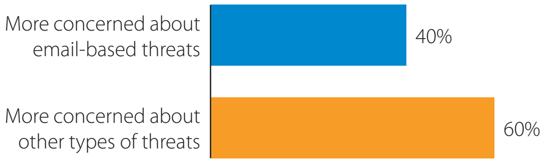
Has your company faced any attempted email-based security threats in the past year?



How has the frequency of email-based security attempts changed in the past year?



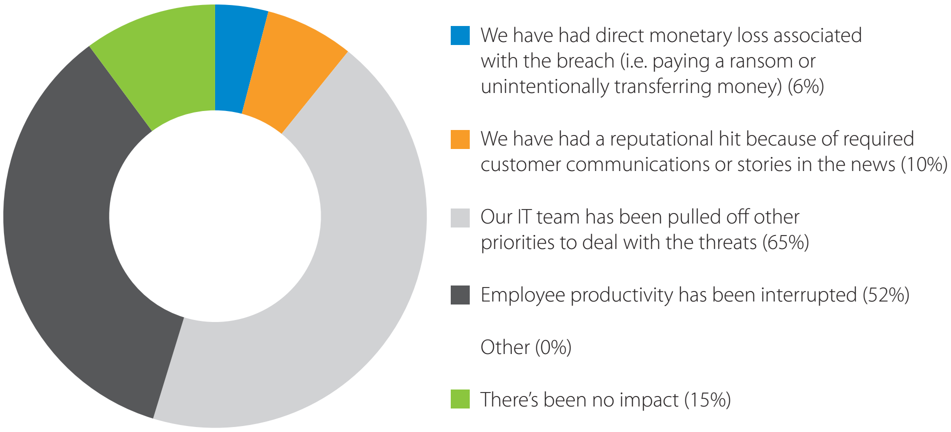
Compared to other types of security threats (e.g. network-centric) how concerned are you about email-based threats?



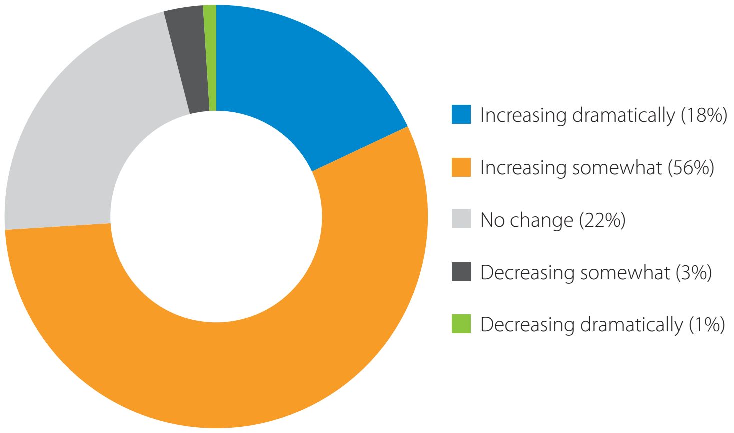
The biggest impact of these has been to distract IT teams from other priorities (65%) and disrupt employee productivity (52%). Both have potentially serious consequences. Tying up IT teams can reduce the value they add strategically in helping to grow the business. This is something which few IT managers can afford given egregious skills shortages facing the industry — slated to hit 1.8m globally by 2022. Lost productivity can also have a major impact on long-term growth and staff satisfaction, leading to employee attrition.

Just 15% of respondents claimed not to suffer an impact from email-borne threats. However, even this small figure is likely to be an over-estimate when one considers that sometimes the cause and effect linking cyber-attacks to business damage are not immediately clear.

What has been the impact of these attempted email-based security threats? Choose all that apply.

