Email Security Trends

Special Report

About the report

Barracuda Networks surveyed global IT stakeholders to capture their experiences and attitudes about the current state of email security.

The survey includes responses from 634 executives, individual contributors and team managers serving in IT-security roles in the Americas, EMEA and APAC. Companies surveyed include small, mid-sized and enterprise businesses in technology, financial services, education, healthcare, manufacturing, government, telecommunication, retail and other industries.

A wide range of questions captured hard data about ransomware, phishing and other threats, as well as the related business impacts, prevention efforts and email-security capabilities most beneficial for stopping attacks.

Key Findings

Email threats are increasing, costs are going up and the impact on staff productivity is escalating.

The vast majority of IT professionals believe that end-user training and awareness programs are a vital pre-requisite to help mitigate threats and improve email security.

Email security threats are pervasive.

- 87% of IT security professional said their company faced an attempted email-based security threat in the past year.

The threat of ransomware is a concern for 88%.

- More than 1/3 have already experienced an attack.

More than 90% said email archiving is critical, citing a variety of business benefits.

- Maintaining an audit trail for compliance purposes, investigating suspicious activity and cutting costs for e-discovery requests were the top reasons.

Larger businesses are more concerned about Office 365 email security; smaller businesses are less concerned.

- While the differences are fairly minor, this could be because larger companies have more data at risk in Office 365, due to having broader deployments rolled out that include SharePoint, OneDrive and other applications.

There's a strong consensus of opinions about employee training and its effect on email-based security.

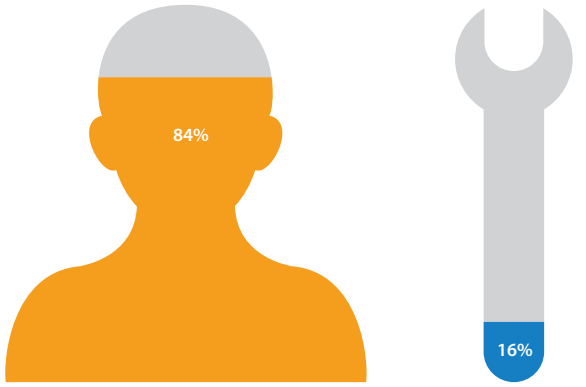
- 100% said end-user training is important to prevent attacks!
- Phishing simulation and social-engineering detection were identified as the most beneficial email-security capabilities.
- 98% said there are better ways to train employees than traditional classroom-style education, including customized examples that are relevant to an employee's department and role, unscheduled simulations of typical attacks, training modules that can be done at the employee's convenience, and rewards for taking the right actions.

Email Security

Email security threats are pervasive. 87% of IT security professionals said their company faced an attempted email-based attack in the past year. Three in four are more concerned about email-based security now than they were five years ago.

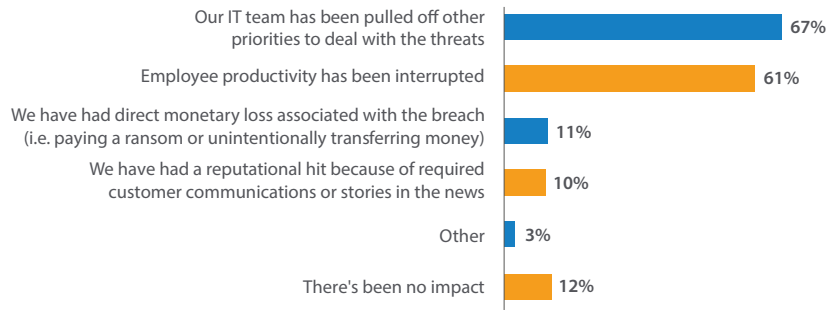
81% said the frequency of email-borne attacks has increased in the past year: 25% said it increased dramatically and 56% said it increased somewhat. 81% also said the overall cost of an email security breach is increasing: 22% said it is increasing dramatically and 59% said it is increasing somewhat.

