The State of Email Security 2020

Email security insights at your email perimeter, inside your organization, and beyond

mimecast™

Contents

A guide to the email galaxy

1

Global business is interspersed with a diversity of industrial sectors, united by a single, common communication thread that is key to any business: email connectivity.

Email continues to be the most popular attack vector, via organizations at their email perimeters, from inside the organization (through compromised accounts, vulnerable insiders, social engineering), or beyond the organization's perimeters (the domains they own and their brands via impersonation).

Cyber threat actors and threat groups are continuously researching and testing out new tactics, techniques, and procedures (TTPs) in an attempt to overcome and exploit this increasingly sophisticated and complicated technology.

To add to the complexity, many global corporations have been forced to adopt remote working policies for office-based employees to help ensure the safety of the workforce during the COVID-19 pandemic, and threat actors have followed them home. An increase in the variety and volume of attacks is inevitable given the desire of financially- and criminally-motivated actors to obtain personal and confidential information.

The fourth annual State of Email Security (SOES) contains the valuable insights, reference points, and key takeaways that you've come to rely on for your organization. And with the depth of knowledge acquired over years of monitoring and analyzing the email security landscape, in conjunction with Mimecast's analysis using detection data during the first 100-day period of coronavirus, SOES 2020 serves as the guide helping to drive continuous improvements to your cyber resilience strategy.

The state of the world in the first half of 2020 is unlike anything we have experienced before, and it's trickled down to have an impact on the IT and security world. As healthcare providers and other essential employees worked as hard and as quickly as possible to contain and mitigate the impact of the COVID-19 pandemic, threat actors undermined and stole from businesses, charities, and governments. Threat actors, who are resourceful and inventive, regularly exploit times of confusion or global events to conduct cyberattacks and email phishing campaigns. They assess how well organizations secure their networks to identify vulnerabilities in infrastructure and defenses, which they use to improve their attack methodologies.

While world leaders, business leaders, and individuals come to an understanding of how deeply this pandemic has affected us and will continue to do so, this report will also share theories and information on how the pandemic has changed the landscape of email security in 2020.

Report methodology

Research firm **Vanson Bourne** conducted a Mimecast-commissioned global survey of 1,025 IT decision makers to gain useful insights into their experiences and outlook on the current state of email security. These participants were interviewed from February 2020 through March 2020 across the U.S., UK, Germany, Netherlands, Australia, South Africa, United Arab Emirates (UAE), and Saudi Arabia. This research was supported by our own expertise, screening more than 1 billion emails a day.

The report highlights the following key findings, along with prescriptive guidance for how to evolve your cyber resilience program.

Key findings over the previous 12 months

51%
have been impacted by ransomware in the past 12 months

77%
believe weak passwords pose a risk of a serious security mistake

58%
saw phishing attacks increase

31%
say they experienced data loss due to lack of cyber resilience preparedness

60%
experienced an increase in impersonation fraud in the last year

82%
have experienced downtime from an attack

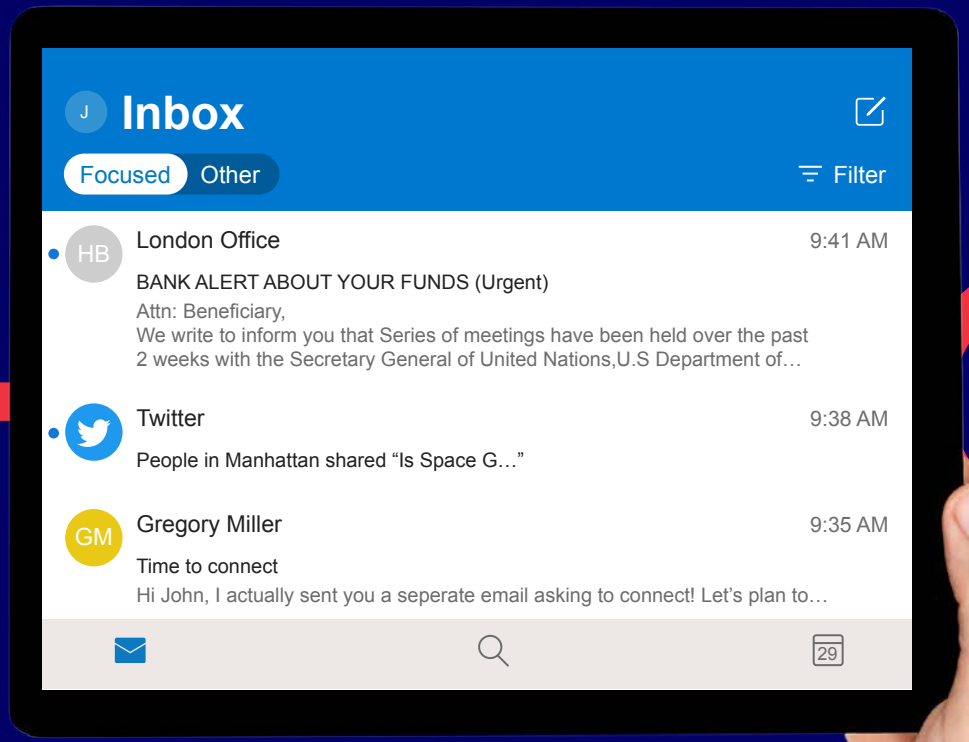
55%
do not provide awareness training on a frequent basis

85%
believe their organization's volume of web or email spoofing will remain the same or increase in the coming year

60%
of respondents' organizations were hit by an attack spread from an infected user to other employees

Email-borne attacks, and why they aren't decreasing

2



2 Email attacks, and why they aren't decreasing

Four years in, the State of Email Security Report provides a snapshot of how email attacks, from phishing and business email compromise (BEC) to ransomware and internal email threats, rise and fall based on threat actors' latest strategies. In 2020, threats are impacting organizations at every level.

After years of frightening narratives and countless examples, the data points to a broad understanding of the potential risk for email-borne attacks – in other words, sophisticated attacks that arrive inside your environment via the email perimeter.