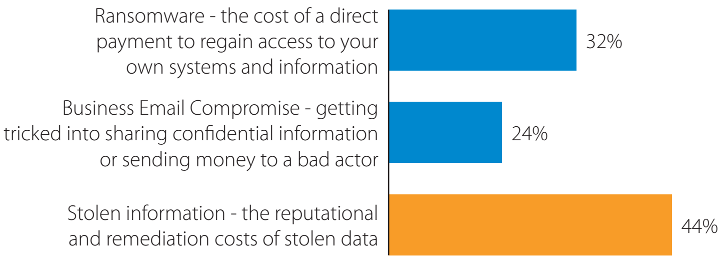


Think of the overall cost of an email security breach including identifying, remediating, communications with those impacted, business interruptions, etc. How is the total cost of each email security breach changing?



Lost staff productivity and business interruption will certainly hit the bottom line, alongside the identification, remediation and clean-up of threats and other consequences of email cyber-attacks. The vast majority (74%) of respondents claimed the cost of email-related breaches was increasing, with nearly a fifth claiming costs have escalated dramatically. Stolen information (44%) was thought to be most costly: both customer data and sensitive IP an incur a major financial liability, not just in direct costs but also subsequent legal action, and the long-term impact on brand reputation. To this, organisations must also add the prospect of GDPR or NIS Directive-related fines, which could reach €20m or 4% of global annual turnover, whichever is higher.

What type of email security breach is likely to be MOST expensive for your company?

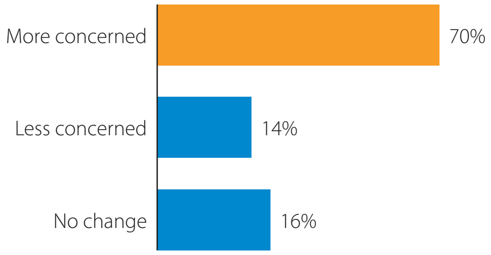


Unlike the GDPR, the NIS Directive covers only providers of "essential services" in key infrastructure sectors. But it enforces strict rules which require regulated organisations to follow best practice security processes.

BEC (24%) and ransomware (32%) were also highlighted as some of the most expensive threats to deal with. FBI figures for 2017 claimed BEC attacks alone resulted in losses of over $676m.

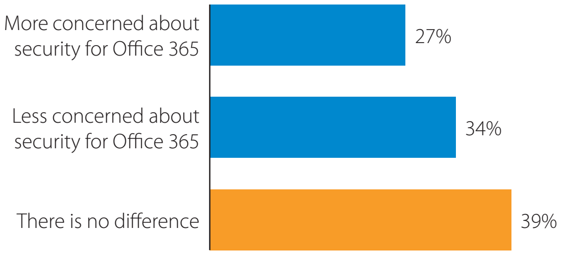
Perhaps it's no surprise that 70% of IT practitioners told us they're more concerned about email security now than five years ago.

How concerned are you about email-based security now compared to five years ago?



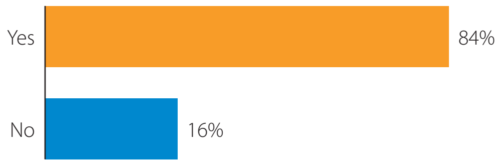
We should also note that moving to the cloud doesn't reduce the need for email protection. Respondents to our poll were just as concerned about email-based attacks via their Office 365 installations as via traditional on-premise — the largest number (39%) claimed there was no difference between the two.

Are you more or less concerned about email-based security attacks in an Office 365 environment compared to other mail solutions?

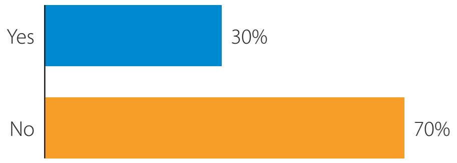


The ransomware epidemic spreads

Is ransomware a concern for you and your organisation?

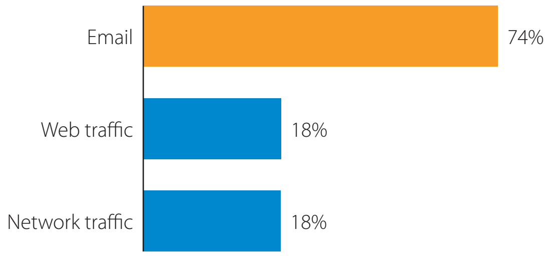


Has your organisation been a victim of ransomware?



