The State of Email Security Report 2019

Providing insight into your greatest email challenges

Contents

1 EMAIL ATTACKS

2 AWARENESS TRAINING

3 THREAT INTELLIGENCE

4 CYBER RESILIENCE

Read this before you dive in...

The Cyber Resilience Imperative

With email being the largest single attack vector on the planet, Mimecast understands the risks your organization faces when trying to defend against the daily scourge of threats; inbound, outbound and even internally too. We get this because we've been there. We've lived through it and we've used what we've learned as fuel to help organizations keep their most prized assets safe.

Keeping your organization secure and productive shouldn't be so hard. We'll be the first to admit that we've got a pretty lofty goal when it comes to helping you save the world (OK OK, or at least your organization) through better email security and awareness, but we know it's possible because we've done it before—and we do it every day for more than 34,000 clients.

We're able to achieve this because we understand organizations need more than just security: they need a cyber resilience plan. What is cyber resilience? **The Cyber Resilience Think Tank**—an independent group of cybersecurity experts and thought leaders—defines it as: "An organization's capacity to adapt and respond to adverse cyber events – whether the events are internal or external, malicious or unintentional – in ways that maintain the confidentiality, integrity and availability of whatever data and service are important to the organization."

To put it simply, cyber resilience is your ability to adapt and respond effectively to every potential threat no matter where it's coming from.

Of course, no great plan was ever constructed without data. To help you create that plan, we're thrilled to offer you the third annual State of Email Security (SOES) report that you can use as a reference for trends and risks that could impact your organization based on the latest research.

Think of the SOES report as your go-to guide for your email security plan. The information provided here should help you take action and make effective, results-driven decisions about your own internal practices and policies. And now in our second year, you can use the year-over-year results to benchmark trends that are key to your organizational success.

This report investigates the most pervasive types of email threats, how security professionals perceive them and what they're doing to combat them. Most importantly, you'll get a list of actionable steps to improve your organization's own email security and cyber resilience.

How this information is collected

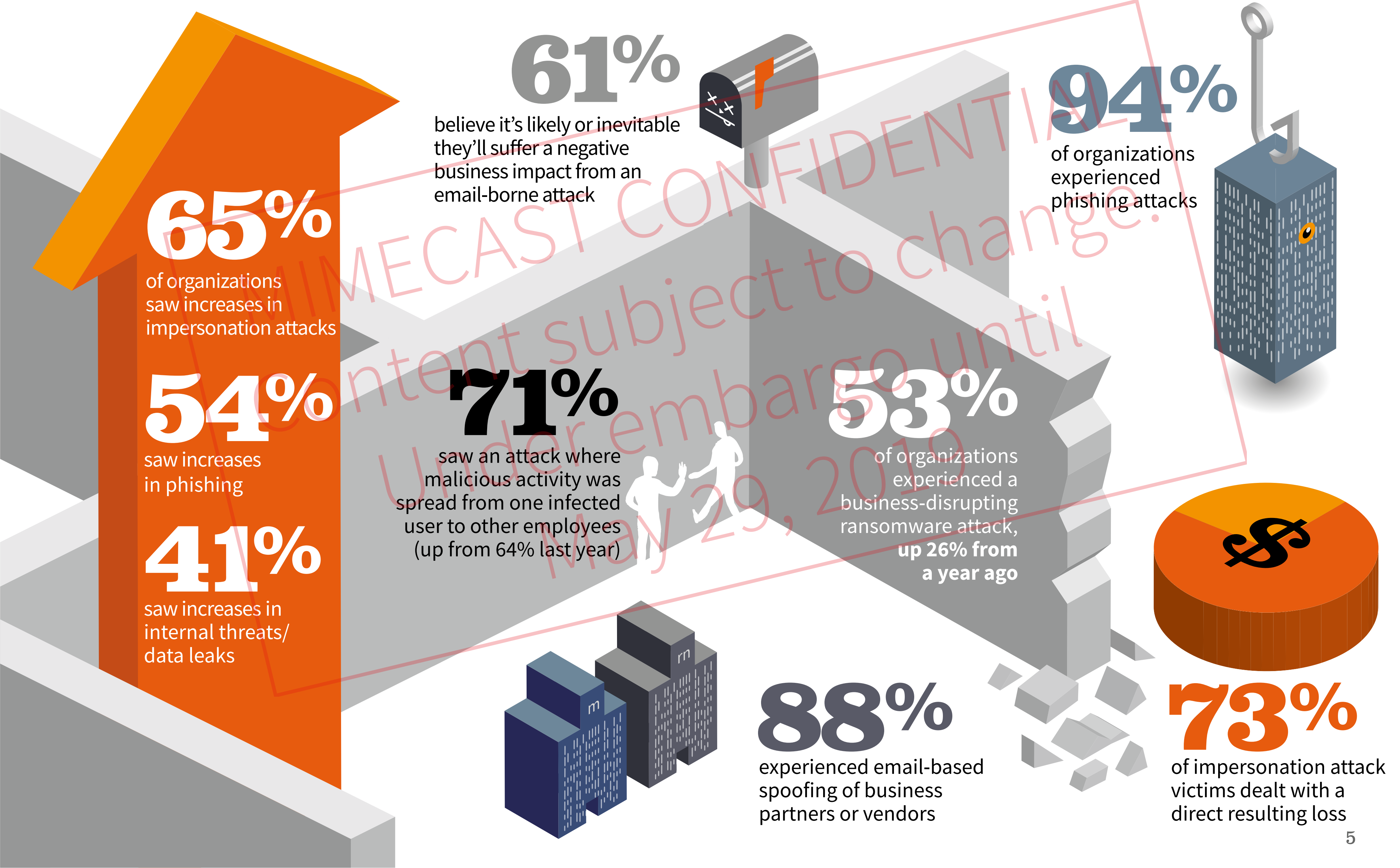
Research firm **Vanson Bourne** conducted a Mimecast-commissioned global survey of 1,025 global IT decision makers to gain useful insight into their experiences and outlook on the current state of email security. These participants were interviewed from December 2018 through February 2019 across the US, UK, Germany, Netherlands, Australia, South Africa and United Arab Emirates.