Which is a greater email security concern?



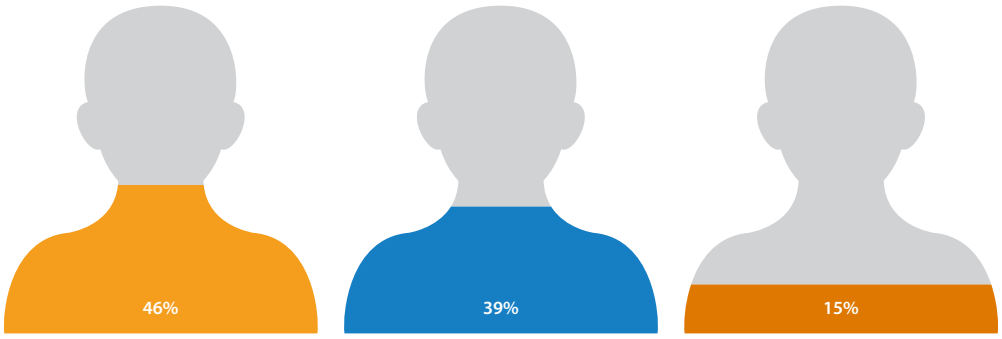
Poor employee behavior is the main concern for most, not the tools that organizations have in place to stop threats. This has always been conventional wisdom; the data now backs it up. It's not surprising humans are the weakest link when it comes to phishing attacks. We're curious and helpful by nature, which is why social engineering attacks are popular and profitable for cybercriminals.

What has been the impact of attempted email-based security threats?

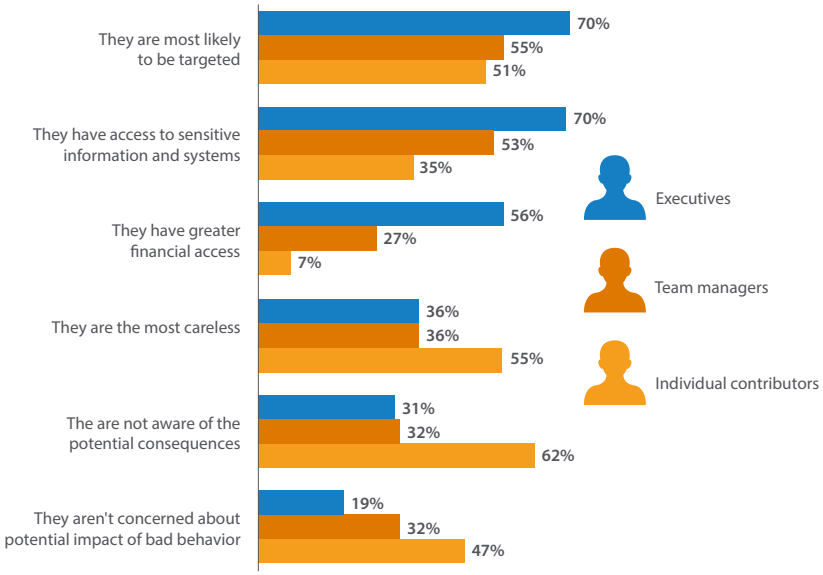


Attempted email-based attacks have already impacted their businesses with interruptions and monetary loss, according to 88% of the IT pros. Half said they are more concerned about email-based threats than any other types of security threats.

Which employees are you most concerned about falling for an email attack, such as phishing?