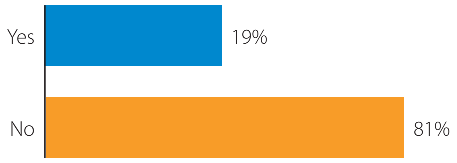
Ransomware was one of the standout threats of 2017 thanks to major global campaigns such as WannaCry and NotPetya. This may account for the 84% of respondents who claim that these threats are a concern, and the 30% who said their organisation has fallen victim. Nearly three-quarters said attacks originated via email. Phishing and social engineering tactics are designed to trick employees into clicking on links and opening malicious attachments in emails spoofed to appear as if sent from a reputable source. Until organisations get better at educating their users, this tactic will continue to pay dividends for the black hats.

Where did your ransomware attacks originate? Choose all that apply.



The one positive is that 81% of those that were hit by ransomware claimed not to have paid the ransom — a tactic recommended by law enforcers and experts. Backing up regularly according to the 3-2-1 rule will help reduce the impact of ransomware attacks and ensure you're not forced into paying for a decryption key which may never be sent.

Did your company pay the ransom?

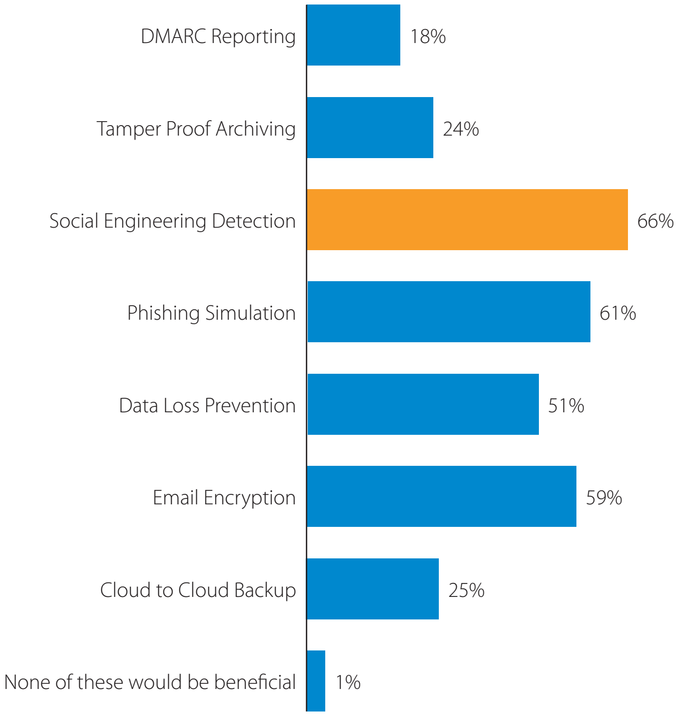


New technologies can help

The good news is that there are plenty of technologies organisations can use to help mitigate the risk of an email-borne attack. Respondents claimed social engineering detection (66%) and phishing simulations (61%) were the most beneficial. Both address key concerns over human error: in either providing a safety net to spot and block attempts to trick employees into clicking on malicious links, or helping to train them to better detect phishing emails from the start.

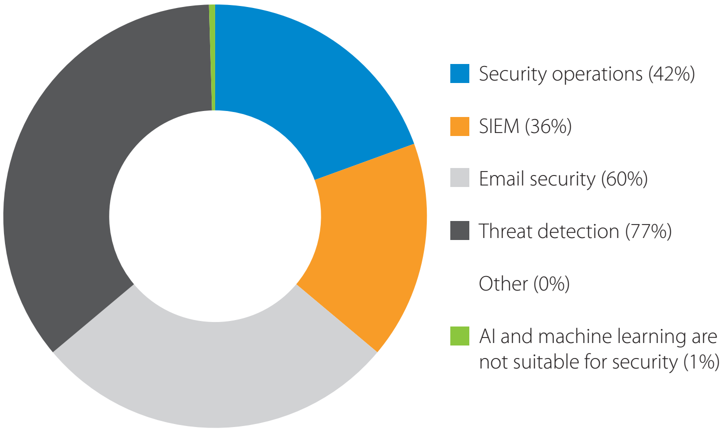
Other popular suggestions for tools that could help included email encryption (59%) and Data Loss Prevention (51%). The former will become increasingly important given the provisions of the GDPR. The law explicitly references encryption as a key technology to help reduce the risk of customer data falling into the wrong hands.

