mimecast®

Securing the Enterprise in the COVID world

The State of Email Security

Contents

01. Email: an invaluable tool and a growing threat

02. The digital workforce is under attack

03. The post-COVID threat landscape

04. Is cyber resilience keeping up with the new dangers?

05. Cybersecurity awareness training: more critical than ever

06. A new urgency for online brand protection

07. Our top 10 takeaways

08. The bottom line

section

one.

As COVID-19 swept the globe, businesses found themselves more reliant than ever on email. But this greater dependence also posed new and insidious threats.

Email: An Invaluable Tool and a Growing Threat.

There's no question that the pandemic-driven shift from office to home-based work was a major contributor. With the flip of a figurative switch, interaction and collaboration shifted to digital only, and companies had to scramble to adjust. Cybersecurity teams, many of which were already resource poor, had new tools, systems, devices, and locations to protect overnight. And where most of the world saw crisis, cybercriminals saw opportunity, a fact that is reflected by the level of attacks organizations experienced during this period.

Among these criminals, email remains the most popular way to try and sidestep a business' defenses.

In response, 55% of technology and security executives, according to a recent PwC survey,[1] planned to increase their cybersecurity budgets and add to their full-time cyber staffs in 2021—even as they expect pandemic-induced disruptions to cause business revenue to decline.

This is in line with a Gartner Group finding that in the wake of the worldwide lockdown, two-thirds (67%) of corporate boards planned to increase their IT and technology budgets by an average of 7%.[2]

Among these criminals, email remains the most popular way to try and sidestep a business' defenses and here, in Mimecast's fifth annual State of Email Security report, we cast a harsh light on their efforts. Included in our 2021 survey results are important insights into the latest wave of email-borne threats and how companies from 10 countries on five continents are poised to counter them.

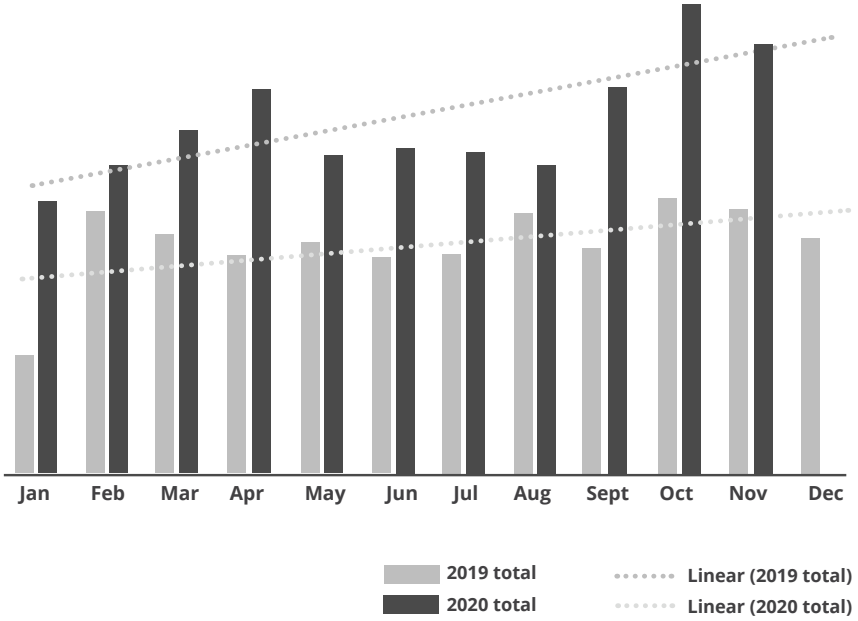
Up-to-the-minute data provided by the Mimecast Threat Center adds additional context and serves to underscore the magnitude of the post-COVID risks posed by increased digitalization of the workplace and growing reliance on email.

section

two.

The Digital Workforce Is Under Attack.

With employees around the world trading cubes, offices and conference rooms for email, instant messaging and Zoom meetings, more sharing of sensitive business information has migrated from conference room white boards and face-to-face conversations to discussions via collaboration tools and extended email threads. This swell of digital activity has presented cybercriminals with numerous new openings for social engineering attacks. To wit, during 2020, the Mimecast Threat Center detected a 64% rise in threat volume compared to 2019.