Some 60% of organizations believe it's inevitable or likely they will suffer from an email-borne attack in the coming year. Due to the depth of this data and its cross-section across sector and nation, it appears that Saudi Arabia – and its primary source of income[1], the oil and gas industry – are on especially high alert.

[1] OPEC, about Saudi Arabia

74% of Saudi Arabian businesses and 73% of leaders in the oil and gas industry globally believe it is inevitable or likely they will suffer negative outcomes from an email-borne attack this year.

Impersonation fraud, business email compromise, and email phishing

Was BEC actually all over the news in the last year, or did it just seem like it? Some could argue the former.[2] You may be asking yourself why this is a critical issue if you have the right cyber resilience strategy in place to prevent these attacks from happening, but the nature of BEC – and impersonation fraud overall – is its ability to bypass spam and AV filters due to a dearth of malware or malicious URLs.

Three-quarters (74%) of respondents had seen impersonation fraud increase or stay the same; this represents a decrease from 78% in 2019. Yet, a review of Mimecast's global customer threat intelligence data highlights the fact that impersonation fraud **increased** by 30% in the first 100 days of COVID-19.[3] How can we justify and understand this delta? Here's one way. Governments worldwide are cautioning against a broad increase in impersonation; in fact, in the U.S. the FBI warned that BEC is expected to increase[4] due to threat actors' ability to take advantage of the global pandemic.

Analysts from the Mimecast Threat Center assess factors like seasonality, or a change in threat actors' tactics, accounts for the minor fluctuations in impersonation, year on year. What remains the same, however, is the use of pattern-of-life analysis to track social media sites, such as LinkedIn, to target individuals within organizations who may have access to executives and financial systems.

When it comes to phishing more generally, 72% of respondents stated it remained flat or increased in the last 12 months at their organizations, a jump from 69% in 2019. And, it's potentially becoming more difficult to stop or prevent due to more advanced tactics like spear-phishing, which increase the cyber threat actors' probability of success, up to 75%.[5]

Increase of impersonation fraud in the first 100 days of COVID-19

30%

[2] BEC Attacks Are Now the Top Cause of Payment Fraud, Cyber Resilience Insights
[3] 100 Days of COVID, Mimecast Threat Center
[4] FBI.gov
[5] What You Can Learn from Our Successful Simulated Phishing Attack of 45 CEOs, Rapid7

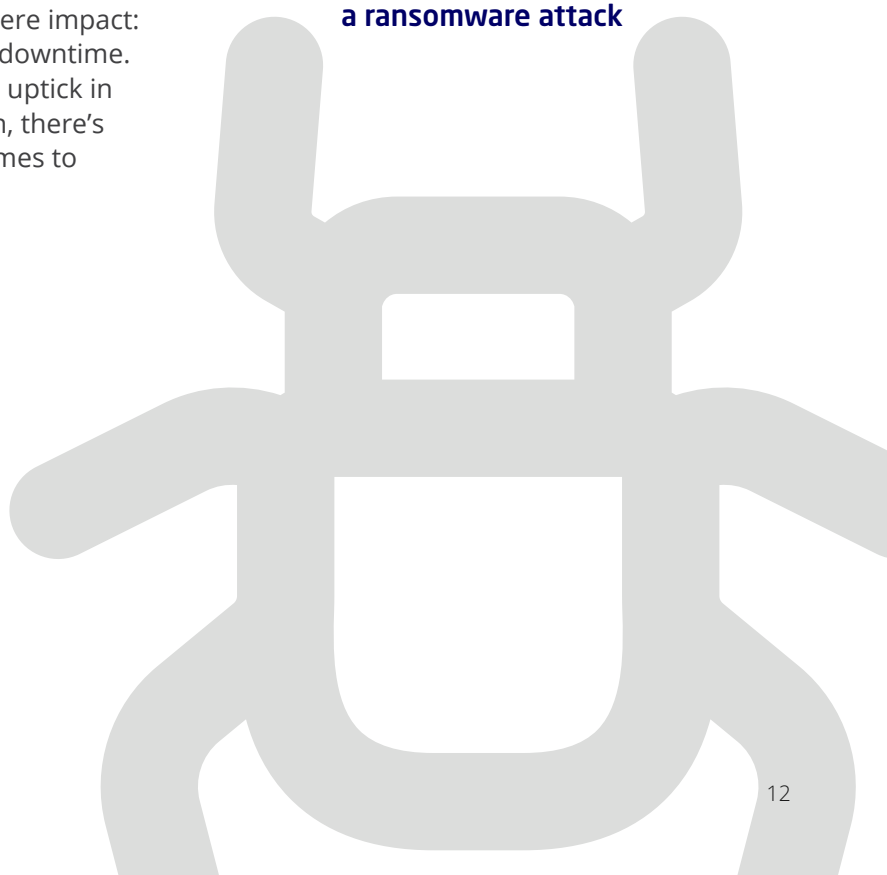
Ransomware

The last 12 months were plagued by high volumes of ransomware targeted at both the private sector and the public sector; indeed, the severity of the 2019 Baltimore municipality ransomware attack[6] serves as a lasting reminder of the need for a layered approach to security. However, organizations of all stripes face ransomware attacks – and downtime as a result – nearly every day.

According to just over half of respondents (51%), ransomware attacks impacted their businesses in the last 12 months, and by now, we know that data loss, downtime, and loss of reputation or trust among customers typically accompany the financial losses. The same is true in this year's research: of those who experienced a ransomware attack, they faced 3 days of downtime, which is consistent with the 2018 and 2019 reports, as well as across nearly every sector surveyed. Despite these losses, organizations tend to expect a less severe impact: they reported expecting just 2 days of downtime. This gap suggests that while we see an uptick in understanding the need for prevention, there's still room for improvement when it comes to planning for ransomware resilience.