Which of the following capabilities for email security would be beneficial to your company?



IT security experts we spoke to also said that artificial intelligence (AI) or machine learning could be a good fit for email security (60%), alongside threat detection. Once again, these technologies can provide a valuable service in spotting and blocking attempts to trick employees into clicking on phishing emails. They do this by learning the organisation's unique communication patterns, so that anything even slightly out of the ordinary raises a red flag.

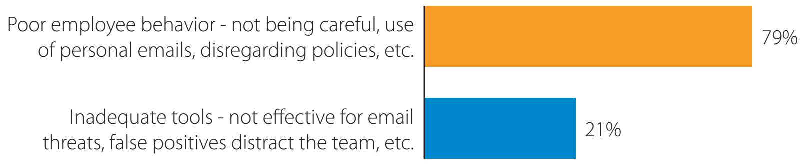
What areas of security would you consider most suitable for Artificial Intelligence (AI) or machine learning? Choose all that apply.



The insider threat grows

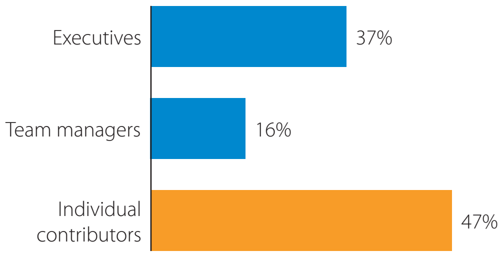
As discussed, email threats offer cyber-attackers a unique opportunity to directly target employees. Without the right tools in place, a single misplaced click could be enough to install ransomware on the corporate network or let attackers in to rifle through customer databases. Respondents recognised the insider threat, claiming that poor employee behaviour (79%) was a greater email security concern than inadequate tools (21%).

Which of the following is a greater email security concern?
Choose the one answer that most closely applies.

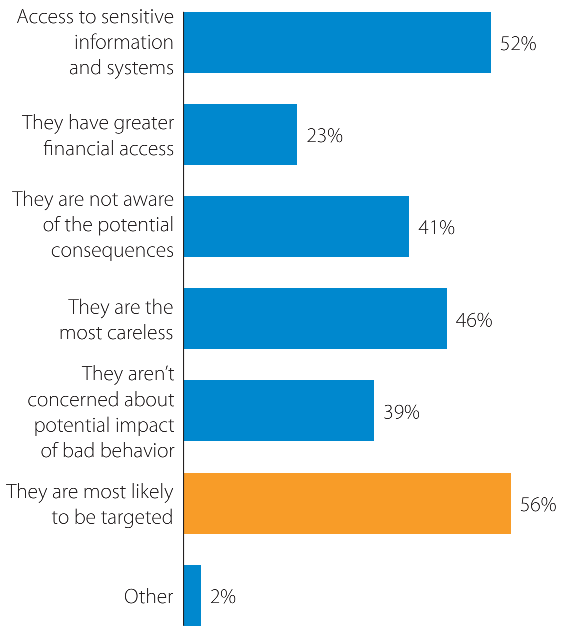


There was most concern over individual staff members falling victim (47%), although executives (37%) were also viewed as a potentially dangerous weak link in the security chain. Finance (26%) and sales (18%) departments were viewed with most caution. Topping concerns for respondents were the fact that these roles and departments have access to sensitive info and systems and are most likely to be targeted. It's clear that IT security experts believe that by the law of averages, if attackers target these users consistently they will get results.