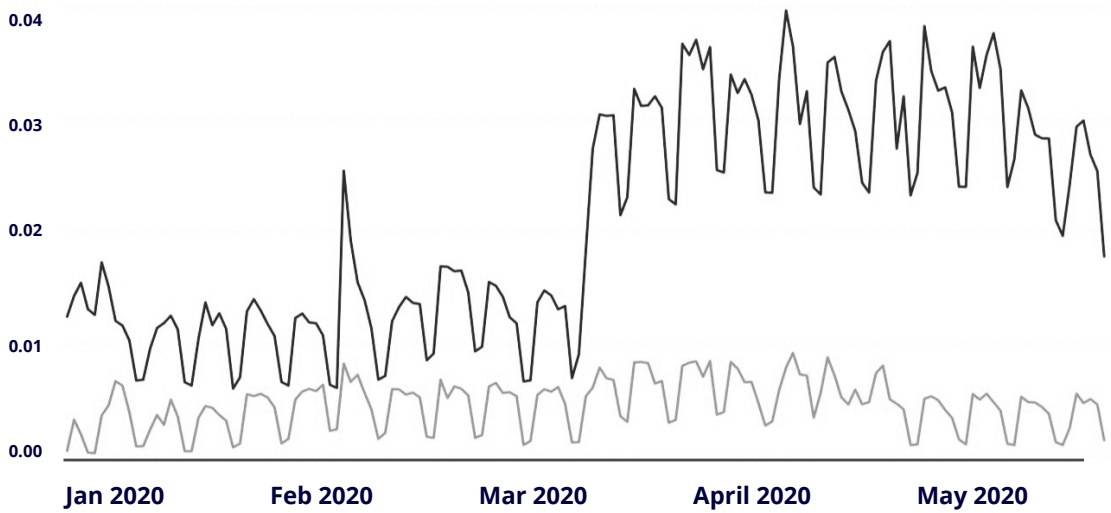


+64% **email threats rose by more than 64% during 2020**

A prime target has been employees newly deployed to work from home, where their attention is often diverted by household distractions and at a time when vulnerability to emotional or fear-based attacks has been high. Threat actors were quick to take advantage of this with a flood of new phishing attacks. The increase in volume was also likely an attempt to overwhelm security operations centers (SOCs) with alerts in the hope that some of them would be overlooked.

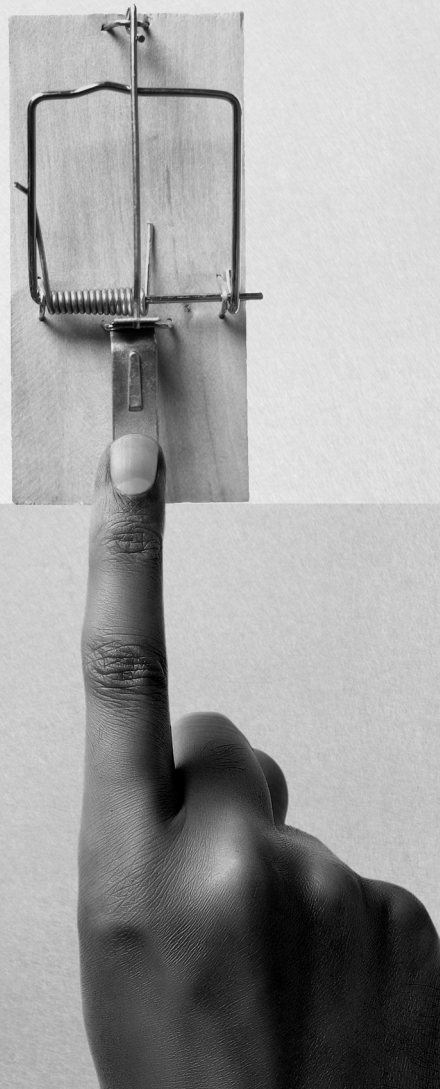
This uptick in cyber fraud has taken a toll and exacerbated many of the threats that companies already faced. For example, since the onset of the pandemic, the Mimecast Threat Center found that employees worldwide are clicking on malicious URLs embedded in emails three times as often as they had before.

Average number of unsafe clicks per user



3x

since the onset of the pandemic, employees are clicking on 3x as many malicious emails as they had before



As the level of risk has grown, these changes to the threat climate have become top of mind for many companies, and there is a looming sense of danger. This mindset is reflected in what the 2021 State of Email Security (SOES) survey participants view as their biggest email security challenges.

60%

of participants zeroed in on the increasing **sophistication of the attacks**

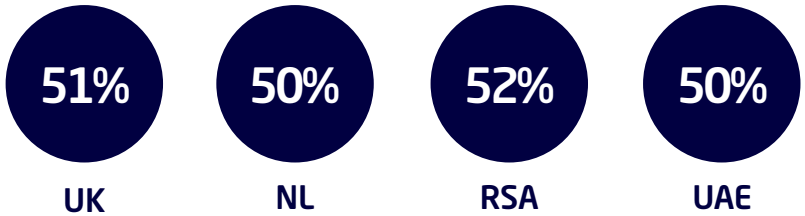
52%

of participants pointed to the growing **volume of attacks**

For a substantial majority (60%) was the increasing sophistication of the attacks that they face. More than half (52%) cited the growing volume of attacks among their top challenges, while even more tellingly, more than four out of 10 respondents (43%) said that employee naiveté about cybersecurity is one of their greatest vulnerabilities.

