

**mimecast**<sup>®</sup>

---

# The State of Email Security Report 2019

Providing insight into your greatest email security challenges



# Contents

## 1

### EMAIL ATTACKS

---

- 6 Confidence is Falling. Here's Why
- 6 Impersonation/Business Email Compromise and Phishing Attacks: Rising and Worsening
- 7 Internal Email Threats and Data Leaks
- 8 Ransomware and Downtime
- 9 Attack Aftermath: The Real Cost of Email Intrusion

## 2

### AWARENESS TRAINING

---

- 10 Humans Pose the Biggest Risk to Your Organization
- 12 Closing the Training Gap

## 3

### THREAT INTELLIGENCE

---

- 13 Immediate Action is Key
- 14 Beyond Indicators of Compromise

## 4

### CYBER RESILIENCE

---

- 16 Creating Your Cyber Resilience Roadmap
- 17 Learning from the Leaders
- 18 Elements of Your Cyber Resilience Plan
- 19 Achieving the Cyber Resilience Imperative
- 20 Top Ten Takeaways

# 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 internal too. We get this because we've been there. We use our knowledge from these experiences 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 keep your organization safe 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 aid in this success 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 that will help you shape 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, you can use the year-over-year results to benchmark trends that are key to your organizational success.

Through this report, we're investigating 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 was collected

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 December 2018 through February 2019 across the US, UK, Germany, Netherlands, Australia, South Africa and United Arab Emirates.

The key areas of focus included:

- Advanced Threats in Email
- Business Email Compromise
- Phishing & Spear-phishing
- Malware
- Insider Threats
- Ransomware
- Business Disruption
- Awareness Training
- Threat Intelligence
- Resilience Strategies

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

**67%**

of organizations saw increases in impersonation / business email compromise 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



**71%**

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

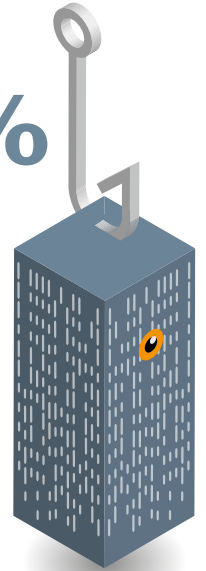


**53%**

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

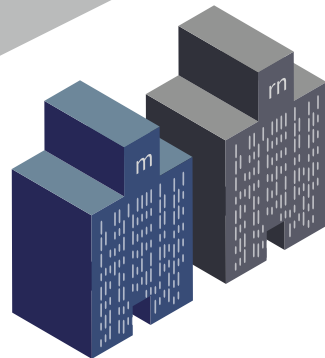
**94%**

of organizations experienced phishing attacks



**88%**

experienced email-based spoofing of business partners or vendors



**73%**

of impersonation attack / BEC victims faced 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. It's no surprise that IT decision-makers are 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 jump from 58% a year ago.

What's more concerning is that nearly 1 in 10 stakeholders feel it's inevitable that their organizations 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/Business Email Compromise 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, or business email compromise (BEC). 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, 67% of organizations said they saw the volume of impersonation attacks increase, and 73% of impersonation attack victims experienced a direct resulting loss.

With the strong likelihood of losses, 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%

61% of respondents believe that suffering a negative business impact from an email-borne attack is either likely or inevitable, up from 58% a year ago.



# 73%

In the previous 12 months alone, 67% of organizations said they saw the volume of impersonation / BEC attacks increase, and 73% of victims experienced a direct resulting loss.

# 1 Email Attacks

As for phishing attacks themselves, 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.