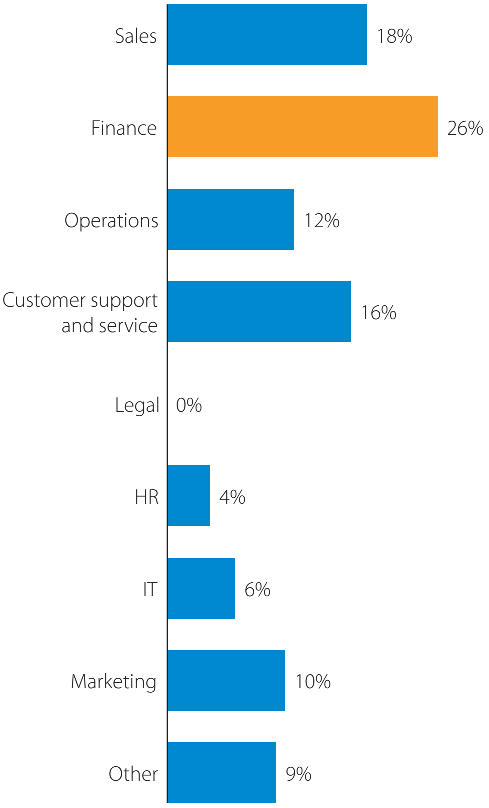
What level of employee are you most concerned about falling for an email security attack (e.g. social engineering, phishing)?
Choose the one answer that most closely applies.



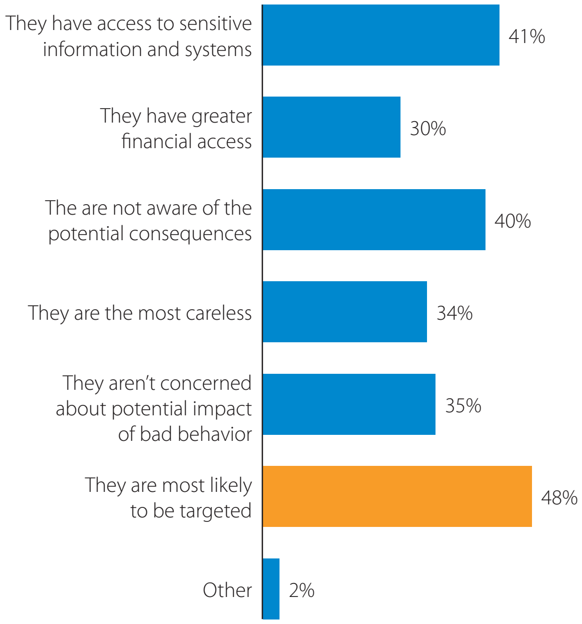
Why are you concerned about that level of employee falling for an email security attack?
Choose all that apply.



Which department's employees do you think are most vulnerable to falling for an email security attack (i.e. social engineering, phishing)?



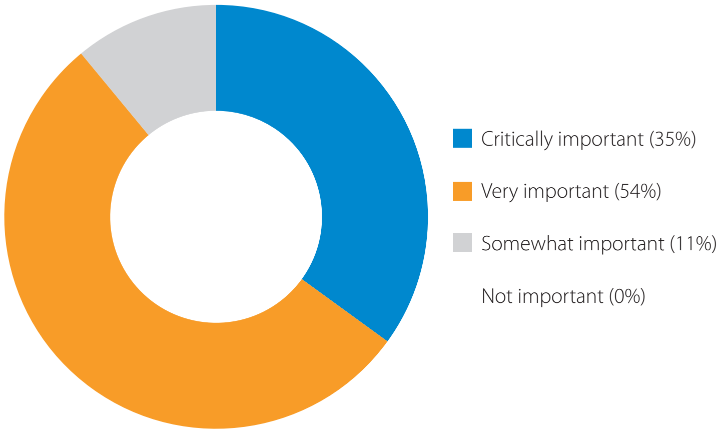
Why are you most concerned about employees in those departments falling for an email security attack? Choose all that apply.



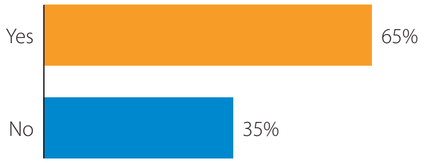
The key to effective user training

The vast majority (89%) of IT security experts believe that end-user training and awareness programmes are important, with over a third (35%) claiming they're critically so. However, a sizeable number (35%) still don't train their employees on how to spot phishing and spear-phishing.

How important are end-user training and awareness programs in preventing email-based security attacks?



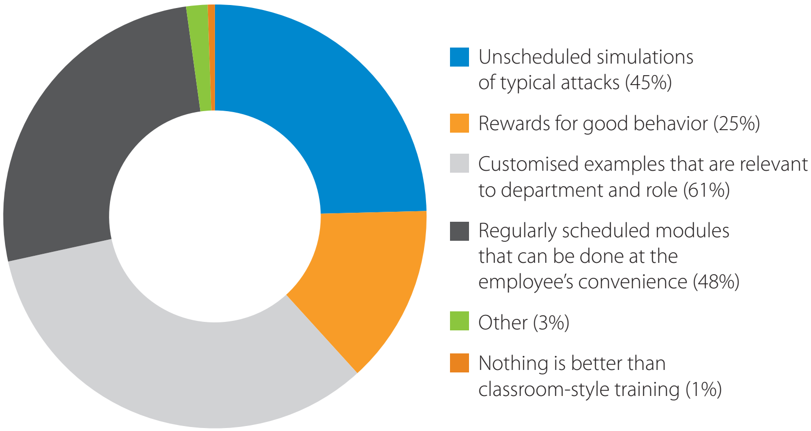
Do you currently train your employees on phishing and spear phishing prevention?



Let's be clear; phishing is one of the most popular tactics employed by cyber-criminals to spread malware and infiltrate the corporate network en route to valuable customer data and IP. Verizon claims that it was responsible for 93% of all breaches it analysed last year. Spear-phishing is a more highly targeted version which may have a greater chance of success as the perpetrators typically make such emails more convincing and relevant to the victim.

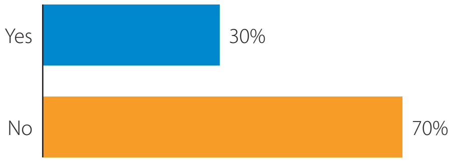
Training your staff effectively should therefore be a key part of any cybersecurity programme. But not all approaches are created equal. Instead of traditional classroom-based approaches, experts recommended using unscheduled simulations of real-world attack simulations (45%), and customised examples that can be tailored so they're more relevant to department and role (61%). Also recommended were regularly scheduled modules that can be completed at the employee's convenience (48%).

In your experience, what approaches to end-user training are better than traditional classroom-style training? Choose all that apply.



Organisations have to think outside the box when it comes to staff training. Traditional approaches simply aren't effective enough and are tough to fit in around other business priorities. It's heartening to see 30% of EMEA respondents have sought the help of a third-party training provider. With in-house training skills increasingly hard to come by, outsourcing this part of your cybersecurity capabilities to an expert provider can offer a lower cost but highly effective way to turn your weakest link into a formidable first line of defence.

Do you have a third-party phishing and spear phishing training provider?



Conclusion

Thanks to new EU-wide data protection and security regulations, it's more important than ever that IT leaders tackle the cyber-threats posed by the email channel. Email has always suffered from a lack of built-in security, and while protocols like DMARC can help, phishing, malware and BEC-related fraud remain major challenges to IT security teams.

As we've seen from this report, email attacks are escalating, costs are increasing and concerns are rising. But there are some positives. With the help of innovative technologies such as AI-powered tools, organisations can get better at spotting spoofed and malicious emails. Combined with a renewed focus on more progressive approaches to staff training, IT security bosses can begin to fight back. By outsourcing training to an expert provider, IT teams can focus on more strategic initiatives, and ensure cybersecurity remains a driver of growth and competitive differentiation.

To find out more about how you can stay ahead of email threats visit: www.barracuda.com/products/email_protection

About Barracuda Networks

Barracuda simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications and data regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organisations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda®

Brunel House
Stephenson Road, Houndmills
Basingstoke RG21 6XR
United Kingdom

t: +44 (0) 1256 300 100
e: emeainfo@barracuda.com
w: barracuda.com