43% **of participants globally said that employee naiveté about cybersecurity is one of their greatest vulnerabilities**

Concerns about employee naiveté, while significant across the board, are heightened in certain countries. In the UK, the Netherlands, South Africa and the United Arab Emirates, half or more of the survey respondents (51%, 50%, 52% and 50% respectively) view the lack of cyber sophistication among employees as a major threat to their companies' security, compared with 43% globally.



Even as the threat environment becomes more pervasive, corporate dependency on email continues to grow, heightening the risks that companies face. The large majority of the SOES survey respondents (81%) noted that the volume of email at their organization has increased over the past year—and this was the case across the board, including for smaller businesses with 250 to 500 employees, as well as the very largest enterprises with more than 10,000 employees.

At the same time, more than two-thirds (70%) consider it likely (39%), extremely likely (26%) or even inevitable (5%) that an email-borne attack will damage their business sometime during 2021. This is up sharply from 2020, when only 59% of SOES survey respondents felt that was the case. Even more significantly, at those companies where the use of email rose during the past 12 months, the portion of respondents who saw an email-based attack as likely or inevitable rocketed to three-out-of-four (75%).

70% **of the companies interviewed expect their business to be harmed by an email-borne attack**

About the Survey Results Included in this Report

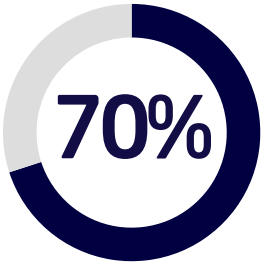
For our 2021 report on the state of email security, Mimecast commissioned research firm Vanson Bourne to conduct a global survey of 1,225 information technology and cybersecurity professionals from 10 countries including the U.S., the UK, Germany, the Netherlands, Australia, South Africa, the United Arab Emirates, Canada, Sweden and Denmark.

Participants were interviewed during February and March of 2021 and included respondents from companies ranging in size between 250 to 500 employees (17% of the total) and more than 10,000 employees (8% of the total). These companies were spread across 12 industrial sectors including technology and telecommunications (15%), financial services (12%), manufacturing (8%), the public sector (8%) and healthcare (6%).

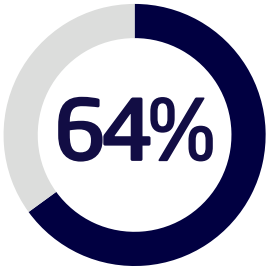
Among the participants, CIOs, CTOs, CISOs, IT Directors, and IT Security Directors comprised 47% of the total. The remainder included IT and SOC managers, as well as security architects and analysts. Report findings were supported by Mimecast's own Threat Center data, based on screening more than one billion emails globally per day.

Key Findings.

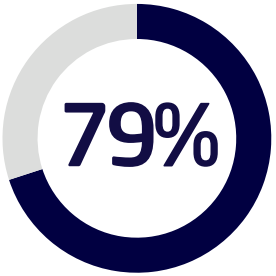
Over the last 12 months



of the companies expect their business to be harmed by an email-borne attack.



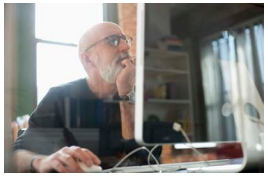
email threats rose by 64%.



of companies were hurt by their lack of cyber preparedness.

3x

since the onset of the pandemic, employees are clicking on 3x as many malicious emails as they had before.

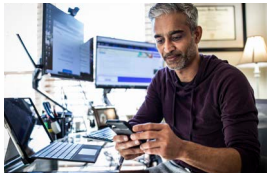


6+/10

companies suffered a ransomware attack.

1/5

ongoing cyber awareness training is only provided by 1 out of 5 companies.

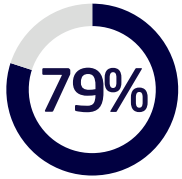


7/10

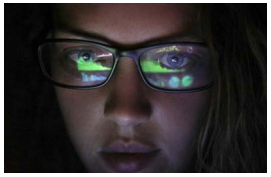
respondents believe that employee behaviors such as poor password hygiene are putting their companies at risk.

of companies still do not have an email security system.

of Microsoft 365 users think their companies need additional email security.

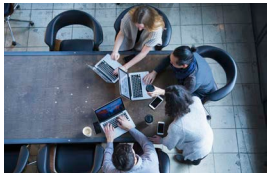


of companies were hurt by their lack of cyber preparedness.



8/10

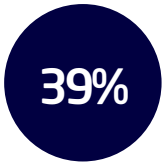
email usage increased this past year at 8 out of 10 companies.