3

days of downtime on average when hit with a ransomware attack

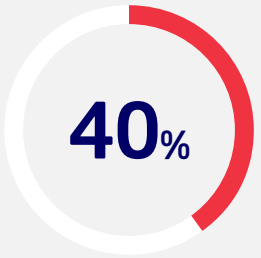


[6] Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts, Baltimore Sun

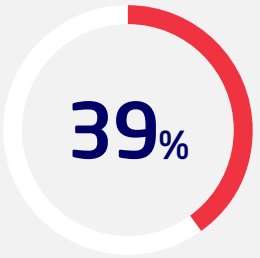
Attack aftermath

All too often, when organizations fall victim to an email-borne attack, it can be a herculean effort to fully recover. Nearly a third of respondents experienced data loss (31%), impact to employee productivity (31%), and business interruption/ downtime (29%) due to a lack of preparedness.

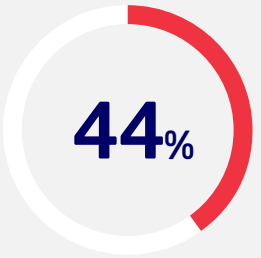
But there's a solution here, particularly for respondents who indicated being impacted by phishing, impersonation fraud/BEC, or ransomware. What happens after an attack is important. Email threats aren't decreasing, so it's critical for organizations to implement a security system for protection against data leaks in internal-to-internal emails, data leaks or exfiltration in outbound email, and malware or malicious links in outbound email. On average, 6 in 10 organizations state they have some kind of security system to protect their data or employees in internal and outbound emails.



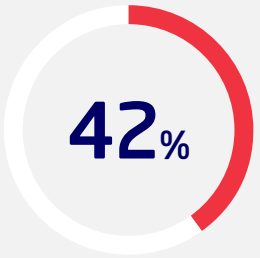
Do not have a system for monitoring and protecting against email-borne attacks or data leaks in internal emails.



Do not have a system for monitoring and protecting against email-borne attacks like malware and malicious links in outbound email.



Do not have a system for monitoring and protecting against data leaks or exfiltration in outbound email.



Do not have a system for automated detection and removal of malicious or unwanted emails that have already landed in employees' inboxes.

90%

UAE organizations have a system or are rolling one out

Some countries, it turns out, are taking certain security systems very seriously.

90% of United Arab Emirates (UAE) organizations say they have a system or are actively rolling one out for monitoring against email-borne attacks like malware and malicious links in outbound email, as well as a system for automated detection and removal of malicious or unwanted emails that have already landed in employees' inboxes.

How security awareness training closes the understanding gap

3

3 How security awareness training closes the understanding gap

Email-borne attacks can also disrupt business inside the organization and network, brought on by internal data leaks and human error. In fact, human error plays a role in half of the world's data breaches,[7] as employees are considered a contributing risk factor to cyberattacks. Even the most robust perimeter-based security system isn't helpful if attackers are able to penetrate your network and operate there, undetected.

It's everyone's responsibility within an organization, from the CEO down, to remain aware of current threats and cyber vectors used to attack an organization. So, if employees are expected to be "the human firewall" or "the last line of defense," as they are often referred to, organizations need to invest in them as such.

What's needed is a frequent, consistent, engaging cybersecurity awareness training program, but only about 1 in 5 respondents (21%) offer training on a monthly basis – a timeframe experts consider the gold standard.

Perhaps even more shockingly, 17% are only trained once per year, a rate that neglects to foster a comprehensive security culture throughout the organization. If there is not a clear cyber resilience or mitigation culture within an organization, vulnerabilities may develop which could be exploited. To be truly successful, security awareness training programs need to meet three criteria as outlined by Forrester Research:[8]

Three criteria to security awareness training programs

Foster a security culture rife with empathy and encouragement, instead of obligatory (or boring!) training and testing.

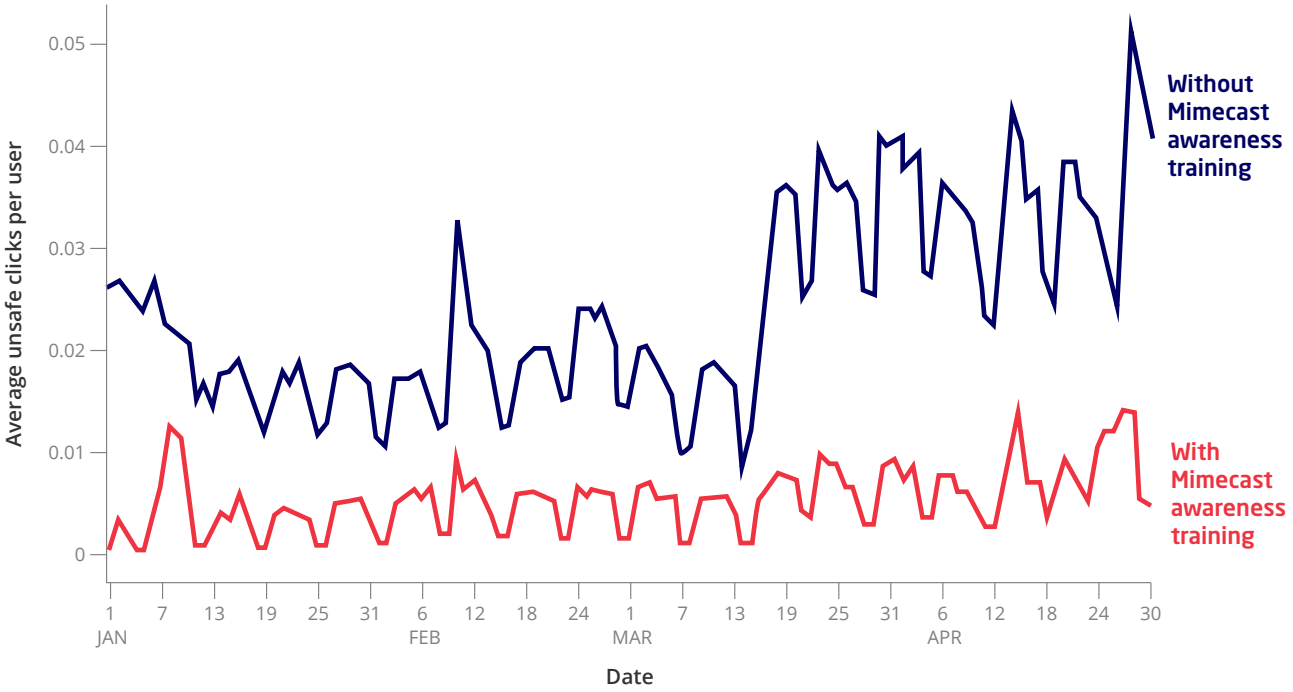
Use engaging, inclusive images and messages to encourage active participation.