The key areas of focus included:

- Email-based attacks
- Business continuity
- Awareness training
- Threat intelligence
- Cyber resilience

This report highlights the following key findings, along with prescriptive insights for how to create (or improve upon) your cyber resilience program.

Key findings over the previous 12 months



65%
of organizations saw increases in impersonation attacks

54%
saw increases in phishing

41%
saw increases in internal threats/ data leaks

61%
believe it's likely or inevitable they'll suffer a negative business impact from an email-borne attack

94%
of organizations experienced phishing attacks

71%
saw an attack where malicious activity was spread from one infected user to other employees (up from 64% last year)

53%
of organizations experienced a business-disrupting ransomware attack, **up 26% from a year ago**

88%
experienced email-based spoofing of business partners or vendors

73%
of impersonation attack victims dealt with a direct resulting loss

1 Email Attacks

Confidence in defenses is falling. Here’s why.

Email attacks are on the rise and they’re not just affecting the bottom line. They’re also causing disruption for the team members responsible for preventing them. Attacks of all stripes, including phishing, impersonation and insider threats, are increasing across the board with no end in sight. As a result, IT decision-makers are finding themselves losing confidence in their organization’s ability to prevent the worst.

A whopping 61% of respondents believe that suffering a negative business impact from an email-borne attack is either likely or inevitable, a 3% increase from a year ago.

What’s more concerning, nearly 1 in 10 stakeholders feel it’s inevitable that their organization will suffer a negative business impact from an email-borne attack in 2019. Let’s take a closer look at the top issues that continue to challenge organizations and impact security and IT employee confidence.

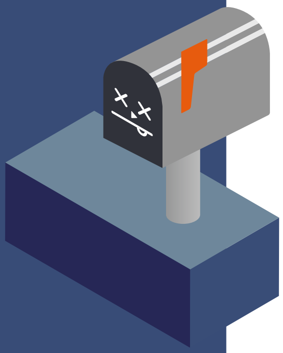
Impersonation and Phishing Attacks: Rising and Worsening

Flip through the latest headlines on any given morning and you’ll see the harsh impact of email impersonation attacks. Security breaches break headlines so often now that reading up on the latest threats almost feels like checking the weather. In the previous 12 months alone, 65% of organizations said they saw the volume of impersonation attacks increase, and 73% of impersonation attack victims experienced a direct resulting loss.

With this strong likelihood, it’s no wonder confidence is taking a hit. And because these highly-targeted attacks can tend to focus on key, C-level personnel, they can be incredibly embarrassing for victims. Suddenly the spotlight is no longer on their outstanding professional portfolios but instead on the negative actions of an employee or, worse yet, an executive of the company.

61%

A whopping 61% of respondents believe that suffering a negative business impact from an email-borne attack is either likely or inevitable, a 3% increase from a year ago.



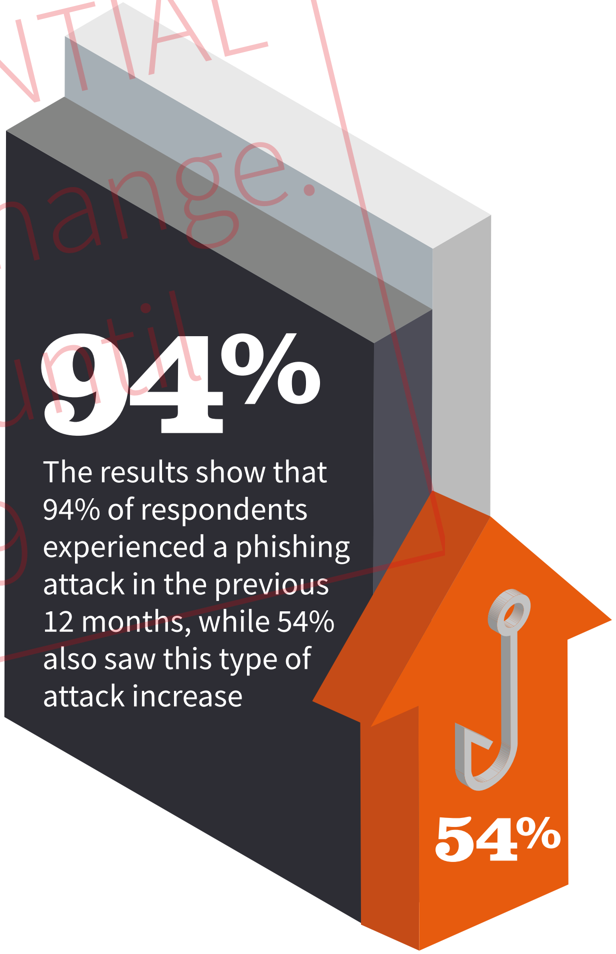
73% In the previous 12 months alone, 65% of organizations said they saw the volume of impersonation attacks increase, and 73% of impersonation attack victims experienced a direct resulting loss.