8+/10

More than 8 out of 10 companies are already making use of DMARC or plan to do so over the next 12 months.

of companies are either using or plan to use a brand protection service.



of companies are using AI and machine learning to bolster their email defenses.

section

three.

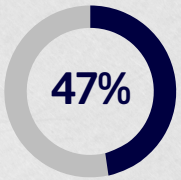
The Post-COVID Threat Landscape.

Although many different types of email-based attacks have proliferated throughout the pandemic, phishing has been the predominant threat, and 63% of the SOES respondents are facing a surge in targeted emails that attempt to lure employees into clicking on a malicious link or attachment. Some messages are familiar and crude, such as those seeking to solicit sympathy for the sender in order to defraud the recipient of money. Others are far more sophisticated and prey on COVID-related fears by purporting to contain important updates or officially sanctioned directives. In most cases, however, and regardless of the ploy, the threat actor's intention is the same: To dupe employees into revealing their log-in credentials.

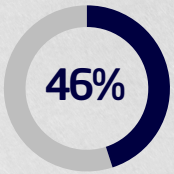
Business email compromise attacks (BEC) in the form of impersonation fraud also rose significantly, with 51% of the survey participants reporting an increase.

63% **since the pandemic began, phishing attacks have increased in 63% of companies**

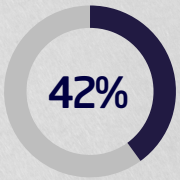
Other mounting threats include:



Spoofing emails
Spoofing emails that make fraudulent use of a company's brand in order to deceive the recipient. Close to half (47%) of SOES survey respondents are fending off an upswing in this type of scam.



Data leaks
Data leaks or other hazards due to carelessness or negligence or on the part of employees. Again, nearly half (46%) of the respondents reported greater fallout due to some type of employee misstep or misdeed.



Brand exposure
Illicit use of a company's brand in order to create counterfeit web sites. Among the respondents, 42% found that misuse of their brand was a growing danger.

Ransomware

6 days average of downtime experienced as a result of a ransomware attack

Of special concern are ransomware attacks, which are affecting more businesses across all regions and industries than ever before.

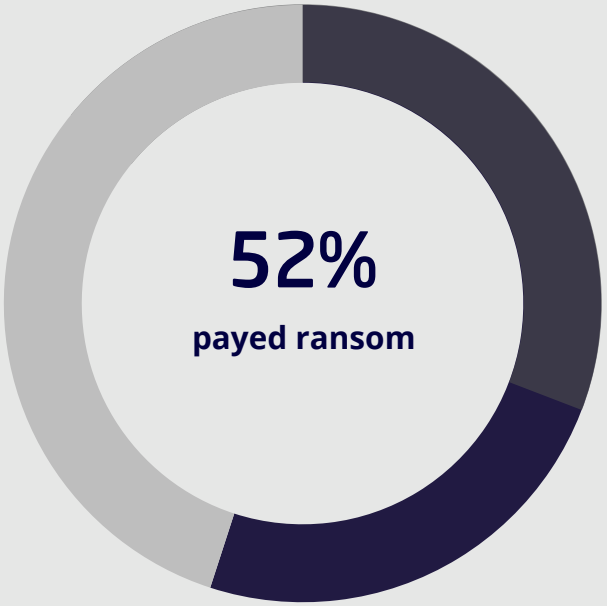
More than six out of 10 (61%) of SOES respondents acknowledged that their business was disrupted by ransomware at some point during this past year. This was a striking increase from 2019, when only 51% of respondents reported the same. Those companies that were afflicted experienced an average of six days of downtime as a result, and for more than a third of them (37%) it was a week or more.

This represents the growing impact of ransomware attacks year over year; in the State of Email Security 2020, organizations reported experiencing three days of downtime on average.

Among the affected companies, more than half (52%) felt compelled to pay the ransom. But of these, only two-thirds (66%) recovered their data. The other third (34%) failed to get their data back, despite paying the ransom.

6 out of 10

endured a ransomware attack last year



66%

recovered their data

34%

failed to get their data back

Collaboration Tools

With travel severely restricted and both employees and customers working from home, collaboration tools such as Slack and Microsoft Teams have become increasingly popular.

Virtually all (98%) of SOES 2021 respondents are making use of team-building and productivity software.

Useful as they are, these tools create new and often complex cybersecurity challenges. In particular, more than two-thirds of SOES respondents (70%) are concerned about the risks posed by the archived business conversations these programs generate.

70%

of participants are concerned over the risks **posed by archived business conversations**

Worries over collaboration tools are more widespread in certain countries. For example, the number of SOES respondents with concerns over the safety of their companies' collaboration tools ranged from three-out-of-four in the U.S. (75%) and Australia (76%), to nearly nine out of 10 (88%) in the UAE.