Take a global view and make training culturally relevant to each region.

[7] Cost of a Data Breach 2019, IBM & Ponemon Institute
[8] The Forrester Wave™: Security Awareness and Training Solutions, Q1 2020

3 How security awareness training closes the understanding gap

With these criteria, employees can make their training stick, playing an active role in their organization's cybersecurity posture. However, the effects of infrequent or monotonous security awareness training can have far-reaching consequences. In fact, researchers found that employees from companies not using Mimecast Awareness Training were more than 5X more likely to click on malicious links than employees from companies that did use the training.[9] The rise in unsafe clicks suggests the need to refresh awareness training for employees and create a more secure working environment.



Employees from companies not using Mimecast Awareness Training were more than

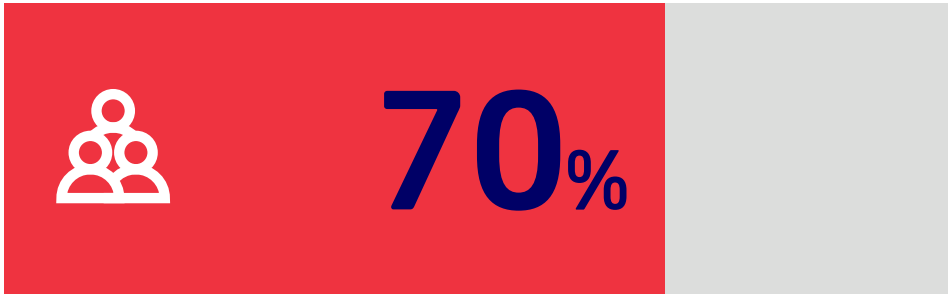
5X

more likely to click on malicious links

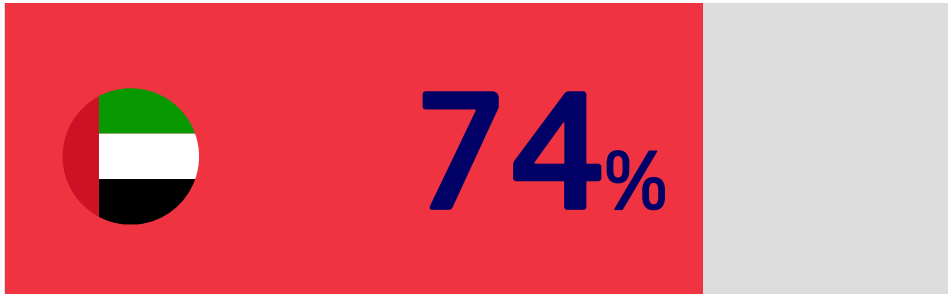
[9] Threat Intelligence Briefing: Security Awareness Training Dramatically Reduces Unsafe Clicks Amid Surging Coronavirus Cyber Threats, Cyber Resilience Insights

Additionally, in 2020, 60% of survey respondents reported having been hit by malicious activity spread from employee to employee.

The IT, telecoms and technology sector reports that 70% have been hit by malicious activity spread amongst employees.



Saudi Arabia and UAE both report higher numbers of threats spread internally at 84% and 74%, respectively.



Respondents believe there is a high level of risk of employees making a serious mistake; for example, 77% believe poor password hygiene poses a risk, and 75% point to inadvertent data leaks as a high risk.

How to close the security awareness gap

Overall, organizations are taking security awareness training more seriously; security awareness training has a high level of awareness (no pun intended) for its success rate. In fact, nearly all of respondents' organizations (97%) offer some kind of training at varying frequencies and formats. About 6 in 10 offer group training sessions, while around 4 in 10 offer various other types like online tests, emailed or printed tips, or 1:1 training.

Respondents told us they offer training that was developed in-house, which can lead to infrequent or inconsistent training modules. Just 23% are using training videos, and barely 1 in 5 (18%) use a single third-party provider.

With frequent, consistent, engaging content that humanizes security, security awareness training is an effective way to reduce risk inside the network and organization.

55%

of public sector/education sector respondents rely on trainings developed in-house due to cost.

33%

of respondents from the energy, oil and gas sector rely on in-house trainings, indicating an effectively trained workforce.

The new mandate: online brand protection

4

In today's global business environment, the only guarantees are risk and uncertainty.