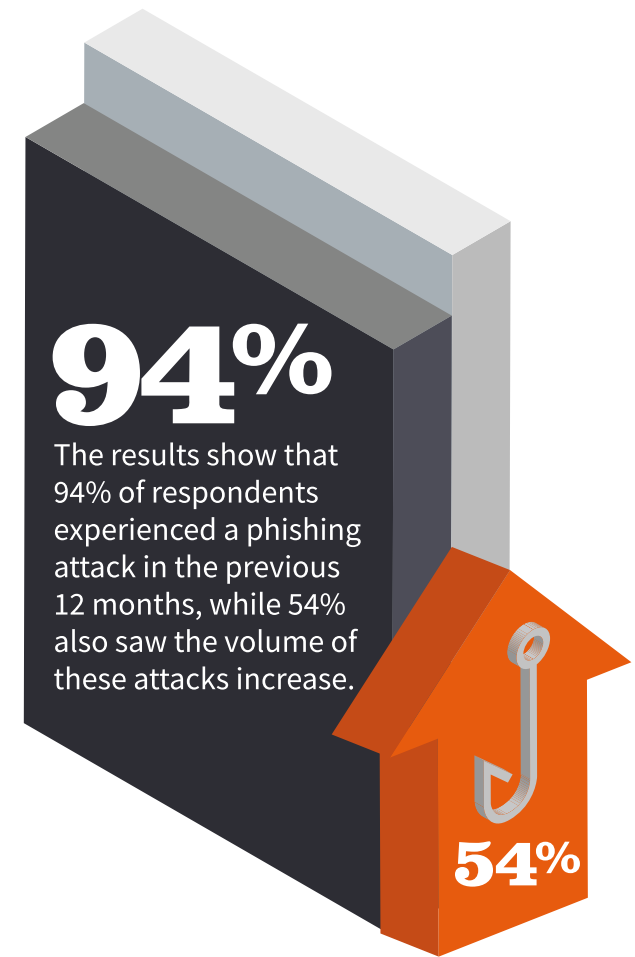
Now, let's consider third-party risk. When organizations choose a business partner, they need to be just as concerned about their security posture as they are about their own. 88% of IT decision-makers saw email-based spoofing of business partners or vendors in the previous 12 months, and over a third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

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 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 to dupe employees.)

## Internal Email Threats and Data Leaks

Internal threats and malicious activity residing within an organization continue 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 reported seeing spread. Next up was infected URLs via email at 40%.

Overall, internal threats and data leaks were 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 one-third of respondents surveyed felt their email security systems fell 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 had already landed in employees' inboxes.



# 1 Email Attacks

## Ransomware and Downtime

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 a decline of ransomware, our research shows this to be premature or perhaps 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: could these organizations truly come through a ransomware attack unscathed, or are they just being naïve? Testing solutions—and holding vendors accountable—is your best path forward.

# Q:

Has a ransomware attack impacted your business operations in the last 12 months?  
Here's how many answered yes:

**UAE**  
62%



**AU**  
51%



**US**  
61%



**NL**  
48%



**DE**  
60%



**RSA**  
42%



**UK**  
39%



# 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 item 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. They're after your data and money, and they won't stop until they get it.

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.\* These startling facts require action against serious losses.

### Dealing with Data, Customer & Financial 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.

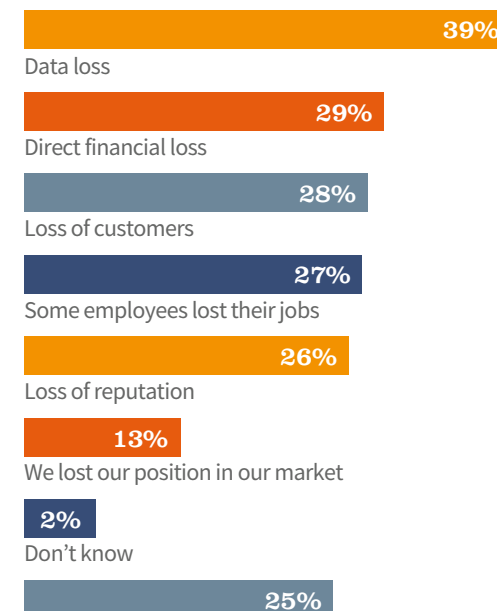
Unfortunately, these rules don't apply to data loss. Once data falls into the wrong hands, you really can't regain what's been lost or repair the damage. Organizations also have a fiduciary responsibility to inform customers, which only compounds the issue.