75% USA

76% AUS

88% UAE

86% business & professional services

76% construction

Likewise, certain industries that make greater use of collaboration tools exhibit higher anxiety over their safety. These include the construction, energy, consumer services and business services sectors, where the level of concern ranged from 76% (construction) to 86% (business and professional services) of respondents.

section

four.

79%

of companies were hurt by their **lack of cyber preparedness**

Is Cyber Resilience Keeping Up with the New Dangers?

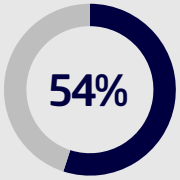
The COVID pandemic may be waning; but as 2021 progresses, bad actors will continue to exploit it. Statistically speaking, the likelihood of them doing so is greater than 95%, according to the Mimecast Threat Center, which analyzes over one billion emails globally each working day.

Attackers' efforts will likely focus on employees who continue to work at home, as well as on those now returning to the office. The unsettled circumstances surrounding another workplace transition will almost certainly create numerous opportunities for social engineering deceptions.

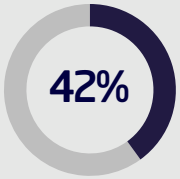
The chief deterrent will be the scope and depth of a company's cyber resilience strategy: Its ability to prevent and adapt to new types of threats and to quickly respond and recover from an attack. The good news is that, per our survey respondents, 44% of the companies surveyed already have a cyber resilience strategy in place. Moreover, these organizations are more confident in their ability to withstand an email-borne attack. Only 63% say that such an attack is likely, extremely likely or inevitable, compared with 76% of respondents from companies without a cyber resilience strategy

The converse is also true: 35% of respondents from companies with a cyber resilience strategy consider it unlikely, very unlikely or even impossible that their organization will be harmed by an email attack, while only 22% of respondents from organizations without a cyber resilience strategy feel that this is the case.

10,000+ Employees
consider an email attack to be:

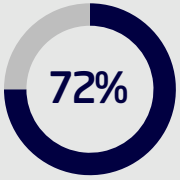


very likely/ inevitable

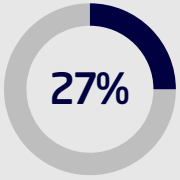


highly unlikely/ impossible

250 - 500 Employees
consider an email attack to be:



extremely likely/ inevitable



highly unlikely/ impossible

Larger companies are also more assured of their ability to ward off an email attack.

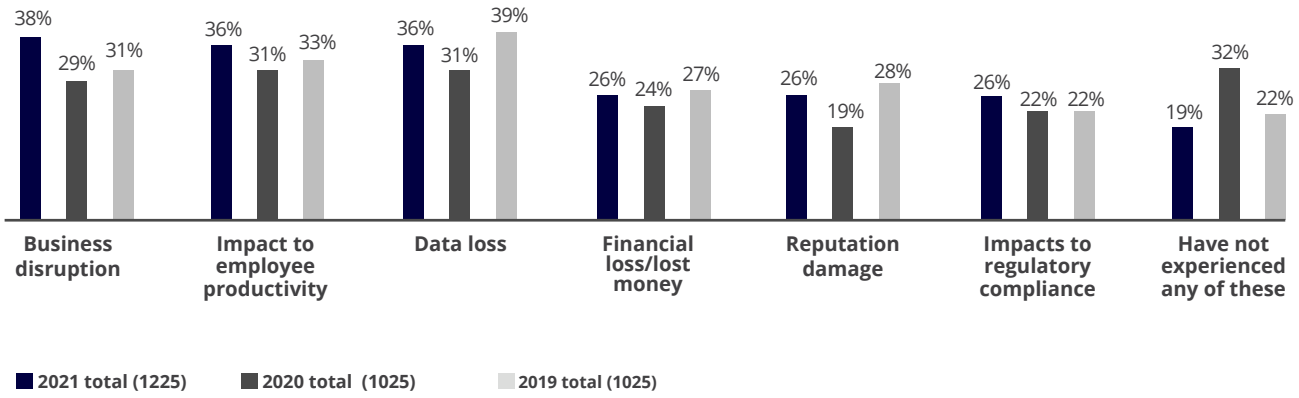
Among survey respondents from companies with 10,000 or more employees, only 54% regard such an attack as very likely or inevitable, and 42% consider it highly unlikely or impossible.

In comparison, 72% of respondents from companies with 250 to 500 employees believe an email attack is extremely likely or inevitable, while only 27% of them think it is highly unlikely or impossible.

Similarly, companies with a cyber resilience strategy were less likely to have been negatively affected by ransomware than those without a strategy (53% to 68%).