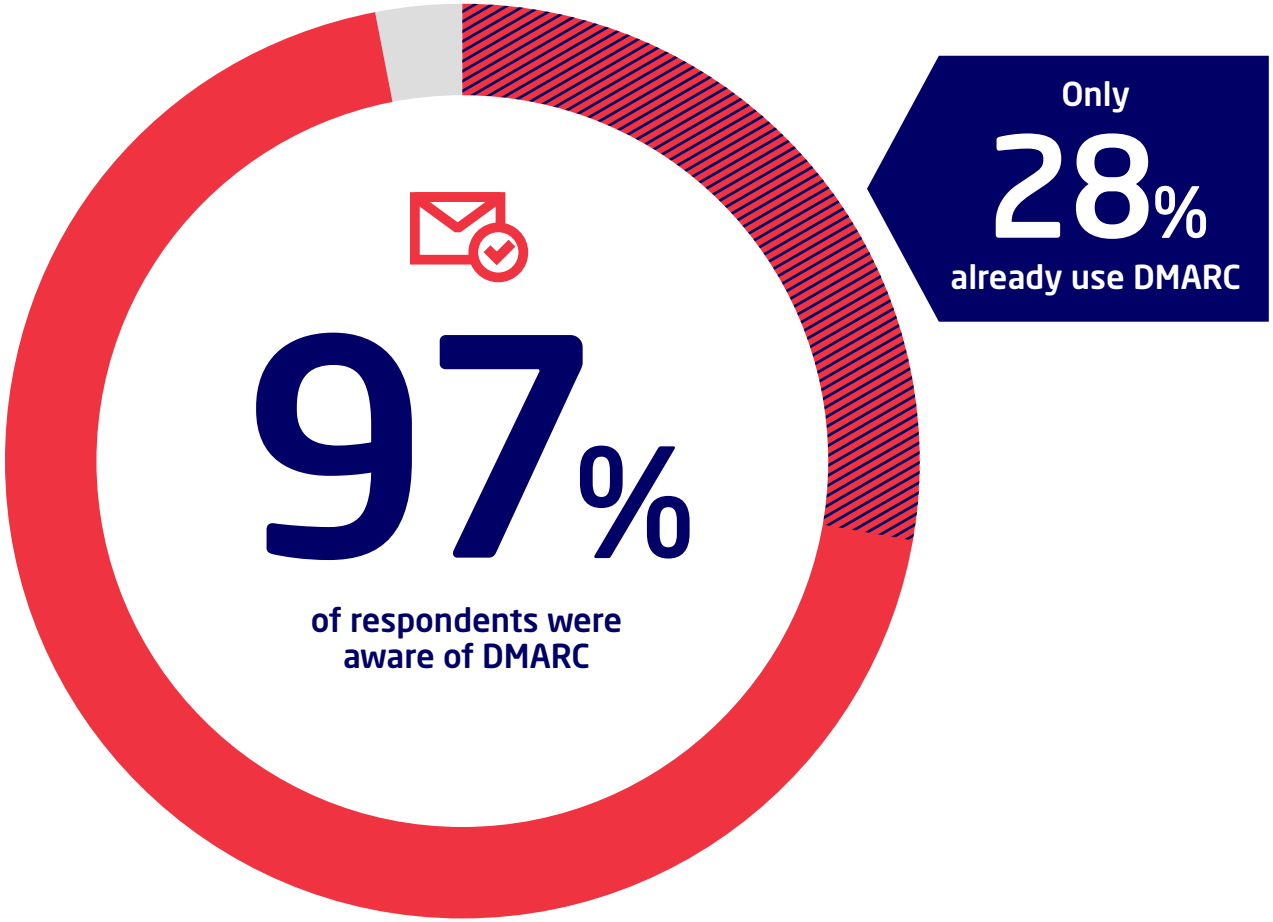
And as domain-spoofing and email-spoofing have evolved to become mainstream attack vectors, particularly during the global COVID-19 pandemic, it's critical for organizations to look beyond their email perimeters to determine how cyber threat actors may be using and damaging their brands online.

Brand trust is incredibly important; if your brand website is cloned and credentials were stolen as a result, then trust in your brand is already in question. Even unsophisticated attackers can trick unsuspecting website visitors, which can unravel years' worth of brand equity. And if you're unaware it's happening, you can't solve the problem.

DMARC and brand protection

Domain-based Message Authentication, Reporting & Conformance, or DMARC, is an email validation system designed to uncover anyone using your domain without authorization, and ultimately block delivery of all unauthenticated mail. There are positive implications for both email senders and email receivers too: on the sender side, the DMARC system helps protect customers and supply chain by monitoring who's sending email on your behalf, and on the receiver side, it protects employees by distinguishing between legitimate and fraudulent senders.

There's high awareness around DMARC and its role in helping to secure email from threats like spam, phishing, and email spoofing.



Brand protection in the C-suite

But while online brand protection has emerged onto many companies' radars in the last two years, it's still not quite risen to boardroom importance.

The KrebsOnSecurity analysis of the global top 100 companies by market value[10] showed that just 5% of companies listed their CSO or CISO among the executive team; these roles usually report to CIOs due to executive silos. But given the importance of financial data managed by the CFO, employee data handled by the CHRO, or intellectual property managed by the CPO, shouldn't the security of the brand be elevated into the executive level?

In any case, the good news is there's widespread visibility into budgeting for brand protection; 98% of respondents reported their organization has a dedicated budget for online brand protection strategies. On the flip side, if this budget isn't allocated properly – for example, with oversight and partnership from a security-savvy C-suite officer, there's potential for a delayed attack response.

In 50% of organizations, the CIO holds budget for email spoofing, exploitation and impersonation, followed by the CISO (42%), CFO (22%), CMO (8%), and legal/compliance (8%). This budget breakdown is a heartening one – some organizations are treating online brand protection as the cross-functional business issue that it is, instead of relegating it as an overly technical security matter.

With this in mind, it's imperative that CISOs and CFOs partner to manage corporate brand. CFOs – while not usually known for their keen sense of cybersecurity – are perhaps best suited to make decisions that keep their business stable and operationally healthy. Working in lockstep with the CISO or CIO, the CFO can guide risk management and budget management towards a balanced approach to brand protection.