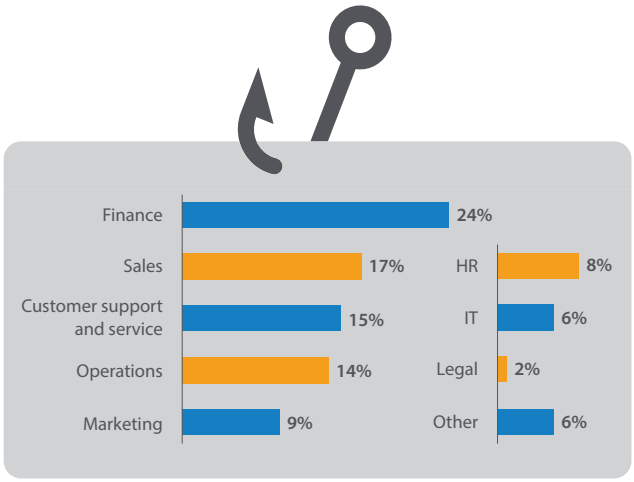


Why are you most concerned about those employees falling for an email attack?



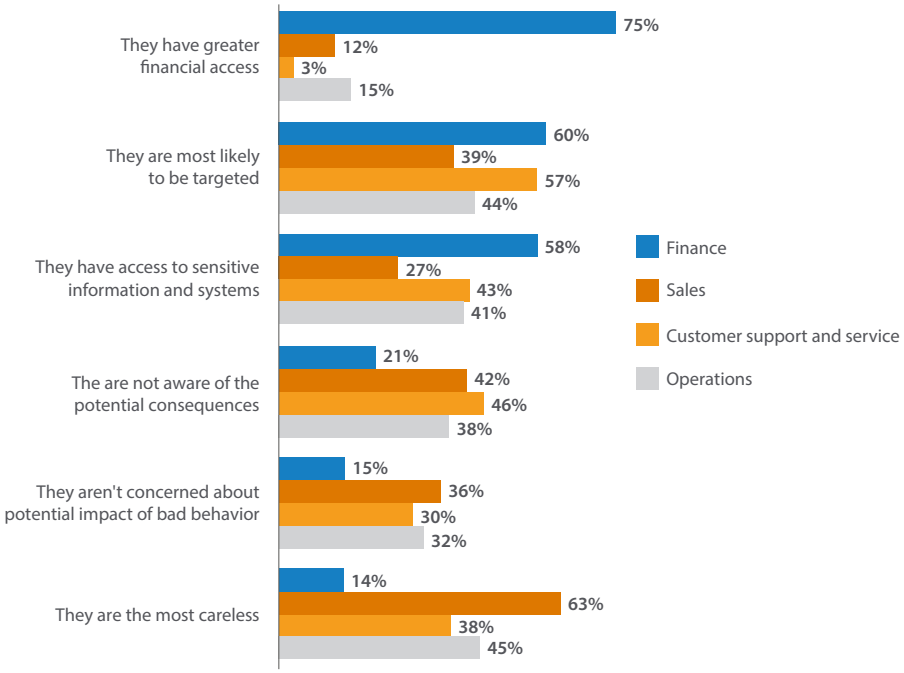
There's no consensus about the type of employee most likely to fall for an attack. Criminals are potentially balancing their attacks and not necessarily targeting any particular type of employee. Email attacks are a numbers game; the more attempts made, the more likely someone will fall for one – and there are a lot more individual contributors available to attack than executives. However, the payoff could be larger when executives fall for a social-engineering attack, due to the availability and quantity of sensitive information they have access to, which explains the increasing popularity of spear phishing and whaling. While frontline staff has less access to sensitive data, they are also less aware of the risks and impacts related to mistakes they can make, perhaps making them easier targets. Criminals are operating their scams like businesses, making risk-versus-reward decisions every day. They are continually experimenting to figure out what works and what doesn't.

Which department's employees do you think are most vulnerable to falling for an email attack, such as phishing?



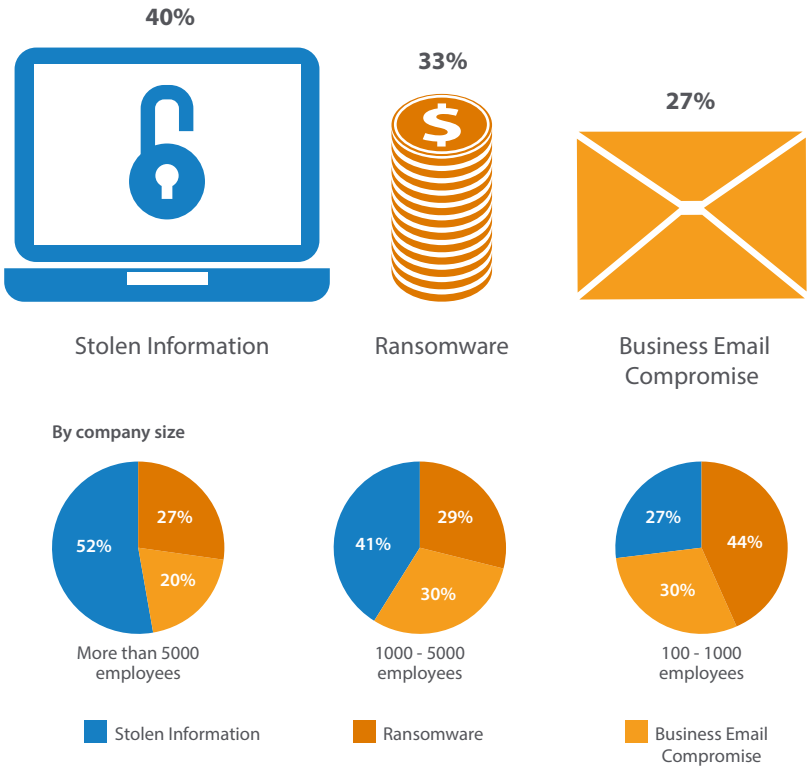
It's not a surprise that finance employees are viewed as the most vulnerable, considering their access to the crown jewels, including bank account information, wire transfer numbers and other valuable business information. It's somewhat surprising and interesting, however, that employees of legal departments were so far down the list, as they typically have access to strategic information related to lawsuits, sensitive information that could be used for insider trading, and other highly confidential matters.

Why are you most concerned about those employees falling for an email attack?



Sales and customer support top the list as the least aware of the potential consequences of making mistakes when receiving a phishing email. This is concerning, as these teams communicate regularly through email, increasing the potential for successful attacks.

What type of email security attack is likely to be the most expensive for your company?

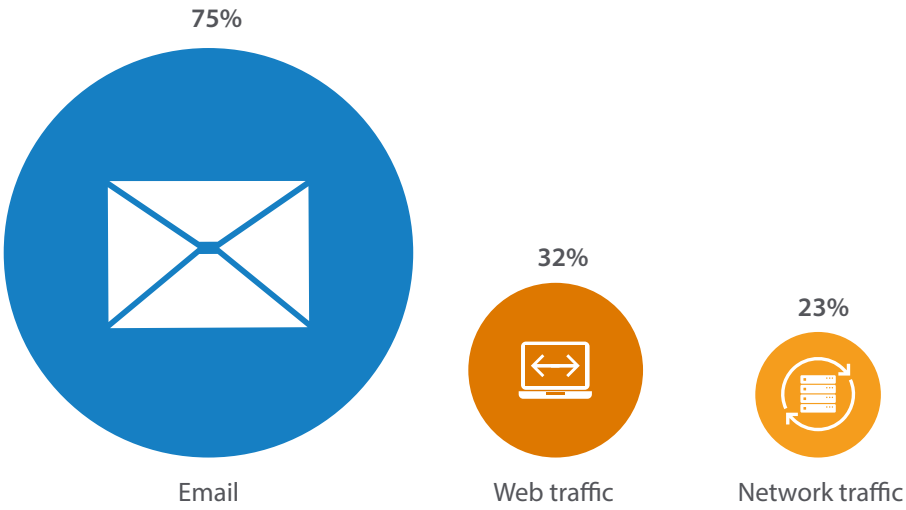


There's no consensus about which type of email security breach would be the most expensive. Information theft is the classic breach example; however, ransomware and business email compromise attacks are still fairly new and have quickly become expensive in their own right, making them appealing to cybercriminals. Criminals apparently prefer direct monetization attacks over traditional theft sales. Unlike information theft, which requires a buyer, these newer attacks don't; they cut out the middleman, meaning less work and a faster, better ROI for the criminals.