The less fortunate survey finding is that 79% of the SOES respondents acknowledge that their company experienced a business disruption, a financial loss or some other setback due to a lack of cyber preparedness. Unsurprisingly, given the intensity of the post-COVID threat climate, this was significantly higher than in prior years.

A lack of cyber resilience preparedness have impacted organizations more this year than in 2020.



What about the more basic question of whether or not a company has a dedicated email security system in place? Again, the SOES survey results present a mixed picture.

On the plus side, nearly all of the respondents (97%) indicated that they either had already deployed various email security systems, were in the process of rolling out such systems or were looking to do so. However, in each of four key areas of email security — monitoring internal email threats, monitoring outbound email threats, protecting against data exfiltration and removing malicious emails already in user inboxes — fewer than six out of 10 currently have safeguards in place, only 26% guard against all four — and 13% have no email security system at all.

Of those with some additional protections already deployed, many are making use of AI and machine learning to bolster their efforts (38% of total respondents.) And in keeping with the above, organizations with a cyber resilience strategy in force are much more likely to be using these technologies (50% of those with a strategy compared to only 29% of those without one.)

What about the more basic question of whether or not a company has a dedicated email security system in place?

13%

of companies still do not have an email security system

Microsoft 365

Many of those companies without dedicated email security appear to be relying entirely on the safeguards provided by Microsoft 365, and these protections are held in high regard by the large majority (81%) of our survey respondents. Yet nearly three-out-of-four (72%) also agree that there is room for improvement. That may be in part because two-thirds (67%) said their organization had experienced a Microsoft 365 email outage during the past 12 months, and nearly half (49%) characterized the impact as moderate to severe.

These findings help account for why, among the 1,175 SOES respondents who are Microsoft 365 users (96%), nearly nine in ten think their companies require additional layers of email security over and above the protections that Microsoft provides.

88% **of Microsoft 365 users think their companies need additional email security**

Respondents from the largest organizations (10,000+) and those within the public sector are the least likely to think that Microsoft 365 provides world-class email security.

Cybercriminals are well aware of this vulnerability and are taking advantage of pandemic-induced confusion and home office distractions to force more such errors. Sadly, it is paying off. As noted earlier, employees are clicking on three times as many malicious emails as they did before the pandemic began.

This state of affairs is reflected among the SOES survey respondents. Seven out of ten (between 69% and 75% depending on the specific behavior) believe that employee behaviors such as careless web browsing, oversharing of company information on social media, inadvertent data leaks and poor password hygiene are putting their companies at risk. And only one out of four (26%)—the lowest percentage since the SOES survey began in 2016—can say with any confidence that their organization has not been hit by an attack that spread from a compromised user to other employees.

7/10

respondents believe that employee behaviors such as poor password hygiene are putting their companies at risk

1/5

Ongoing cyber awareness training is only provided by 1 out of 5 companies

section

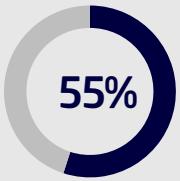
five.

Cybersecurity Awareness Training: More Critical Than Ever

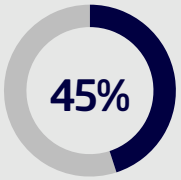
No matter how good employees are at their jobs, the biggest security risks at most companies arise from human error. This has been confirmed by researchers from Stanford University, which found that 88% of all data breaches are caused by employee mistakes.[3]

The situation is somewhat better among those companies where the volume of email increased over the past 12 months. Among this group, nearly half (49%) are providing ongoing or monthly awareness training, compared with fewer than a third (32%) of organizations where email levels remained steady or declined. Likewise, only 19% of companies where the use of email is increasing fail to offer awareness training, or limit it to a one-time event or a very occasional occurrence, in contrast to the more than one-third of companies (36%) where the volume of email has not increased.

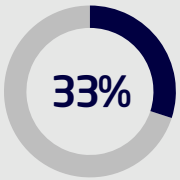
This less-than-optimal state of affairs is underlined by a 2020 Forrester research study, conducted in Australia, New Zealand, Hong Kong and Singapore. The APAC study, which was sponsored by Mimecast [4], found that when it comes to security training programs:



of organizations do not base their programs **off of data and behavioral science**



do not capture **feedback from employees**



do not **utilize metrics to monitor success**

With employees using their own devices for work and connecting through their own networks at home, regular cybersecurity awareness training is needed to cope with the greater prevalence of cyber risk in the work-from-home environment. This is especially true given the ever-more-sophisticated phishing attacks targeting employees, who tend to get more careless and therefore more susceptible to misdirection when they're distracted by a sometimes stressful home environment. Home network hygiene is critical, and employers must offer awareness training that is ongoing, engaging and uses encouragement—as opposed to fear—to instill new behaviors in employees.

section

six.