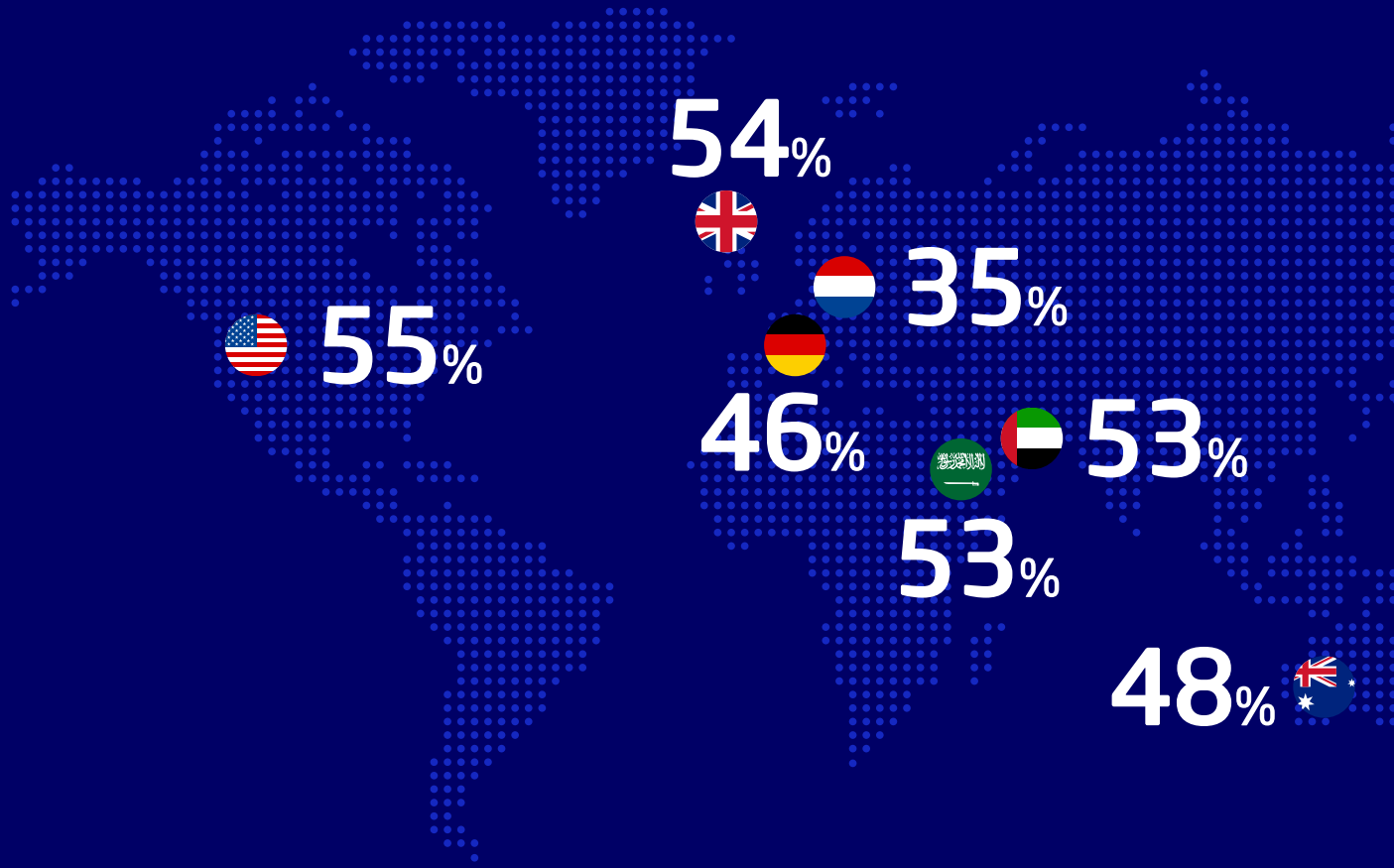
It's much more likely for CFOs in Saudi Arabia, UAE, South Africa, and the Netherlands to manage budget for corporate brand at 48%, 34%, 39%, and 36% respectively.

[10] A Chief Security Concern for Executive Teams, Krebs on Security

Web and email spoofing

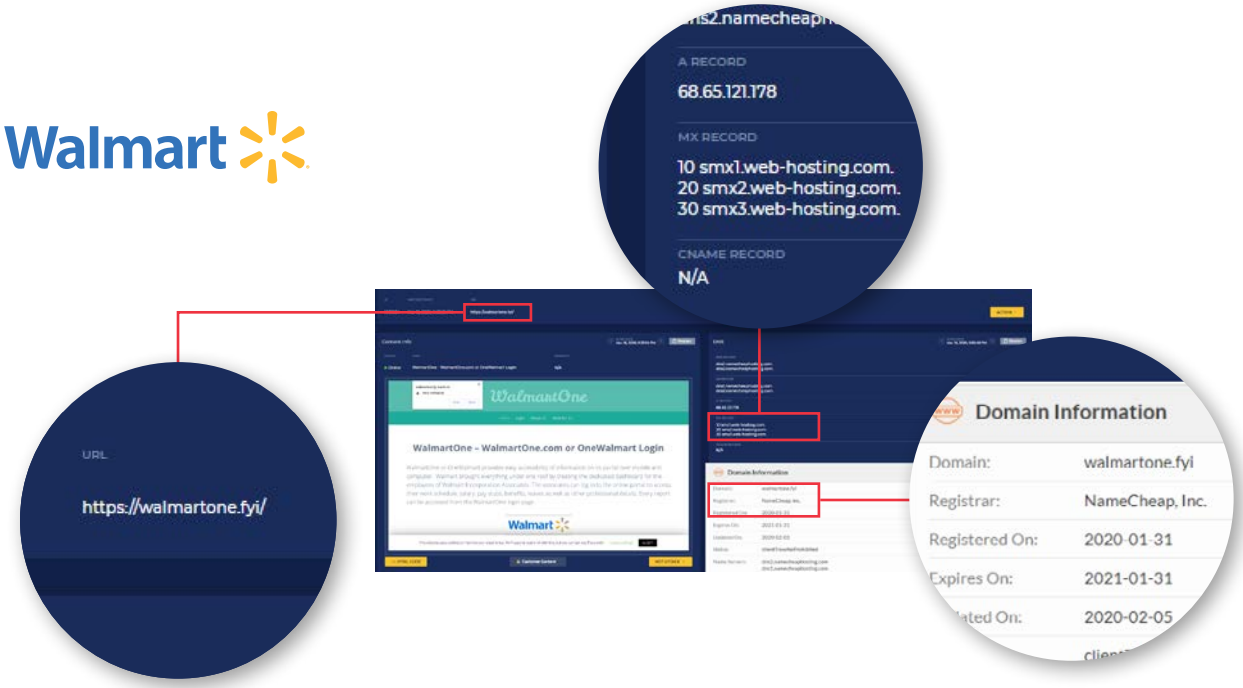
Nearly half of organizations (49%) surveyed report anticipating an increase in web or email spoofing and brand exploitation in the next 12 months, yet 84% report feeling concerned about a web domain, brand exploitation, or site spoofing attack. The same 84% are concerned about an attack that would directly spoof their email domain.

In fact, these concerns are justified: there are numerous reported web and email spoofing attacks, and on average, organizations have been made aware of 9 web or email spoofing attacks in the last year. This doesn't show the whole picture; there could be many more. After all, unless you're actively looking for these exploits, or unless someone takes the time to report them to you, they're difficult to find as they often don't arrive to your organization.