1 Email Attacks

Now, let's consider third-party risk. When organizations choose a business partner, they need to be just as concerned about their security posture as they are about their own. 88% of IT decision-makers saw email-based spoofing of business partners or vendors in the previous 12 months, and over a third (41%) of organizations have seen this issue increase with attackers looking to gain access to money, sensitive intellectual property or login credentials.

As for phishing attacks, it appears to be more a matter of when rather than if organizations will face them. The results show that 94% of respondents experienced a phishing attack in the previous 12 months, while 54% also saw this type of attack increase. Specifically, 45% of organizations saw an increase in targeted spear-phishing attacks with malicious links.

These social engineering-heavy attacks are clearly a significant concern for organizations because they're often one of the most difficult types to control. With the vast majority of these attacks preying on human psychology, it doesn't take more than a cleverly-spoofed email or a damaging text message to trick even the most skilled team member. (Think of that big $46 million heist at tech firm Ubiquiti a few years back, when attackers used impersonation techniques to pose as C-level execs and dupe employees.)



The results show that 94% of respondents experienced a phishing attack in the previous 12 months, while 54% also saw this type of attack increase

Internal Threats and Data Leaks

Internal threats and malicious activity residing within an organization continues to be a vexing problem. Of those surveyed, 71% were hit by an attack where malicious activity had spread from one infected user to other employees in the last 12 months, up from 64% a year ago. The biggest culprit: infected email attachments, which 47% of organizations report seeing spread. Next up was infected URLs via email at 40%.

Overall, internal threats and data leaks are rising as well, with 41% of respondents noting an increase. This could be why many aren't confident their email security systems can handle internal threats either. Approximately a third of respondents surveyed feel their email security systems fall short in monitoring and protecting against email-borne attacks or data leaks in both internal-to-internal and outbound emails, as well as automated detection and removal of malicious emails that have already landed in employees' inboxes.

1 Email Attacks

When thinking about insider threats, organizations should consider much more than malware. Even the most loyal employee could give up your sensitive and valuable corporate data under the right circumstances, including under the threat of blackmail or extortion. They're humans, and they can (and do) make mistakes. This is why awareness training is important to get employees to stop, think and verify. But we'll get to more on awareness training soon.

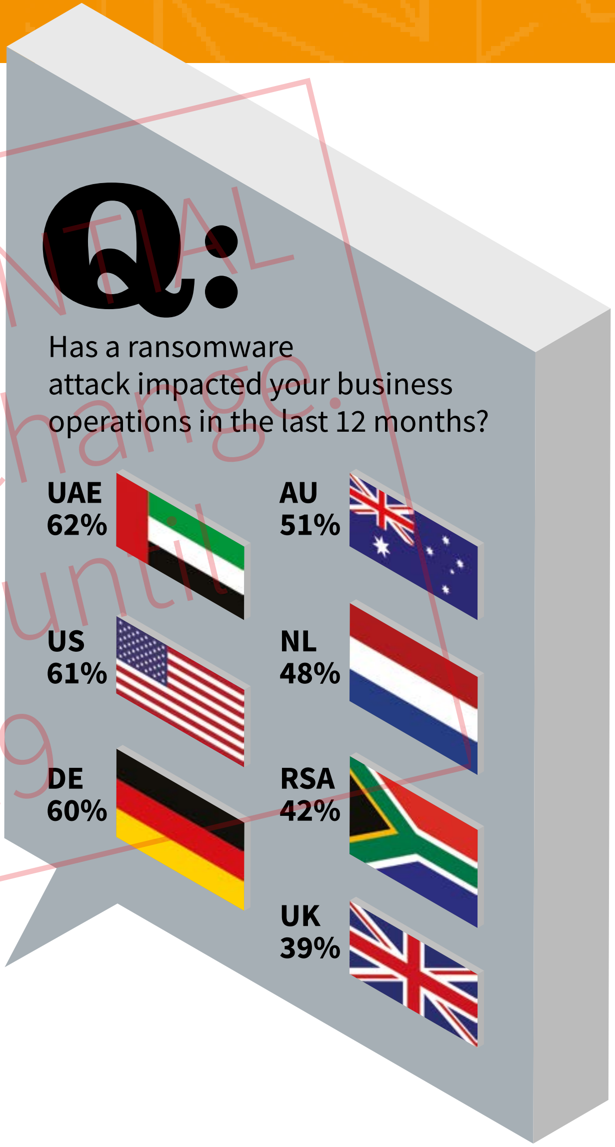
Ransomware and Downtime

The impact of a single email attack can disrupt business operations for days and cause data access issues, especially when it involves the often-costly consequences of ransomware. Not only is ransomware not going away, research confirms it's growing.

While some have been reporting on the decline of ransomware, our research shows this to be premature or perhaps is a case of wishful thinking. As a whole, ransomware attacks are up 26% from just one year ago with more than half (53%) of organizations encountering a ransomware attack that directly impacted business operations. This nearly doubles last year's 27% figure.

The impact is not solely monetary. 86% of organizations that experienced an impactful ransomware attack suffered at least two days of downtime as a result, with three days being the average amount of downtime—the same as last year.

For organizations that didn't experience a significant ransomware attack, 28% expect they could get by without experiencing any downtime if they were hit. This result begs the question: are these organizations supremely confident in their solutions, or are they just being naïve? Testing solutions—and holding vendors accountable—is the only way to know for sure.



Q:

Has a ransomware attack impacted your business operations in the last 12 months?