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, 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 organizations encountered an email-based impersonation attack in the last 12 months, suffering losses in the following categories as a result:



My organization has not suffered any losses because of an email-based impersonation attack in the past 12 months



# 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. Research shows that human error ranks even higher for cyber risk than software flaws and vulnerabilities. So high, in fact, that it's a contributing factor in more than 90% of breaches\*\*.

The results of real-life testing are eye-opening, and chilling. Mimecast 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: when properly trained, alert and aware, your people can serve as an integral part of your security program and your first line of defense.

More and more organizations are catching onto

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.

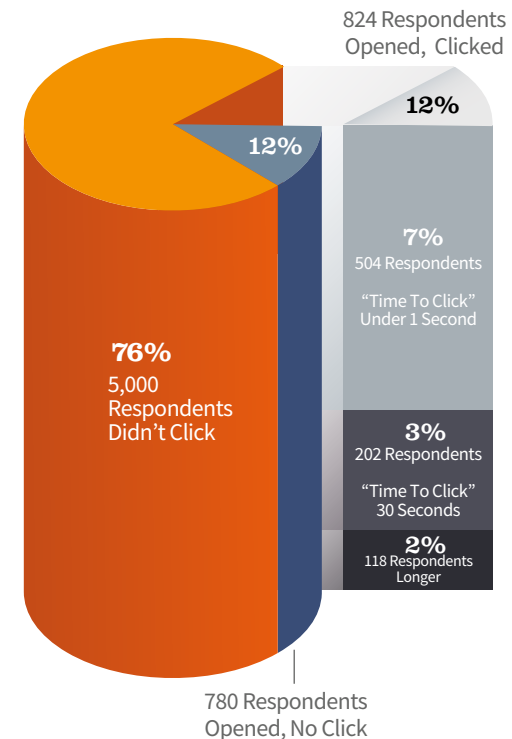
On the flip side, 51% of organizations are only conducting awareness training quarterly or even less frequently. And just under 10% conduct training only once at induction for employees, on an ad hoc basis, after a security breach, or not at all.

In a recently-conducted analysis comparing answers to security questions before and after training, results showed that employee knowledge on security topics increased by 400% or more\*\*\*.

These results reinforce the need for engaging training that is delivered persistently over time and that concentrates heavily on helping employees detect and avoid email-borne attacks.

## People Don't Think. They Click.








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



\*\*2018 Cost of a Data Breach Study by Ponemon, sponsored by IBM.

\*\*\*Internal studies conducted in 2018 of Mimecast Awareness Training participants.

# 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	62.3%	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 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

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 security awareness training at a total of four times per year, is it possible the overall impact could get lost in the noise? And, is the group setting the best way to get awareness training across to an audience? Think of it like a substitute teacher popping in a video for the entire class; interest wanes, retention rates are low, and the takeaway falls flat.

Can group training be effective? Perhaps. But they 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 effective and tends to be more expensive than other methods in the long run.

## Closing the Training Gap

Awareness training itself is mission-critical and should be considered as seriously as any other security system. As noted before, nearly 100% of organizations are doing some kind of training. But the devil is in the details. Some types of training work, and some don't. 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

**An insider's perspective on what makes their training work:**

*"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

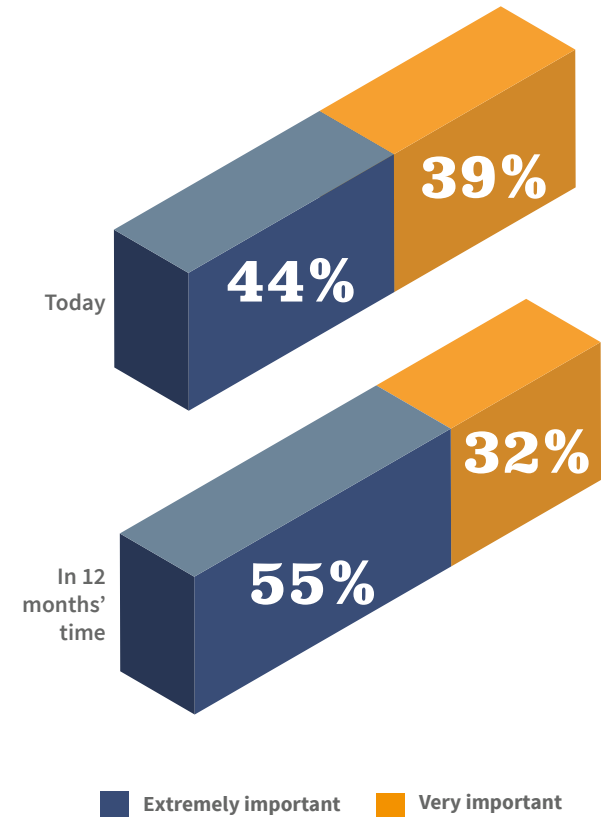
Seeing where your biggest threats are coming from is pivotal in preventing a serious business impacting attack. Overall, organizations seem to understand this. The research revealed that 90+% are already using in-house or commercial threat intelligence sources. Additionally, 44% of all stakeholders see threat intelligence as an extremely important asset to their organization. 39% say it's very important, and 55% note that it will be extremely important in the next 12 months.

Based on years of data and insights, we know threat intelligence means different things to different people. This can range from looking at indicators of compromise after they're already in an organization to threat data getting integrated and shared throughout all systems. For those only looking at those initial indicators, it may be time to rethink that strategy.

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 their enterprise. Looking at just those indicators could result in time investigating, triaging and actioning events that have little to no context.

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. The process should follow more than just pumping in indicators. It should also be focused on efficacy and accuracy to reduce administrator heartburn and organizational impact.

## Importance of Threat Intelligence



# 3 Threat Intelligence

Research shows that nearly six in ten 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, 10% noted that threat intelligence isn't happening at all in their organizations and will not be happening in the future.

## Beyond Indicators of Compromise

Let's go back to indicators of compromise: if you're just looking at them 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 understanding how your attackers think and incorporate that information into your already-budgeted and running security systems to the greatest degree possible. Doing so is a cost-effective way 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."*

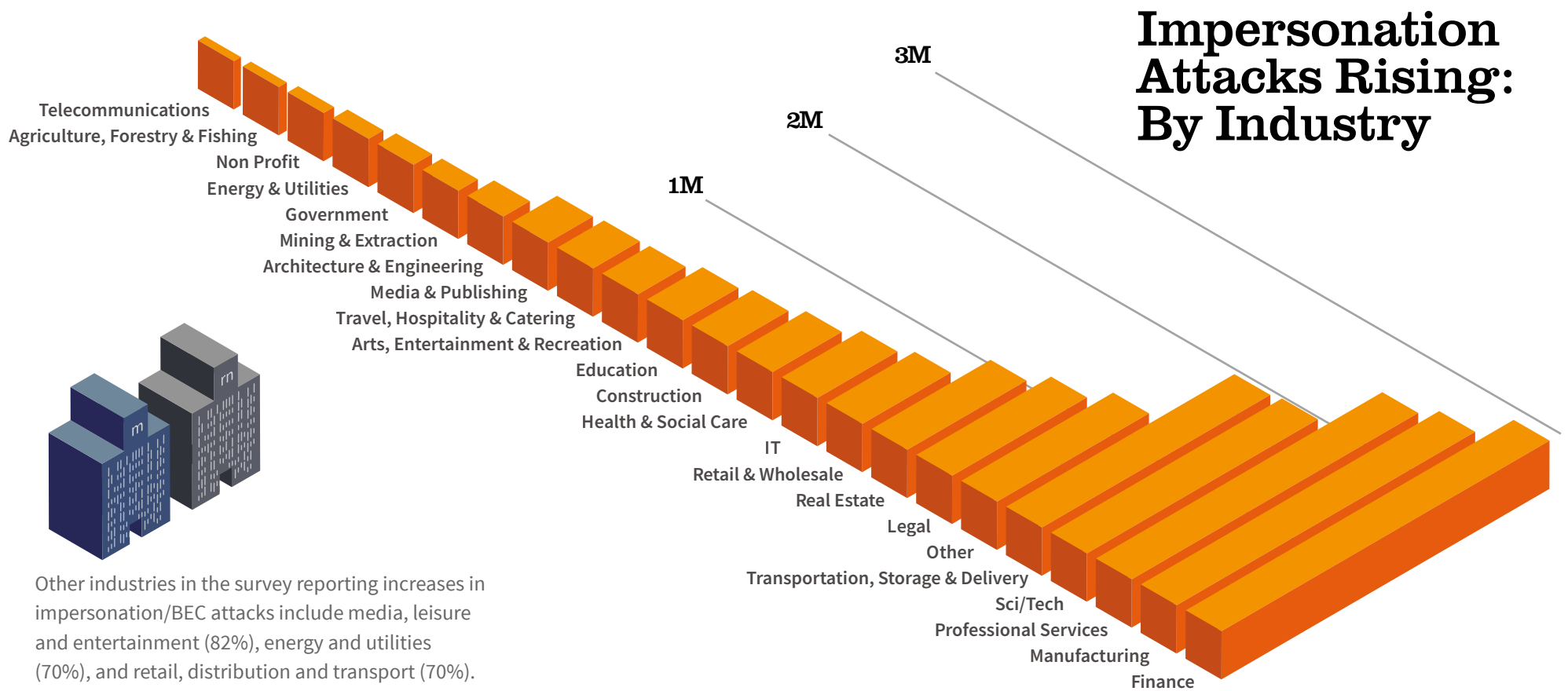
**MALCOLM HARKINS**  
Chief Security & Trust Officer  
Cylance Inc

Cyber Resilience Think Tank member

# 3 Threat Intelligence

In the survey, at least two-thirds of organizations in the finance (68%), professional services (66%) and manufacturing (66%) reported increases in impersonation/BEC attacks.

During a four-month sample of data collected by the Mimecast Threat Analysis Center, those three industries saw the largest volume of impersonation attacks.



\*Data collected 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 organizations 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%).

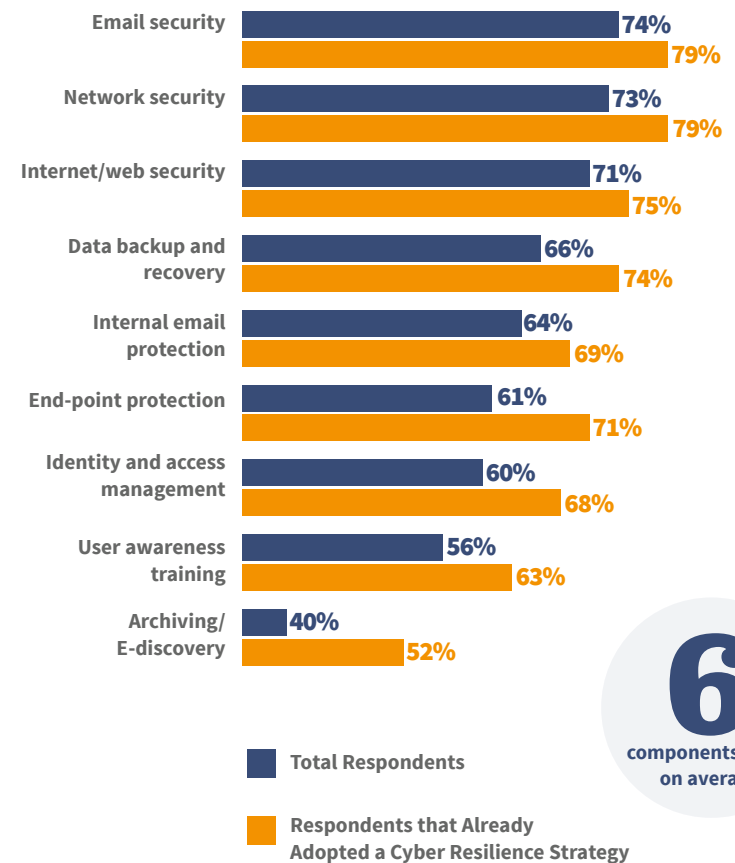
## Learning from the Leaders

Cyber resilience can mean many things to different people, but some have indicated it's about strategically implementing preventive 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 characteristics.

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

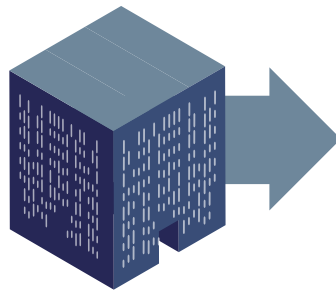


\*Our study calculated highly mature organizations based on multiple factors including the number of employees working exclusively in security; the organization's ability to protect against email attacks; attitude toward cyber resilience strategy; components included in their cyber resilience strategy;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

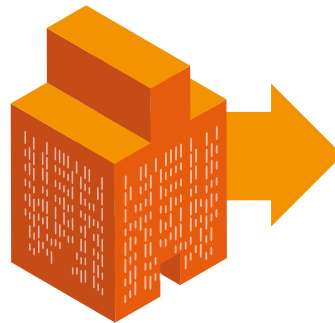
# 4 Cyber Resilience

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

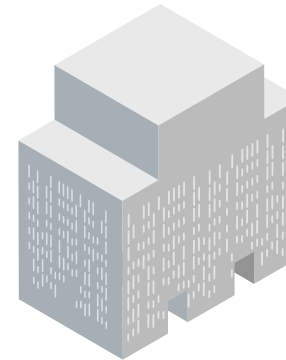
- Have a more comprehensive cyber resilience strategy
- Employ more skilled cybersecurity employees
- Train employees in cybersecurity awareness
- Have a plan to keep email running
- Be able to recover data from a ransomware attack



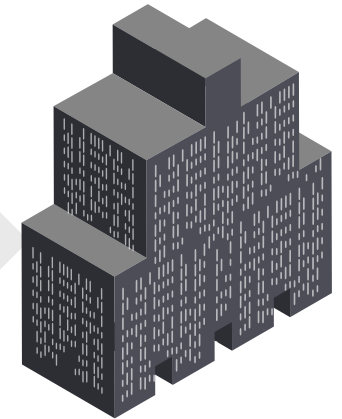
**Highly Immature Organizations**  
Cyber resilience non-starters



**Immature Organizations**  
Cyber resilience laggards



**Mature Organizations**  
Cyber resilience adopters



**Highly Mature Organizations**  
Cyber resilience leaders

No losses from impersonation attacks in last 12 months	15%	20%	26%	39%
Requiring 1 day or less to recover from attacks	24%	29%	32%	39%
Haven't seen attacks where malicious activity was spread	19%	28%	28%	40%



# 4 Cyber Resilience

## Elements of 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 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. It's about providing effective security controls **before**, continuity **during** and automated recovery **after** an attack.

These survey 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 Impersonation attacks aren't slowing down.**

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 Internal threats 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 ten (38%) of those who suffered losses because of email-based impersonation attacks noted data loss as the thing that hurt their organization the most.

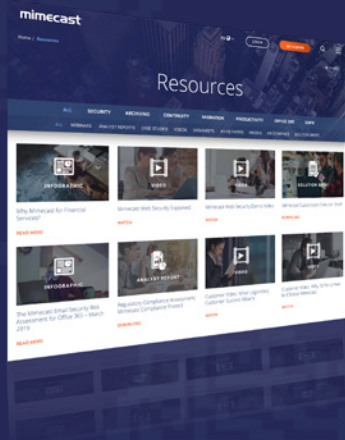
**9 Awareness training needs serious attention, improvement and investment.**

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](http://www.mimecast.com)