- **All regions expect web and email spoofing attacks to increase in the coming year, with the U.S. (55%), Saudi Arabia and UAE (53%), and UK (54%) on the highest alert.**
- **In the US the average goes up to 11, followed by Germany and the UK, both at 9 average attacks in the last year.**

This high level of concern from respondents may be indicative of a stronger understanding of the threat landscape, the diverse number of cyber threats to organizations, or the strong certainty of attack. The Mimecast Threat Center has seen countless incidents of brand exploits in the first few months of 2020 due to the COVID-19 pandemic. For example, the retail sector was heavily targeted with spoofing of major retail brand domains that preyed on insecurities around product shortages.



Is cyber resilience improving?

5

In 2019, 75% of respondents either had a cyber resilience strategy or were actively rolling one out. This year, it's gone up to 77%, and email security (71%), network security (66%), web security (63%), and data backup/recovery (62%) are once again the most common components of a cyber resilience strategy. Just over a third (34%) included brand exploitation protection for email-spoofing and website-domain spoofing, while 39% noted their strategies included penetration testing for key systems and regularly testing incident response processes.

Yet, 1 in 5 respondents are planning to implement a cyber resilience strategy at some point in the next 12 months or beyond, begging the question: why hasn't one been implemented yet? Given the data indicates that organizations are still seeing data loss (31%), a negative impact to employee productivity (31%), and business downtime (29%) due to a lack of cyber resilience preparedness, a cyber resilience strategy seems prudent.

While cyber resilience strategies vary from organization to organization – and certainly they differ across sectors depending on the regulatory or industry needs – they reflect a sense of awareness and preparedness about what threats might come their way. This year, the data suggests a high level of confidence in the respondents' cyber resilience strategies, but it also shows a clear need for improvement given we're still seeing significant levels of data loss and downtime.

Who should take responsibility and ownership of cyber resilience? It's a complicated question, and unfortunately there is no one-size-fits-all plan. However, it is cross-functional, meaning the CIO or CISO shouldn't hold sole ownership, so we should treat it as such. Cyber resilience is a risk management issue, and much like budget ownership for online brand protection, organizations should guarantee a partnership between senior leadership functions to ensure success.

The financial services industry appears to be the most stacked: organizations in this sector stand out by having not just the highest rates of foundational protections like email, network, and endpoint security, but also internal email protection (68%), penetration testing of key systems (53%), brand exploitation protection (41%), and security orchestration, automation and response, or SOAR (37%). The Mimecast Threat Center assesses this is a necessary development; as attacks have become more opportunistic and sophisticated, alongside the increasing threat of ransomware, the financial services industry will need extremely comprehensive measures in place for security – and business continuity.

The healthcare industry stands out for its dedication to security from inside the network. It exceeded industry averages with strong implementations of internal email protection (71%), user awareness training (63%), and web security (73%).

31% of organizations are seeing

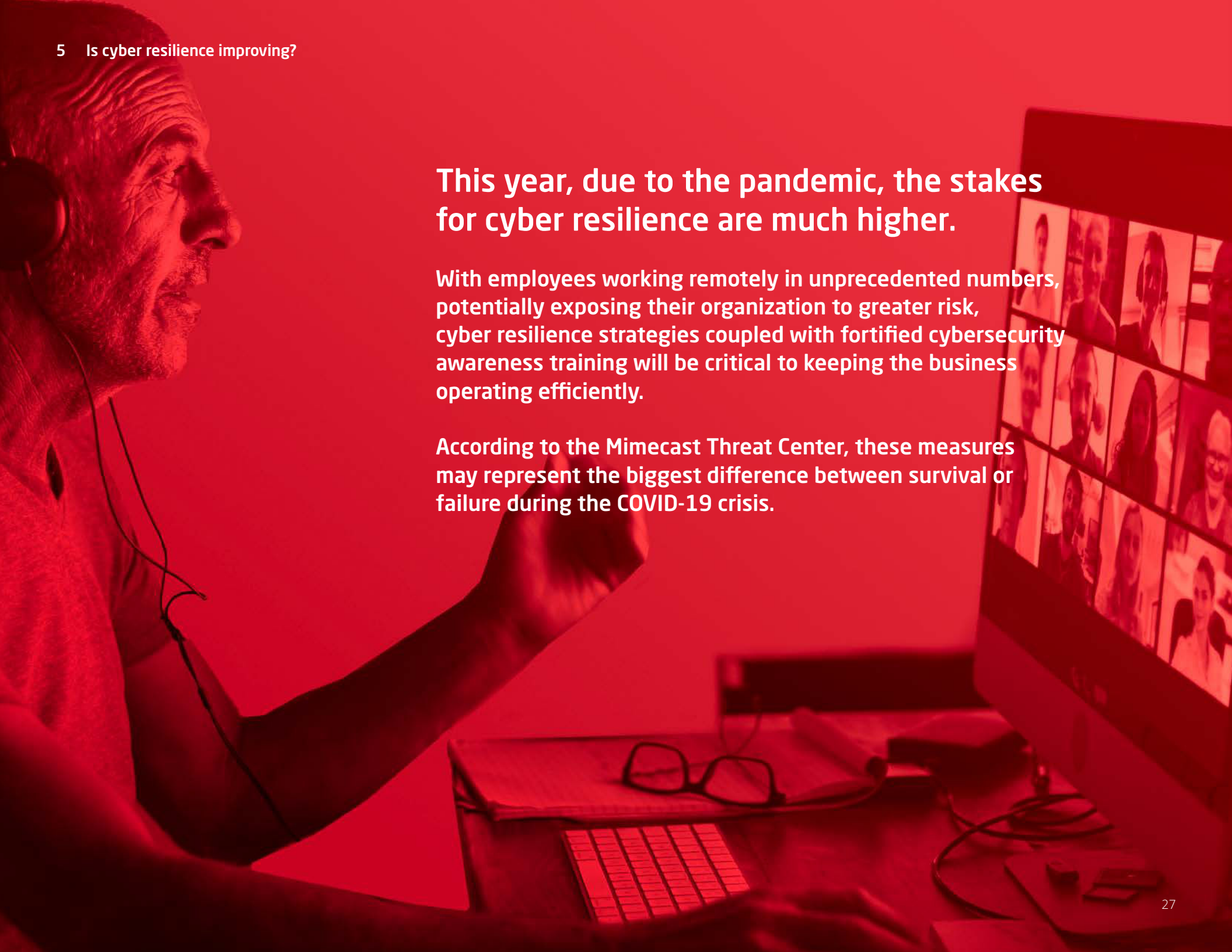
Data loss

31% of organizations are seeing

Negative impact to employee productivity

29% of organizations are seeing

Business downtime



This year, due to the pandemic, the stakes for cyber resilience are much higher.