1 Email Attacks

Attack Aftermath: The Real Cost of Email Intrusion

Preparing in advance for any major event is crucial, but it needs to become a non-negotiable in email security. It's no longer enough to just play defense while cybercriminals are off honing their tactics daily. These criminals are aggressive and persistent when it comes to doing their homework and organizations should mirror this behavior.

Data from 2018 shows that organizations across the board run about a 30% chance of experiencing a major data breach, a 25% increase from 2014. On average, it will cost organizations close to $4 million when a breach occurs.* As a result, organizations must consider the cost of standing pat. By not increasing your cyber resilience posture, you're only increasing the likelihood you'll experience a costly breach.

Dealing with Data Loss

In the wake of an attack, there are many issues that arise—from downtime to time-consuming investigations and remediation—but with enough time, sweat, and resources, a complete recovery is possible.

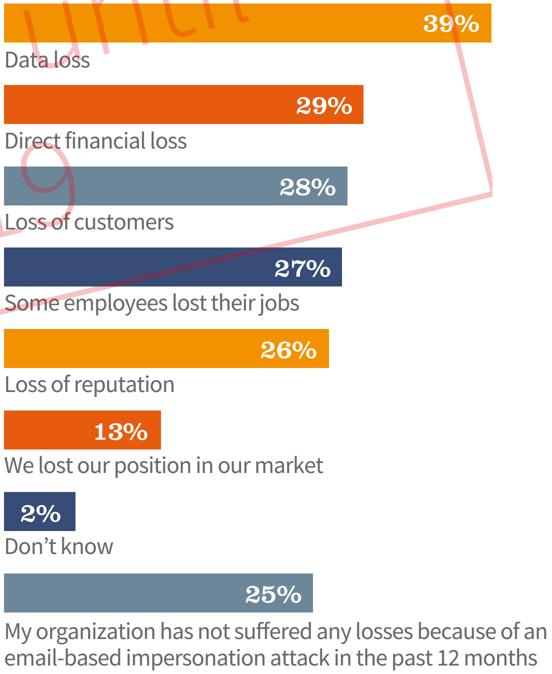
On the other hand, these rules don't apply to data loss. Once data falls into the wrong hands, you really can't regain what's been lost or repair the damage. Organizations have a fiduciary responsibility to inform customers, and that only compounds the issue.

Of the organizations that encountered an email-based impersonation attack in the last 12 months, 73% experienced a direct loss (data, financial, or loss of customers). When asked what specifically was lost during these events, 39% cited data, 29% said financial, and 28% noted lost customers. Moreover, nearly four in 10 (38%) of those who suffered losses because of email-based impersonation attacks noted data loss as the thing that hurt their organization the most.

**Data breach and cost stats: 2018 Cost of a Data Breach Study by Ponemon, sponsored by IBM. Evenly spread between SMB and enterprise organizations*

The Impacts Of Suffering An Attack

Nearly three quarters (73%) of respondents whose organization encountered an email-based impersonation attack in the last 12 months, report that their organization suffered a loss as a direct result of this type of attack in that time. Here's what they reported losing.



2 Awareness Training

Human error poses one of the biggest risks to your organization.

You might have an incredibly talented, diverse group of professionals at your organization. But cybersecurity's dirty little secret is that no matter how skilled your employees are, they still usually represent your biggest risk. Human error ranks even higher for cyber risk than software flaws and vulnerabilities. So high, in fact, that they're a contributing factor in more than 90% of breaches**.

The results of real-life testing are eye-opening, and chilling. We recently conducted a phishing simulation with a 6,500 employee software company that does not provide awareness training. The results showed that more than 500 employees clicked on a phishing email link in under a second. Thankfully, there's a flipside to this: Properly trained, alert and aware, your people can serve as an integral part of your security program and your first line of defense.

There are positive trends to report when it comes to awareness training adoption globally. Our survey found that 98% of organizations offer cybersecurity awareness training to their employees, with 25% saying they offer training on an ongoing (or, more than once monthly) basis, up from 11% a year ago.

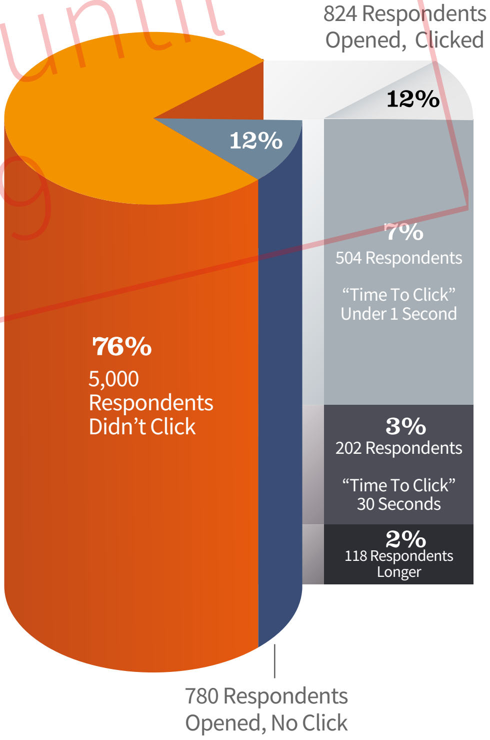
However, just 51% of organizations are conducting awareness training to spot cyberattacks only quarterly or even less frequently than that. Just under 10% conduct training once at induction for employees and never again, on an ad-hoc basis after a security breach, or don't do any training at all.