Ransomware

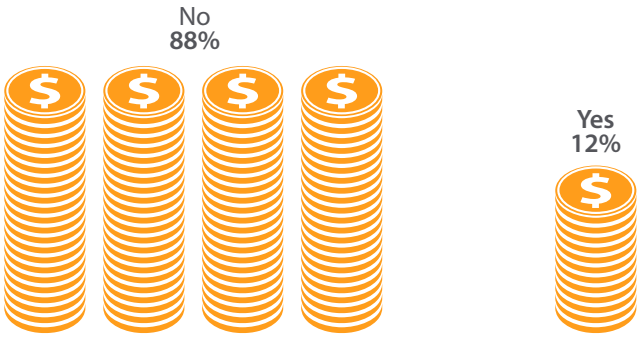
The threat of ransomware is a concern for 88% of those surveyed. 35% said their organization has already been a victim of ransomware.

Where did your ransomware attack originate?



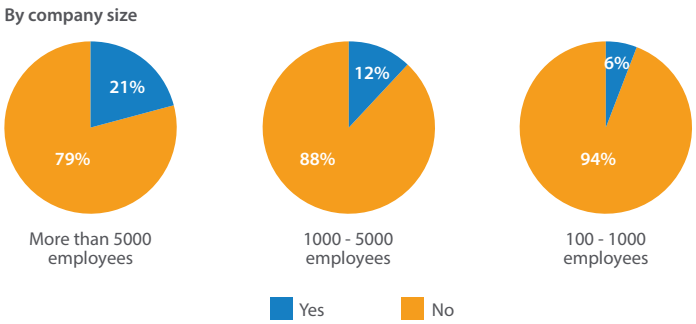
IT pros indicated that ransomware attacks typically came from more than one source. Attacks can be very hard to diagnose, so this could be due to uncertainty or multi-vector attacks, as some sophisticated ransomware scams involve email, website links and malware downloads. Typically, the focus is on resolving the problem as quickly as possible, rather than identifying the source of the attack. Even if an organization has the resources to conduct a root-cause analysis after the fact, there's no guarantee the source of the attack will be conclusively identified due to their complexity and evolution.

Did your company pay the ransom?



While the percentage of companies paying the ransom was small, enterprises were more likely to do so than small and mid-sized businesses.

Based on how pervasive ransomware attacks have become, along with the accompanying media coverage, it's somewhat surprising to see such a small percentage of companies paying. Perhaps it's actually a glimmer of hope: maybe organizations had comprehensive backup solutions in place and were able to rapidly recover critical data without paying.

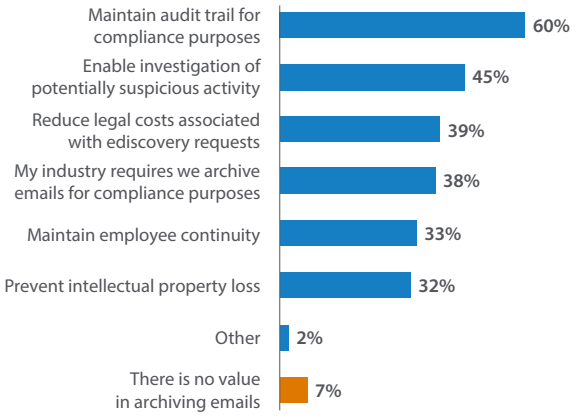


It's not surprising that enterprises were more likely to pay ransom than smaller companies; they are more likely to have the resources to do so. They also likely understand that the soft costs of recovering from an attack, including lost time and productivity, can be much higher than paying the ransom.

Archiving

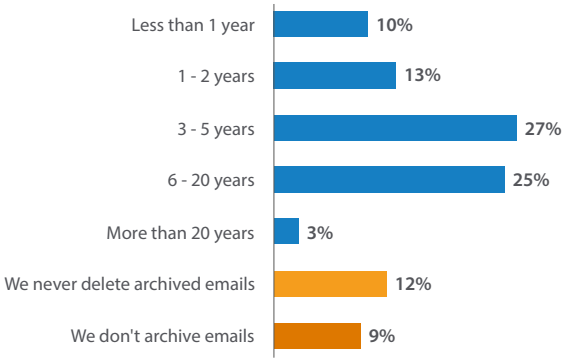
93% of IT pros said email archiving is critical, citing a variety of business benefits. Half of those surveyed said their company archives emails for a retention period of five years or less.

What value is gained by archiving emails?



The value of archiving is recognized on a widespread basis and not just by those in highly-regulated verticals. It's not surprising that compliance tops the list of reasons, but it's also evident that there's a rising awareness of archiving's usefulness for eDiscovery, business continuity and a variety of other use cases. Businesses of all sizes, across all industries, understand the high costs that can be incurred due to legal actions, audits, data loss and security threats when data isn't protected in an archive. Archiving's crucial contribution to data accessibility—providing rapid access via robust search capabilities—is strongly underscored by all the cited use cases.

How long does your company archive its emails?



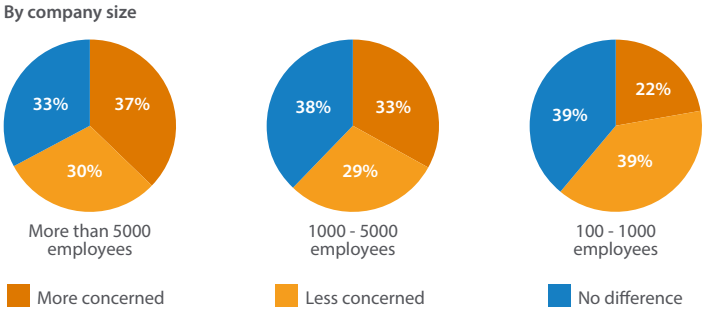
It's clear based on the range of retention periods that businesses are working to optimize their individual retention policies. Businesses appear to be striking a balance: they are retaining emails for the length of time required to meet industry-specific compliance requirements and then getting rid of them for risk-management purposes. A documented email governance policy that regulates the retention and disposal of email helps every company, regardless of industry, to reduce overall risk.

Office 365

There has been a big shift with regard to cloud security in the last five to 10 years. In the past, IT pros favored on-premises systems, as cloud was considered less secure. Now, cloud computing has become more mainstream. This increased confidence in the cloud is a sign that professionals are more educated about the nuances of cloud security; they understand the cloud doesn't mean more risk, it requires focusing attention on a different set of risks.

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

There's no consensus about Office 365 security concerns. Larger businesses are more concerned about Office 365 email security; smaller businesses are less concerned. While the differences are fairly minor, this could be because larger companies have more data at risk in Office 365, due to having broader deployments rolled out that include SharePoint, OneDrive and other applications.

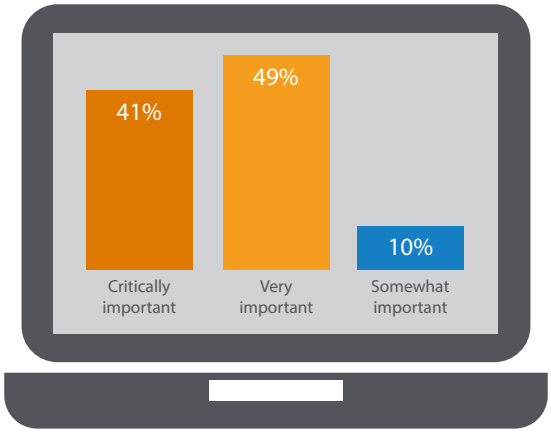


Large enterprises are likely to have more resources and a greater focus on security in general than smaller businesses.

Employee Training

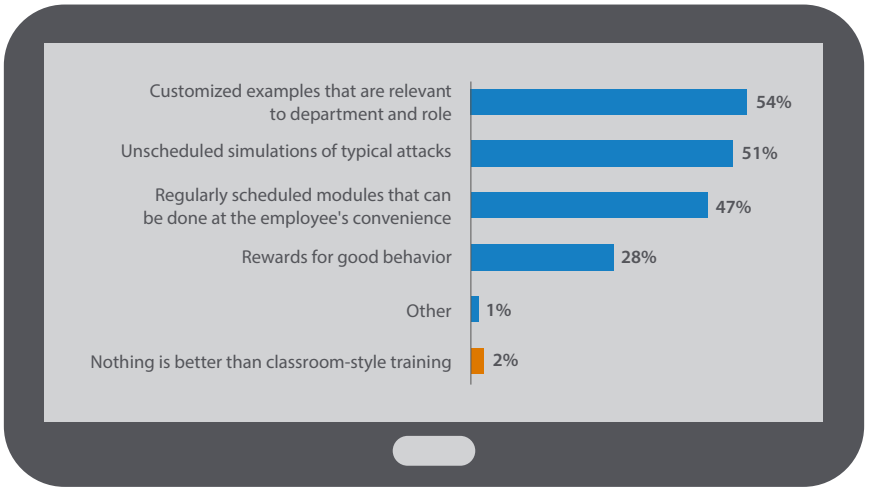
There's a strong consensus of opinions about end-user training and its effect on email-based security. 100% said end-user training is important to prevent attacks.

How important are end-user training efforts to prevent attacks?



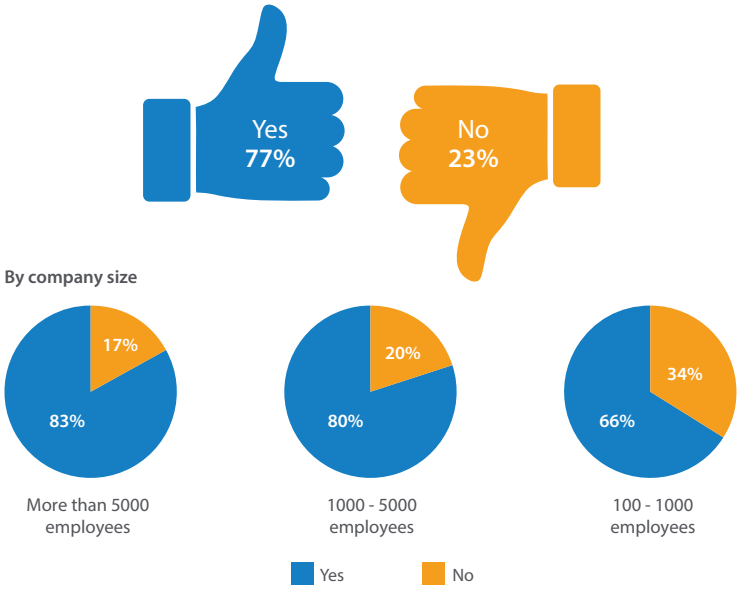
90% said end-user training was critically or very important and 10% said somewhat important. No one said end-user training was not important. This is a good thing because IT pros are well aware of the risks presented by user error; training isn't just nice to have, it's a top priority because targeted attacks have become so nefarious and effective.

In your experience, what approaches to end-user training are better than traditional classroom-style training?

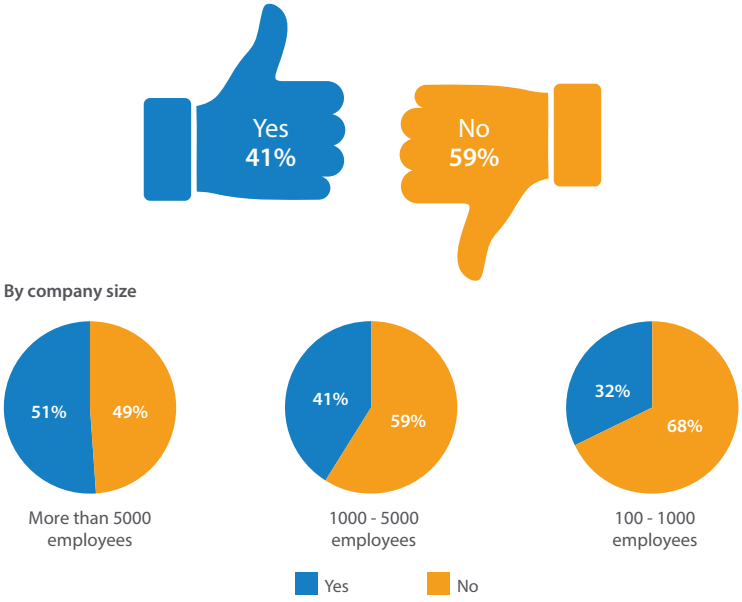


Modern businesses are embracing new and scalable approaches. 98% said there are better ways to train employees than traditional classroom-style education, including customized examples that are relevant to an employee's department and role, unscheduled simulations of typical attacks, training modules that can be done at the employee's convenience, and rewards for taking the right actions.

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

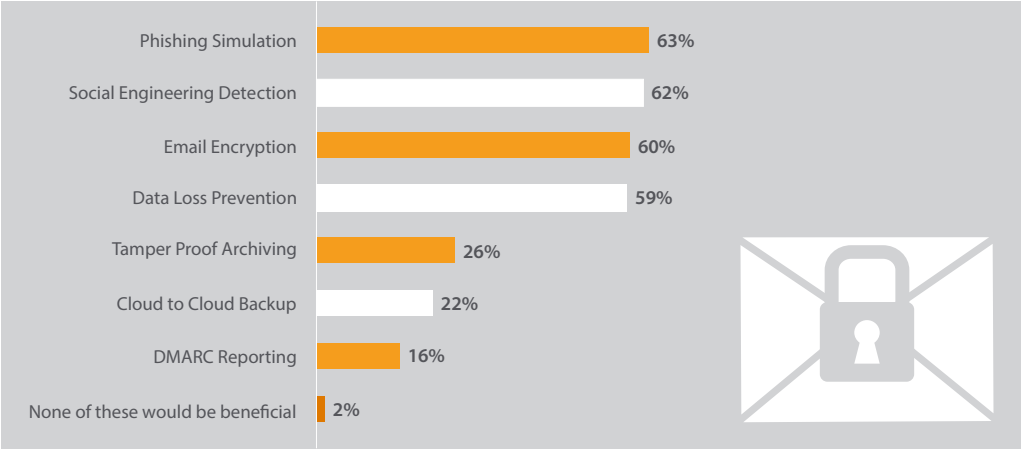


Do you have a third-party phishing and spear phishing training provider?



There's a gap between good intentions and actions: While 100% say employee training is important, only 77% are doing it. This is likely due to a number of factors, including budget limitations, other priorities needing focus and the non-scalable, classroom approaches available. Larger organizations (more than 1,000 employees) are more likely to implement training. This isn't uncommon; enterprises are often early adopters, with smaller organizations following behind. Larger organizations have more people and more risk as a result; they also have more resources for items like employee training.

Which email-security capabilities would be beneficial to your company?



Phishing simulation and social-engineering detection were identified as the most beneficial email-security capabilities. This data highlights the widespread severity of phishing attacks and the importance of trying to fight them. It's not surprising that phishing simulation tops the list of desired capabilities, based on the prevalence of the attacks and how successful they can be for cybercriminals.

About Barracuda Networks, Inc.

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 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployment configurations. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data protection. Get more information at barracuda.com.

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com