With employees working remotely in unprecedented numbers, potentially exposing their organization to greater risk, cyber resilience strategies coupled with fortified cybersecurity awareness training will be critical to keeping the business operating efficiently.

According to the Mimecast Threat Center, these measures may represent the biggest difference between survival or failure during the COVID-19 crisis.

Microsoft 365 and a layered security approach

As more users move to cloud-based email, they experience the benefit of predictable costs, better collaboration, a simplified infrastructure, and critical services like data protection. But on the security front, when a popular platform like Microsoft 365 is missing necessary security layers, users may receive emails that should otherwise have been held. There can also be challenges with business continuity; if there's even a short outage, users are more likely to bypass corporate security with personal email accounts to conduct business.[11]

According to 96% of respondents at small- and medium-sized businesses, as well as enterprises, the overwhelming choice for email provider was Microsoft 365. However, there's room for improvement when it comes to security and resilience: only about 1 in 5 (22%) agree that Microsoft 365 provides world-class security for their organizations. Meanwhile, 59% of respondents experienced a Microsoft 365 outage in the last 12 months. At present there is no in-built, or inherent business continuity, within Microsoft 365 services should there be an interruption to Microsoft cloud services via common attack methodologies, such as a DOS attack, a datacenter hardware failure, or other form of interruption in relation to their cloud services.

With the number of outages occurring, 65% of respondents state they have already added or are in the midst of adding additional layers of continuity and cyber resilience.

59% of respondents experienced a Microsoft 365 outage in the last 12 months

[11] Top 5 Reasons to Build Cyber Resilience Into Office 365 Email, Cyber Resilience Insights

Top ten takeaways

6

Leaders are beginning to understand the email perimeter is constantly under attack.

The magnitude and scale of possible attacks at the email gateway is of concern to most; 60% of respondents believe it's inevitable or likely they will suffer from an email-borne attack in the coming year.

1

Impersonation, phishing, and business email compromise are increasing at a concerning clip.

72% of respondents saw an increase in phishing at their organizations, and due to the global pandemic, threat actors are broadly using impersonation and BEC to steal from unsuspecting users. The Mimecast Threat Center corroborated this assessment – researchers saw a staggering 30% jump in impersonation from January to April 2020.

2

The effects of ransomware still aren't improving year over year.

More than half of respondents experienced a ransomware attack this year, and in 2018, 2019, and 2020 respondents experienced an average of 3 days of downtime.

3

Monthly security awareness training is the best way to train employees, but it's not happening.

21% of respondents offer training monthly, and most organizations aren't educating employees according to best practices.

4

In the absence of security awareness training, unsafe URL clicks and data leaks will ensue.

Mimecast Threat Center found that employees from companies not using Mimecast Awareness Training were more than 5X more likely to click on malicious links than employees from companies that did utilize the training. The risk these clicks pose is significant: 60% of respondents were hit by malicious activity spread from employee to employee.

5

Looking beyond your email perimeter towards online brand protection is a business issue that can no longer be ignored.

There's high awareness of the need to protect your online brand and maintain customer trust, but just because the attacks aren't visible to you, doesn't mean they're not happening. 97% of respondents are aware of DMARC, but it's just one piece of the brand protection puzzle.

6

Budget ownership for online brand protection may shed light on how quickly an organization can respond to an attack.

Nearly all organizations – 98% - have a dedicated budget for email spoofing, exploitation and impersonation. Who manages the budget, whether it's the CIO, CISO, CFO, CMO, can vary; what's critical is the partnership between the budget owner and a savvy cybersecurity leader that leads to the right knowledgebase and tools investment to detect and respond to brand exploit.

7

You're right to have growing concern about web and email spoofing.

On average, there are 9 web or email spoofing attacks per organization each year – and that's just what they know about. 49% of respondents anticipate an increase in web or email spoofing in 2020, and the majority (84%) are concerned about direct brand exploitation or email domain spoofing attacks.

8

If there's one thing we all agree on, it's that cyber resilience strategies are necessary but still incomplete.

More than three quarters (77%) have a cyber resilience strategy or are actively rolling one out, and respondents told us their strategies are stacked with email security, network security, web security, and data backup and recovery solutions. But respondents are still experiencing data loss (31%), a negative impact to employee productivity (31%) and business downtime (29%) due to a lack of cyber resilience preparedness.

9

When it comes to delivering world-class security, Microsoft 365 needs more cyber resilience.

While 96% of respondents use Microsoft 365 for email delivery, the impact to their organizations following an outage or other security event created a lasting impression of the need to build in greater resilience with components like email security.

10

The bottom line

The state of email security in 2020 is unlike any other year, and business as usual is a phrase we can no longer use.

At the close of 2019, many IT and IT security decision makers were planning to bolster their security posture with protections at the email gateway, within their organizations to protect employees and customers, and beyond their organizations' four walls to uphold brand trust. These protections are still underway; in fact, they are more critical than ever.

At the same time, comprehensive data from Mimecast Threat Center indicates a severely negative impact to businesses in the first half of 2020, and experts predict we'll see these attacks for months to come. Threat actors are relying heavily on impersonation and brand exploitation to take advantage of the uncertainty during the global COVID-19 pandemic. The usual email and web security defenses are no longer good enough; to prevent and protect your business against threat actors now and in the future, it's critical to integrate security awareness training as well as to protect your online brand.

Visit mimecast.com/state-of-email-security to learn more

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.