The consistent increases in breaches or losses due to email attacks proves this fundamental fact: cybersecurity awareness, and email security in particular, needs to be a priority. You're training your employees to stop, think and verify that the action they are about to take is not letting the bad actors in.

You and your teams are best served with a robust training program that covers a broad array of security topics, concentrated heavily on teaching employees how to detect and avoid email borne attacks.

People Don't Think. They Click.

- 2019 phishing simulation
- 6,500+ employee technology firm
- No awareness training program



*** IBM Sec. Svcs 2014 Intel Index; Willis Towers Watson – 2017, 90% based on claims data for cyber insurance*

2 Awareness Training

What types of cybersecurity and awareness training does your company offer employees?	Total	US	UK	Germany	Netherlands	Australia	South Africa	UAE
Group training sessions with our IT/IT security team	52.0%	64.7%	56.6%	61.3%	52.0%	68.0%	62.0%	72.0%
Interactive videos highlighting best/worst practices to keep in mind	45.0%	56.3%	42.9%	34.7%	35.0%	39.0%	30.0%	61.0%
A formal online test to learn about threats and prompts questions to respond to	44.1%	49.7%	49.7%	32.7%	36.0%	38.0%	31.0%	62.0%
An emailed or printed list of tips to keep in mind	43.7%	42.0%	42.3%	33.3%	29.0%	56.0%	45.0%	68.0%
One-on-one training sessions with our IT/IT security team	43.5%	45.0%	32.6%	47.3%	45.0%	43.0%	35.0%	60.0%
Sends prompts for me to note whether or not a link is “safe” prior to a allowing me to visit certain websites	38.4%	45.3%	31.4%	23.3%	41.0%	36.0%	37.0%	54.0%
Other	0.6%	0.7%	0.6%	0.7%	1.0%	0.0%	1.0%	0.0%
My company doesn’t provide any training	2.0%	1.3%	2.9%	1.3%	4.0%	1.0%	4.0%	0.0%
Number of respondents	1025	300	175	150	100	100	100	100

2 Awareness Training

So, how do you make cybersecurity training stick? It must be frequent, engaging, and updated to evolve with cybercriminals' latest techniques. It should be supplemented with phishing simulations. And, a good program will have a mechanism in place to allow you to identify higher risk employees and provide them additional or enhanced training.

One thing that organizations forget to focus on is the notion that training must be engaging so that, above all else, people actually remember it and want to apply the lessons actively.

The most widely used method (62%) of awareness training happens in a group session. Following group training sessions, other popular methods include interactive videos highlighting best/worst security practices (45%), formal online testing (44%), reference lists of tips (44%) and one-on-one training sessions (44%).

If more than half of organizations are capping off security awareness training at a total of four times per year, is it possible the overall impact could get lost in the noise in the context of a group setting? Think of it like a substitute instructor popping in a video for the entire class; interest wanes, retention rates are low, and the takeaway falls flat.

The bottom line here is that group sessions tend to be longer affairs, creating a burden for a busy workforce. Further, scaling in-person events is hard to do, meaning the training is too infrequent to be reinforcing itself effectively and tends to be more expensive than other methods in the long run.

Closing the Training Gap

Email security best practices need to start at the top. Company leaders must keep security awareness at the forefront of everything they do. Awareness training itself is mission-critical and should be considered as seriously as any other security system. Educating employees on email security cannot be achieved through one-off training sessions or siloed events that involve non-interactive materials like sterile corporate videos and mass-produced pamphlets.

Expert Insight

How an engaging training platform succeeds:

> "Its unique method of presentation—being humorous and topical, while also poignant—is very effective. For the first time, we have staff looking forward to their security awareness training."

SVP, CORPORATE SECURITY
Structural Engineering Consulting Company
1,500 employees

Source: TechValidate

Training

must be *engaging* for it to work, *frequent* enough to stick and *brief* enough to not be a burden

3 Threat Intelligence

Immediate Action is Key

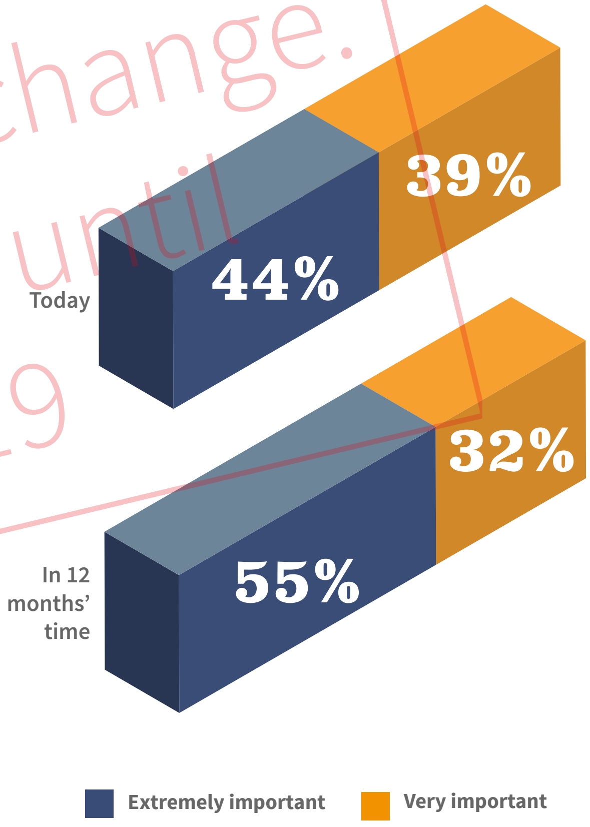
Seeing where your biggest threats are coming from is pivotal in preventing a serious business impacting attack. Overall, organizations seem to understand this because the research revealed that 90+% are already using threat intelligence sources, whether in-house or commercial options. That's a pretty healthy-looking number, yet just 44% of all stakeholders see threat intelligence as an extremely important asset to their organization. Meanwhile, only 39% say it's very important, and 55% note that it will be extremely important in the next 12 months. So, why are these stats all over the map?