A New Urgency for Online Brand Protection

Online brand impersonation and exploitation is a serious danger facing many companies. And, as with other cyber risks, the COVID pandemic has amplified the extent of this threat.

Among the economic changes wrought by the pandemic, there has been a marked shift to conducting more business online. The perpetrators of cybercrimes have been quick to seize on this and have stepped up their efforts to defraud businesses and their customers through spoofing attacks. Per the SOES survey, incidents where the company's brand was impersonated or misappropriated to create a counterfeit website increased at 42% of the respondents' companies, while an even greater number (47%) reported a rise in malicious email spoofing that made fraudulent use of their company's domain.

The level of concern over these types of attacks has risen accordingly. More than nine out of 10 respondents (91%) say they would be concerned if a counterfeit website misappropriated their company's brand, compared with the 84% of respondents who felt the same way last year. Similarly, 93% of respondents would be greatly concerned if bad actors spoofed their company's email domain, versus 84% in the 2020 survey.

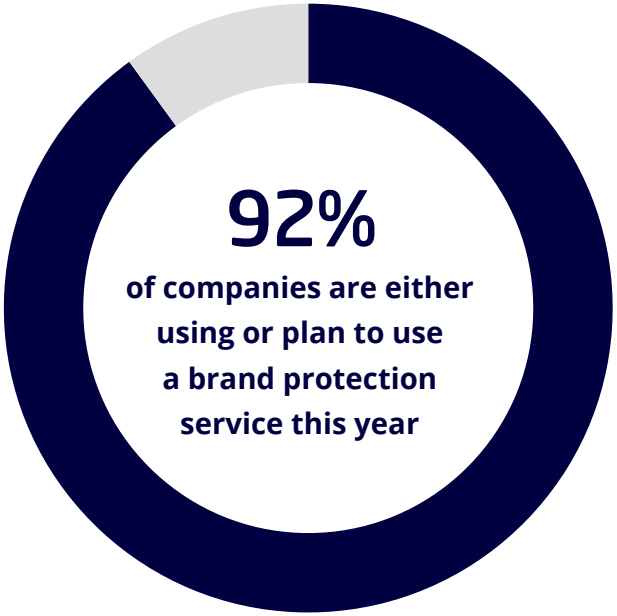
91%

of companies are concerned that counterfeit websites will misappropriate their brand

Spoofing attempts against corporate websites are a regular occurrence worldwide. Among SOES respondents, efforts to defraud their companies by either cloning their website or creating a lookalike web domain took place an average of nine times during the past year. **This happened most frequently in Germany, where companies spotted such scams an average of 14 times, and least often in the Netherlands, where companies identified brand-based fraud only five times on average.**

9x **average times a year**

efforts to defraud companies by either cloning their website or creating a lookalike web domain



There are encouraging signs that this level of apprehension is translating into tangible efforts to safeguard companies' brands. More than nine of 10 (92%) respondents report that their organizations are either making use of or have near-term plans to make use of a service to detect and protect themselves against counterfeit websites and other attempts to impersonate their brand. Of these, nearly 8 out 10 (77%) have already deployed such a service.

DMARC

To safeguard their brands, companies are also making use of Domain-based Message Authentication, Reporting and Conformance—better known as DMARC.

This email authentication protocol was developed to help determine whether a given email is legitimate and actually originated from within the domain with which it is associated. First published by the Internet Engineering Task Force in 2015, the protocol helps protect companies against domain spoofing.

DMARC allows an organization to set a policy that helps prevent spoofed email from reaching its employees, customers or other unsuspecting recipients. The policy instructs the recipient's email system how to respond to any emails that attempt to misappropriate the company's domain.

Per this year's SOES survey, more than eight out of 10 (85%) respondents indicated that their companies are already making use of DMARC (26%); are in the process of implementing the protocol (30%); or plan to do so over the next 12 months (29%).

8+ out of 10

companies are already **making use of DMARC** or plan to do so over the next 12 months

section

seven.

Top Ten Takeaways

This year's State of Email Security report contains a wealth of information and many important insights. But among its many lessons, these 10 stand out:

.01 The COVID threat landscape has become much more treacherous.

During 2020, email threats rose by nearly two-thirds as commerce became more dependent on email and bad actors seized on pandemic-induced disruptions to press their agendas. Seven of 10 companies are bracing for the worst and expect their business to be harmed by an email-borne attack.

.02 Phishing and BEC attacks are more insidious than ever.

Since the pandemic began, phishing attacks have surged by 63% as malefactors play on COVID-related fears and target employees who are often distracted by their new work-at-home environments. The results are painful, as employees have been duped into clicking on three times as many malicious emails as they used to.

.03 While beneficial to business, collaboration tools represent increased security risk.