Based on years of internal data and insights, we know that threat intelligence means different things to different people, so it's no surprise that there will be variation in the success rates of threat intelligence efforts. If organizations feel threat intelligence is just looking at all the indicators of compromise already within their systems and dealing with them, they may want to rethink that as an overall threat intelligence plan.

When resources are limited and teams are scrambling to make sense of threat intelligence in-house, they're not going to get as much value out of those indicators. Indicators are merely post-breach, isolated metadata and may not have direct bearing on your enterprise. Looking at just those indicators could result in time investigating, triaging and actioning events that have little to no context withoutproper curation.

Email security systems handle massive amounts of data, and they are the frontline of defense from attacks (i.e., seeing most attacks in their earliest stages). With this in mind, threat intelligence gathered and used by your email security systems needs to be a high priority and a key part of your security strategy in evaluating your security vendor. The process they follow should be more than just pumping in indicators. It should also be focused on efficacy and accuracy to reduce user heartburn and organizational impact.

Importance of Threat Intelligence



3 Threat Intelligence

Research shows that nearly six in 10 respondents are using email security systems that provide threat intelligence data to their security teams. Yet when it comes to consuming threat intelligence data and applying it to other systems, just over half (55%) have that key capability. Meanwhile, more than 10% noted that threat intelligence efforts are not happening at all in their organizations and will not be happening in the future.

Beyond Indicators of Compromise

Let's go back to the idea of true threat intelligence: if you're just looking at indicators of compromise after they've already infiltrated your organization, it's not enough. While some organizations understand that automating the consumption of threat intelligence into existing systems for maximum protection is key, many still aren't there. But integrating what organizations see from user behavior in email activity, which remains the top attack target worldwide, is a great place to start.

This is where a holistic approach, that includes both email security and threat intelligence, provides the most effective method. This bigger-picture view allows organizations to make their threat intelligence more actionable each and every day and empowers them to focus on users who are more likely to click on malicious links or attachments. It also allows them to identify users who may be experiencing a lot of targeted attacks likely because they have had a lapse in personal security, for instance, potentially using their business accounts for personal use.

It's also worth noting that you don't need record-breaking budgets to reap the benefits of threat intelligence. Focus on counter-intelligence and understanding how your attacker sees you as a victim. If you have not taken the time to implement these measures on your already budgeted and running security systems, this is a cost-effective manner to raise the bar against threat actors. Don't be the lowest common denominator; make the bad actors work for their foothold and become more resilient to attacks.

Expert Insight

Taking Threat Intelligence Inventory

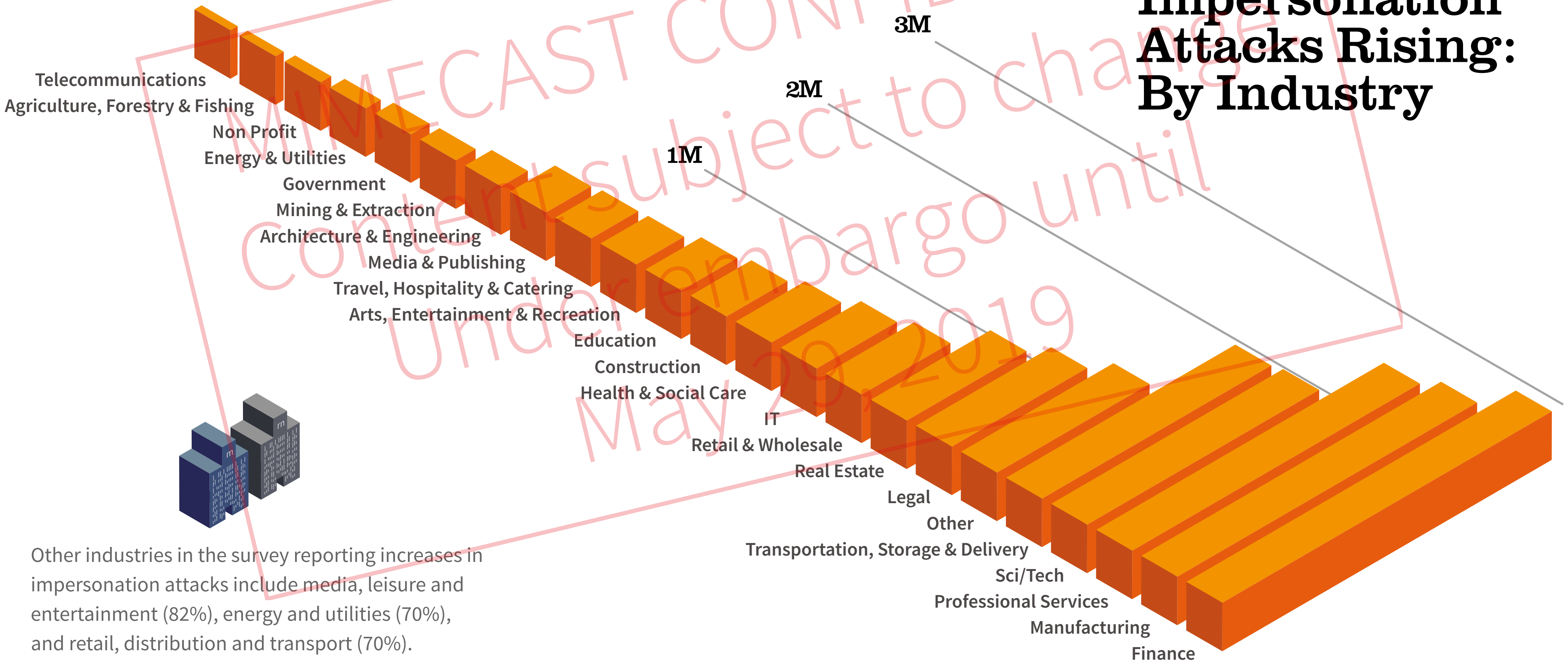
"[Gather] information from what you've already experienced in an incident database of internal issues ranging from phishing emails to malware infections. Refer to this constantly as you determine the best course for technology and strategies for your program."

MALCOLM HARKINS
Chief Security & Trust Officer
Cylance Inc

3 Threat Intelligence

In the survey, industries reporting increases in impersonation attacks in the previous year include finance (68%), professional services (68%) and manufacturing (66%).

During a four-month sample of data from the Mimecast customer grid, those three industries saw the largest volume of the same kind of attacks.



Other industries in the survey reporting increases in impersonation attacks include media, leisure and entertainment (82%), energy and utilities (70%), and retail, distribution and transport (70%).

Data collected from the Mimecast customer grid between July 1 and Nov. 1, 2018.

4 Cyber Resilience

Creating Your Cyber Resilience Roadmap

Here's a startling fact: of the stakeholders surveyed, less than half (46%) of their organizations have a cyber resilience strategy in place. Meanwhile, 29% are in the process of rolling one out, and 22% are currently planning or have a longer timeline for launching their cyber resilience plan. It's a silver lining that the number of organizations with a cyber resilience strategy is up from 27% last year, yet it's also clear that most companies still have plenty of work ahead in this area.

Out of the organizations that do have a cyber resilience plan in place (or are working toward implementing one in 2019), on average there are six different major areas of focus. These key areas include email security (74%), network security (73%), web security (71%), data backup and recovery (66%), internal email protection (64%) and endpoint protection (61%).

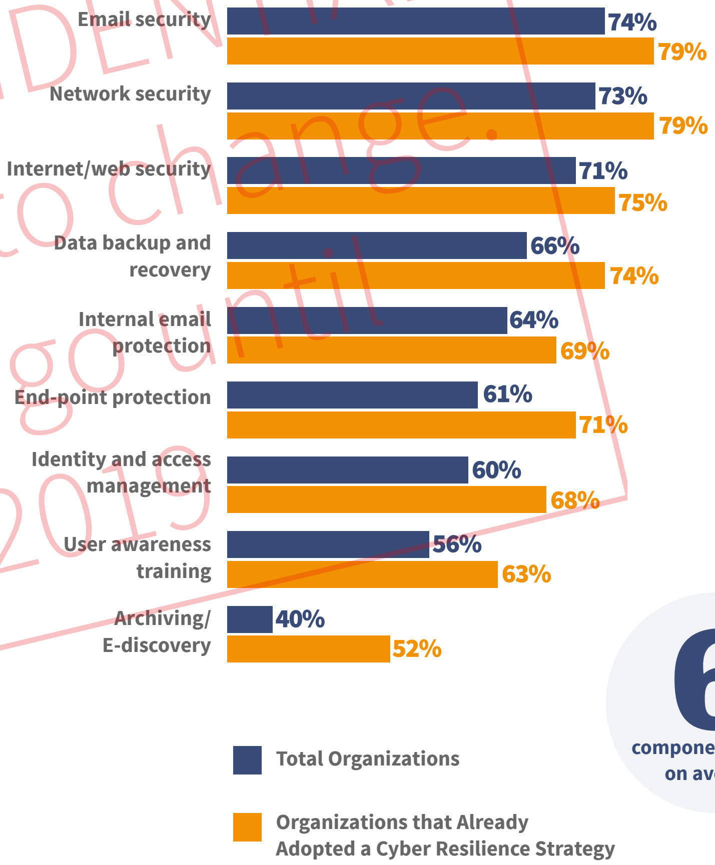
Learning from the Leaders

Cyber resilience can mean many things to different people but some have indicated it's about strategically implementing preventative measures to ensure you're fully prepared for whatever security risks come your way. When it comes to taking action ahead of an attack, we found that the most mature organizations* shared a few common tactics.

For starters, they appear to be more aware and more prepared in general, focusing on a combination of prevention and detection. Just over 10% of highly-mature organizations noted that it is inevitable their organization will suffer a negative business impact resulting from an email-borne attack in 2019. What's more, 65% recognize that upon suffering an email-based attack, it's critical that their organization maintains email uptime during the episode.

Cyber resilience leaders from highly-mature organizations also offer a greater selection of training methods, rather than a one-size-fits-all approach. Not only that, but they also conduct their email security awareness training on a more frequent basis than their less mature counterparts.

Elements of a Cyber Resilience Strategy



6
components each, on average

Our study calculated highly mature organizations based on multiple factors including the number of employees working exclusively in security; the organization's ability to protect against email attacks; attitude toward cyber resilience strategy; components included in their cyber resilience strategy; types of web security systems used; sources of threat intelligence data; types of cybersecurity and awareness training offered; and frequency of training.

4 Cyber Resilience

Our study indicates that mature cyber resilience leaders are most likely to:

- **Have a more comprehensive cyber resilience strategy**
- **Employ more skilled cybersecurity employees**
- **Train employees in cybersecurity awareness**
- **Have a plan to keep email running**
- **Be able to recover data from a ransomware attack**

Not surprisingly, highly immature organizations are the least likely to perform the tasks listed above. Mature organizations aren't afraid of change; they're the earliest and the fiercest adopters of any tools or best practices that level up their cyber resilience strategy.

Highly Immature Organizations

Cyber resilience non-starters

Least likely to:

- have a comprehensive cyber resilience strategy
- employ specialist cyber security employees
- use sources of threat intelligence
- train employees in cybersecurity awareness

Immature Organizations

Cyber resilience laggards

Mature Organizations

Cyber resilience adopters

Highly Mature Organizations

Cyber resilience leaders

Most likely to:

- have a more comprehensive cyber resilience strategy
- employ more specialist cyber security employees
- use more sources of threat intelligence
- train employees in cybersecurity awareness

Steps for Your Cyber Resilience Plan

The four dimensions of cyber resilience include:

1. **Threat protection**
2. **Adaptability**
3. **Durability**
4. **Recoverability**

So, what do all these things mean in the context of creating your cyber resilience roadmap? For starters, **threat protection** is your key to prevention. This is where the focus falls on stopping bad things from happening. Think of this dimension as your defense strategy. After that comes **adaptability** which, at a high-level, means that your plan can't be static. Attackers adapt constantly in their techniques and your plan needs to do the same in terms of techniques, technologies and people.

Once those are rock-solid, you need to make sure you've got **durability** covered as well. These are the details that matter during an attack when everything is going haywire and you still have a business to run. Durability means having a continuity plan that allows you to keep running without a hitch (other than that fire in the background your teams are diligently working to extinguish).

Finally, your plan must account for **recoverability**, allowing you to return to a good state at lightning speed (whatever that particular window might look like for your business). For some industries, this means losing no time at all because entire systems—and even lives—depend on their services. The average two to three days of downtime mentioned earlier for ransomware incidents is simply not acceptable for most organizations—think minutes versus days.

Expert Insight

Expert Insight:
CISOs in the Spotlight

"A CISO must create the permissive financial and business environment that is needed to deliver cyber resilience. They must educate decision makers, produce the roadmap, plan a major infrastructure project, secure resources from the wider business – and above all else, deliver on expectations."

PHIL OWEN
Global Head of Information Security
IHS Markit

4

Cyber Resilience

Achieving the Cyber Resilience Imperative

After consuming this research, your organization will be better prepared to face cybersecurity challenges and navigate the road to stronger cyber resilience. These results bring to bear that becoming a cyber resilience leader begins with teamwork. Security leaders within the organization should work toward raising everyone's awareness and understanding of email security policies and best practices. As the evidence shows, frequent and engaging training is an integral piece of this puzzle—coupled with understanding the importance of integrating effective threat intelligence.

When every employee in your organization, regardless of title, understands that they play a key role in your security success, things begin to change for the better. These cultural shifts are not only positive reminders that each team member is a vital part of the process, but they're key to improving your overall security posture.

Top Ten Takeaways:

1. **Playing defense only won't cut it; in 2019 and beyond, you've got to be prepared for the worst.** 61% of respondents believe that suffering a negative business impact from an email-borne attack is either likely or inevitable.

2. **Security breaches don't just slow you down, they have a direct impact on your business.** The average downtime from a ransomware attack is three days—the same number as the previous year.

3. **Create your plan to combat impersonation attacks.** In the previous 12 months alone, more than 85% of respondents experienced an impersonation attack, and about two-thirds saw these types of attacks increase.

4. **One bad click can quickly create a cascade of bad events.** 71% of organizations saw malicious activity spread from one infected user to other employees, an increase over last year's 64%.

5. **Phishing isn't going away anytime soon.** 94% of respondents experienced a phishing attack in the previous 12 months.

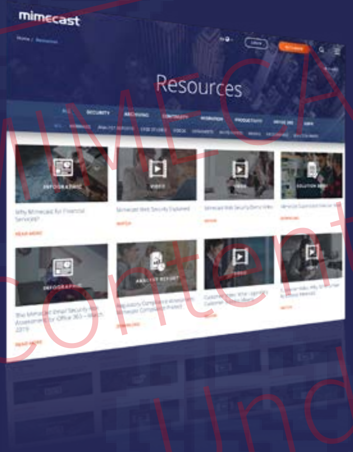
6. **If you're part of a supply chain, you're a significant target.** 88% of IT decision-makers saw email-based spoofing of business partners or vendors in the previous 12 months.

7. **Ransomware is on the rise—still.** More than half (53%) of organizations encountered a ransomware attack that directly impacted business operations. This is way up from the previous year, when it was just 27%.

8. **Data loss should be your biggest concern.** Of the organizations that encountered an email-based impersonation attack in the last 12 months, a jaw-dropping 73% experienced a direct loss (data, financial, or loss of customers). Nearly four in 10 (38%) of those who suffered losses because of email-based impersonation attacks noted data loss as the thing that hurt their organization the most.

9. **Awareness training needs serious attention, improvement and investment.** The most widely used method (62%) of awareness training happens in a group session. Is that the most timely or engaging method?

10. **You can start a cyber resilience plan in four straightforward steps**. Less than half (46%) of organizations have a cyber resilience strategy in place.



Visit the Mimecast Resource Center

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.

www.mimecast.com