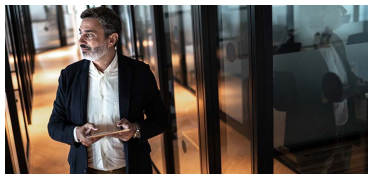
Given global restrictions on travel and in-person meetings, nearly all companies are now using collaboration tools like Slack and Microsoft Teams for team building and to coordinate projects. Useful as they are, these tools pose their own set of cybersecurity challenges, and more than two-thirds of the SOES respondents are concerned about the risks.

.04 Ransomware is everywhere.

More than six out of 10 companies were disrupted by a ransomware attack last year, losing six days of work on average. Among the businesses that were affected, more than half felt compelled to pay the ransom but only two out of three of them recovered their data. The other third never saw their data again—despite paying the ransom.

.05 Cyber preparedness is wanting at too many companies.

These are heavy statistics: By their own acknowledgement, in 2020, nearly eight in 10 companies had their business disrupted, incurred a financial loss or suffered some other setback due to their lack of cyber preparedness. Even worse, email security at more than 40% of businesses falls short in one or more critical areas, and 13% of businesses don't have an email security system at all. Given the post-COVID threat level, this state of affairs is no longer sustainable.



.06 Microsoft 365 security is good - but a layered defense is much better.

Many businesses rely on the safeguards provided by Microsoft 365 to keep their email secure, and these are well regarded. Nevertheless, nearly nine in 10 companies strongly believe they need additional layers of email security over and above what Microsoft provides.

.07 Cybersecurity technologies will increasingly incorporate AI and machine learning.

More than a third of companies are making use of AI and machine learning to bolster their cyber defenses. This is even higher among companies that have a cyber resilience strategy in place. It's still early days for these technologies and their application to cybersecurity, so mark this as a rising trend—one that's sure to play out more fully in the months and years ahead.

.08 Cybersecurity awareness training needs to be a bigger priority.

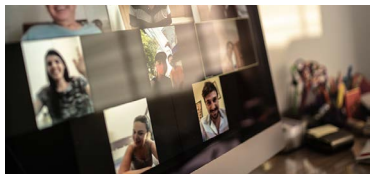
Although seven out of 10 companies believe employee behaviors such as careless web browsing and inadvertent data leaks are putting them at risk, fewer than half provide ongoing cyber awareness security training at least once a month, and one in five provide little or no training. Yet studies have shown that awareness training is a low-cost and highly effective means of reducing an organization's cyber risk. Giving higher priority to cybersecurity training would benefit a great many businesses.

.09 Spoofing and brand impersonation represent a new front in the cyber wars.

By their own admission, nine out of 10 companies are threatened by online brand impersonation and misappropriation, putting their customers, their finances and their reputations at risk. Luckily, the great majority of businesses are fighting back and enlisting specialized services to detect and defend against counterfeit emails and websites.

.10 Cyber resilience pays off.

A cyber resilience strategy that helps a business adapt and respond to new threats is clearly paying dividends to those that have one in place. Such companies are more confident in their ability to withstand and prevent an email-borne attack and are less likely to be hindered by one. They are also much less likely to be disrupted by ransomware, are far more likely to have implemented DMARC to safeguard their brand and are far more likely to have incorporated AI and machine learning into their defenses than those without a strategy.



section

eight.

In 2020, companies and their cybersecurity teams worldwide confronted a digital pandemic of email-borne malware, phishing attacks and ingenious uses of social engineering to compromise their systems. Bad actors were quick to capitalize on the chaos created by a global contagion, targeting millions of suddenly remote and disoriented workers.

The Bottom Line

To their credit, many organizations rose to the occasion, increasing their cybersecurity budgets and adding to their security staffs—even as their revenue in many cases was falling. Moreover, a notable minority have a cyber resilience strategy in place, allowing them to lay the groundwork for more formidable defenses.

Much work, however, remains to be done: Expectations of a damaging email attack among survey respondents remain high; many employees are still ill-equipped to recognize and cope with a cyberattack, while far too many companies still lack basic email protections.

To meet these and other challenges, cyber preparedness is key, and the importance of a cyber resilience strategy cannot be overstated. Likewise, it stands to reason that companies using advanced technologies such as AI and layered email defenses—while also regularly training their employees in attack-resistant behaviors—will be in the best possible position to sidestep future attacks and quickly recover.

mimecast®

Relentless protection. Resilient world.™

1. “2021 Global Digital Trust Insights,” PwC
2. “Gartner Says 69% of Boards of Directors Accelerated Their Digital Business Initiatives Following COVID-19 Disruption,” Gartner
3. “Human Error Is Still the Cause of Most Data Breaches in 2021,” Influencive
4. “Designing Effective Security Awareness & Training Programs in APAC,” Forrester

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Mimecast’s expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure.