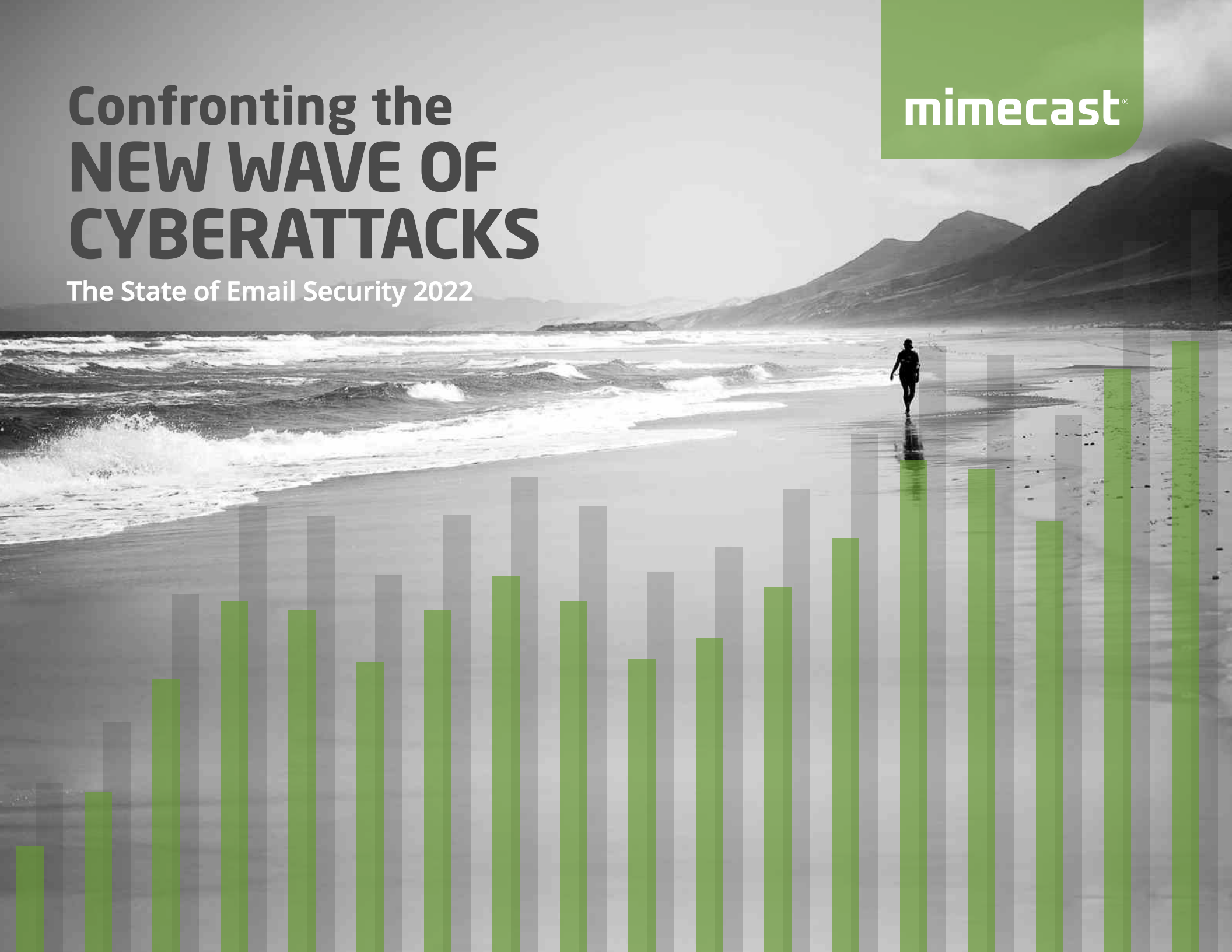
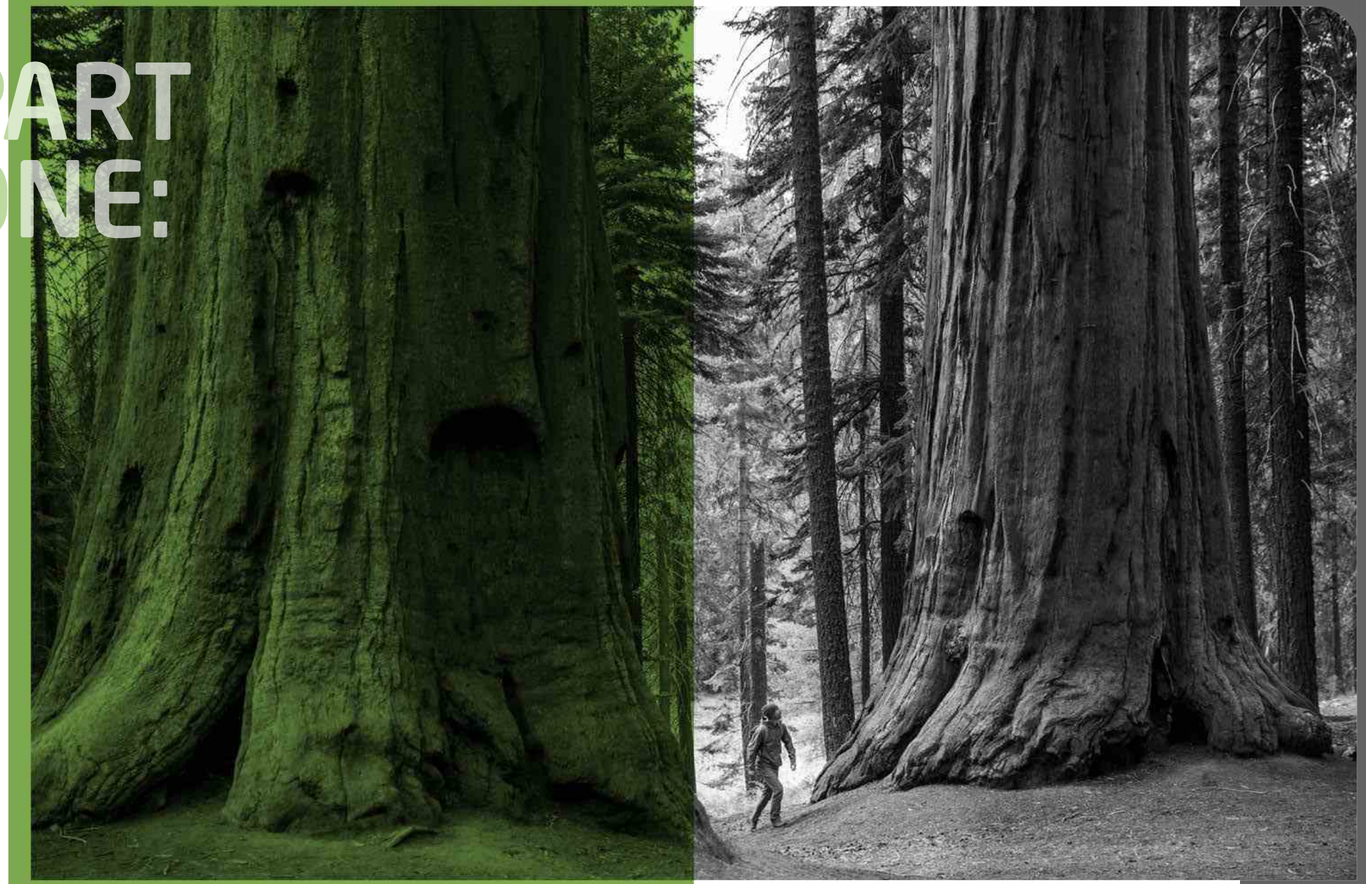
Confronting the NEW WAVE OF CYBERATTACKS

The State of Email Security 2022



PART ONE:



A Digital Pandemic of EPIC PROPORTIONS

Like the virus responsible for the worldwide pandemic, email-based cyber threats continued to mutate in 2021, causing global havoc.

As Mimecast's sixth annual *State of Email Security* report makes clear, businesses around the world continued to find themselves in the crosshairs not just of a novel coronavirus, but also a torrent of new cyberattacks. Any hope that this onslaught would abate once the world had adjusted to the pandemic was short lived.

In 2021, the cyber threat landscape in country after country became more treacherous, not less.

With the number of publicly reported data breaches soaring past last year's total, 2021 appears to be the worst year on record for cybersecurity.[1] Phishing was the biggest culprit, with 36% of data breaches due, at least in part, to employee credentials stolen through a phishing attack,[2] 96% of which occur through email.[3]

Ransomware is also running amok. According to recent reports, a staggering 84% of U.S. organizations have reported phishing or ransomware attacks in the past 12 months[4] and the average ransomware payment climbed to $570,000 during the first half of 2021, up from $312,000 in 2020.[5]

2021 appears to be the **worst year on record** for cybersecurity.

But for organizations that have been infected, the financial costs of this digital pandemic have been much higher. The average cost of a data breach is now **$4.24 million**, up from $3.86 million in 2020.[6] A data breach that compromises 10 million records costs a business $50 million on average; one that compromises 50 million records can cost as much as $392 million.[7]

All this has led to a change in how cyber threats are perceived by corporate leadership. The research firm Gartner tracks board-level attitudes toward cybersecurity — and has seen a sharp shift. Five years ago, only 58% of board members considered cyber-based threats a significant business risk. In 2021, that figure rose to **88%**.[8]

For cybersecurity professionals seeking more resources with which to counter these threats, that shift in perception is a welcome development. So, while the big picture is unquestionably grim, not all is doom and gloom. Mimecast's *State of Email Security 2022* (SOES) study sheds light on the gains in cyber resilience that many companies are making, even as it reveals shortfalls and places where there is considerable room for improvement. To better understand the current cyber threat variants and what's required to contend with them, let's get into the report's nitty gritty.

PART TWO:

MORE VARIANTS
and Greater Apprehension

8 in 10
companies are bracing for the fallout from an email-borne attack.

The picture that emerges from this year's SOES report is one of markedly increased apprehension over the dire consequences of an email-borne attack. Indeed, **8 out of 10** of this year's SOES survey respondents believe it is likely, extremely likely or even inevitable that their organization will suffer negative consequences in 2022 as the result of an email-based cyberattack.

This resignation is significantly greater than it was last year (80% vs 70%) at the high point of the COVID outbreak, and for the four years prior. Such pessimism is founded in the recognition that as COVID took hold, companies and government entities became much more reliant than ever before on email, collaboration tools and other forms of electronic communications. This has not escaped the attention of the world's cybercriminals.

Hackers experienced considerable success by taking advantage of the widespread fear and chaos that characterized the early days of the pandemic. They soon realized, however, that increased dependency on digital messaging was fast becoming a fixture of the post-COVID world and responded by refining their tactics and stepping up their attacks.

Among the 1,400 SOES respondents, **79%** reported an increase in email volume at their organization, including 33% who indicated that the increase was significant. At the same time, nearly three-out-of-four (**72%**) of the respondents said the number of email-based threats had also risen during the past 12 months, with more than a quarter (26%) characterizing the increased threat level as significant. This was especially true of survey participants from the technology and telecommunications sector, where 8 out of 10 (**80%**) reported seeing more threats than the year before.

These threats are also increasingly sophisticated, according to a majority of the respondents (52%), and they considered this their top email security challenge for the coming year. The most prevalent form of attacks are phishing attempts, with 55% of the study participants noting that these are on the rise and nearly all (**96%**) of the respondents acknowledging that their organization had faced this threat in the past year. Business email compromise attacks and data leaks due to careless, negligent or compromised employees were also extremely widespread (encountered by 92% and 93% of the respondents, respectively).

Yet while all these types of attacks have become more pernicious and are taking place more frequently than they did before, the most troubling variant and the one that's proliferating the fastest is ransomware.

79% of respondents reported an increase in email volume at their organization

72% of the respondents said the number of email-based threats had risen during the past 12 months

96% of respondents acknowledge that their organization had faced a form of phishing attack in the past year

KEY FINDINGS

Over The Past 12 Months

Only 23% of companies provide cyber awareness training to their employees on an ongoing basis, but 87% offer it at least once a quarter.

80%
of companies are bracing for the fallout from an email-borne attack.

More than 8 out of 10 respondents believe their company is at risk due to inadvertent data leaks by careless or negligent employees.

98%
of companies are either using or plan to use a brand protection service this year.

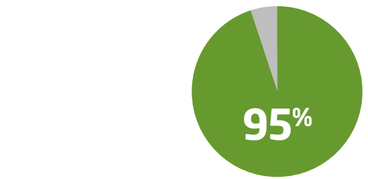
When faced with a ransomware attack, **64%** of companies paid the ransom, yet nearly 4 out of 10 of them failed to recover their data.

96%
of companies have been the target of an email-related phishing attempt.

52%
Cyberattacks are growing increasingly sophisticated according to 52% of the respondents.

On average, **14%** of IT budgets are allocated for cyber resilience.

To counter brand spoofing, **89%** of companies are making use of DMARC or plan to do so over the next 12 months.



of respondents say their cyber resilience has been impaired by insufficient funding.

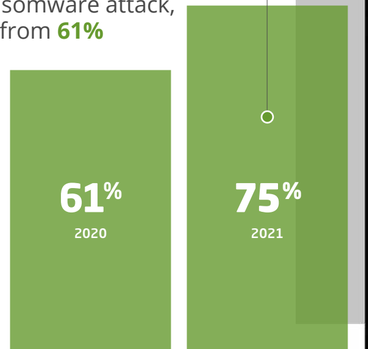
99%
of companies either have a system to monitor and protect against email-borne threats or are actively planning to roll one out.

Email usage rose at **8** out of **10** companies

96%
of companies either have a cyber resilience strategy or are actively planning to put one in place.

3 out of 4 companies are receiving an increased number of email-based threats.

75% of companies were hurt by a ransomware attack, up from **61%**



Among Microsoft 365 security email users, 79% experienced an outage during the past year.

PART THREE:

Ransomware Is DOMINANT

Stated bluntly, the ransomware outlook is grim. Analysts predict that the frequency of these attacks will rise to one every two seconds, as the perpetrators refine their malware and methods of attack. The cost of these attacks is expected to reach **$265 billion by 2031**.[9]

These warnings are right in line with this year's SOES findings that **75%** of companies were hurt by a ransomware attack, up from 61% in 2020. The attacks, however, were not evenly distributed. Among organizations that experienced a significant rise in email threats during that past 12 months, an eye-popping **88%** were victimized by ransomware. This compared with only 65% of organizations where email threats did not appreciably increase — but even for these companies, damage from ransomware was still more pervasive than it was for all companies the year before.

There were also some notable differences in how the ransomware threat played out among different countries and industries. In the U.S., for example, 41% of the companies surveyed suffered significant consequences from a ransomware attack compared with only 17% in Canada. Likewise, nearly two-out-of-three (64%) of media, leisure and entertainment companies were significantly harmed by ransomware, compared with less than a third (29%) of manufacturers.

Measured in terms of downtime, a quarter of the companies (25%) that were infected with ransomware experienced outages of two to three days. But nearly as many (22%) were down for a week, while another 15% had outages up to two weeks.

When confronted with a ransomware attack, nearly two-thirds (**64%**) of the victims felt compelled to pay the ransom, *yet nearly four out of 10 of them (39%) failed to get back their data*. With fewer than a third of the victimized companies (**32%**) able to recover their data without paying a ransom, it is no small wonder that the number of these attacks is skyrocketing, given how lucrative they are for the perpetrators.

In the face of all this, most companies are urgently seeking to inoculate themselves against ransomware and other email-borne threats. Their efforts to date, however, have been uneven.

Nearly **two-thirds** of ransomware victims were forced to pay the ransom.

PART FOUR:

Cyber Resilience: Improving — But Not Always

The best medicine is prevention and that is no less true for a cyberattack. This is where an organization's cyber resilience comes into play: How well can it identify and prevent new threats, and how quickly can it recover from those that get through.

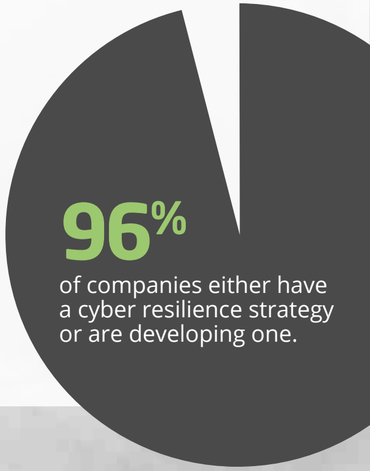
This year's SOES data indicates that companies are taking cyber resilience more seriously than they ever have before — but also that the majority are still not where they want to be in terms of cyber preparedness. To better understand this, we need to take a deep dive into the SOES data.

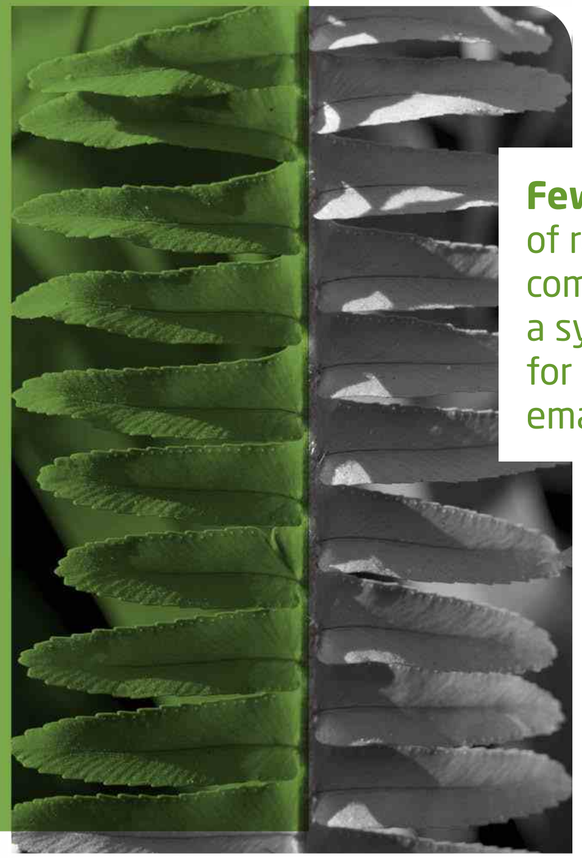
Among this year's SOES participants, more than a third (**38%**) currently have a cyber resilience strategy in place. But that compares poorly to the prior year, when 44% reported the same and even worse to the 2020 SOES survey, when 49% of the respondents indicated that they had such a strategy. But does this really mean that in the face of mounting attacks fewer organizations are taking the necessary steps to defend themselves?

In the 2022 survey, another **37%** of companies responded that they are actively in the process of rolling out a cyber resilience strategy, while an additional 17% said they would be doing so in the next 12 months and 4% more stated that they too would be implementing a cyber resilience strategy but that it would take them more than 12 months to do so. In aggregate, however, **96%** of this year's respondents either already have, are in the process of implementing or have plans in place to implement a cyber resilience strategy, a nearly identical percentage to 2021 (94%) and ahead of the 2020 total (93%). So, viewed through this lens, the level of cyber preparedness is very high and hasn't declined at all.

But why then is the percentage of organizations that already have a cyber resilience strategy in place trending downward? One probable explanation is that the goal posts have moved. Confronted with both a sharp rise in the pervasiveness and perniciousness of the attacks that they face, **cybersecurity professionals are likely to have redefined what it means to be cyber resilient**. The level of preparedness deemed adequate prior to the COVID pandemic is seen as inadequate today, given the increased reliance on email and other collaboration tools, and the more treacherous threat landscape.

Supporting this are the findings that **more than a third** of the 2022 respondents blame an insufficient degree of cyber resilience for interfering with overall employee productivity (39%), loss of data (38%), business disruptions (35%), financial losses (33%) and damage to their company's reputation (31%). Moreover, these consequences are becoming more widespread over time. For example, only 24% of companies attributed any financial losses to their lack of cyber preparedness in 2020, compared with **33%** today.





Fewer than half of respondents' companies have a system in place for monitoring email attacks.

Some Countries and Industries Are Better Prepared

The survey data also reveals large discrepancies in the level of cyber preparedness among different countries. In the U.S., which was ground zero for many of the most damaging and far-reaching cyber onslaughts in 2021, nearly half of the organizations surveyed (**47%**) have a cyber resilience strategy in place. Saudi Arabia, Germany and Denmark are not far behind (44%, 43% and 42%, respectively), but countries like Sweden and the Netherlands lag dangerously, with only about one in four (26% and 21%) of their respondents' companies having already implemented a cyber resilience strategy.

Similar discrepancies also appear among different industries. For instance, while close to half of financial services companies (47%) already have a cyber resilience strategy, the same is true for just 27% of companies in the media and entertainment sector.

These differences fade, however, when the number of companies that are actively preparing a resilience strategy or planning to do so is taken into account. In both the U.S. and the Netherlands, for example, nearly every organization surveyed (97%) either has, is currently implementing or has plans to implement a cyber resilience strategy over the next 12 months.

Not surprisingly, a very similar pattern emerges regarding the different types of cybersecurity systems companies either have or are planning to deploy. Fewer than half (**47%**) of the respondents' companies have deployed a system for monitoring and defending against email-borne attacks or data leaks in internal-to-internal emails. But when you take into account the additional **27%** who are in the process of rolling one out, the **19%** who expect to do so within the next year and the **6%** of respondents who say they are planning to deploy one more than 12 months from now, **99%** of SOES participants either have or plan to install an email security system of this nature.

Here, too, there are significant differences among industries, with some sectors moving to deploy email security protections more quickly than others. This is true, for example, for both the financial services and IT and technology sectors, where well more than half (**57%** in each sector) have already implemented such systems.

47% of financial services companies already have a cyber resilience strategy

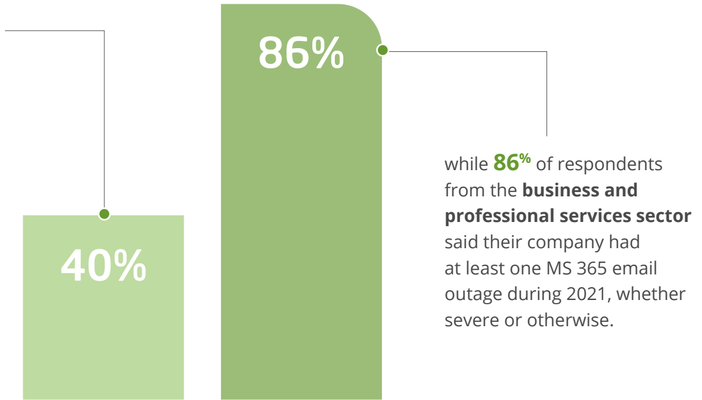
the same is true for just **27%** of companies in the media and entertainment sector.

Additional Protections Needed for Microsoft 365

Notably, **90%** of survey participants feel that additional safeguards are needed for Microsoft 365. Nearly 8 out of 10 respondents (**79%**) reported that their organization suffered an MS 365 email outage in the past year, and nearly a third (**30%**) characterized it as severe.

Again, some industries were hit harder by these than others:

Severe outages were experienced by **40%** of respondents from the **IT and technology sector**



while **86%** of respondents from the **business and professional services sector** said their company had at least one MS 365 email outage during 2021, whether severe or otherwise.

Artificial Intelligence and Machine Learning: Becoming Part of Cybersecurity's Natural Ecosystem

During the time between the SOES 2021 and 2022 surveys there has been a **notable increase** in the number of respondents whose companies are **incorporating artificial intelligence and machine learning** into their cybersecurity efforts.

Specifically, in the 2021 study, 38% of participants said they were currently making use of some combination of AI and ML, with another 49% indicating they were preparing to do so, for a total of 87%. In the just-completed 2022 survey, **46%** said they were already using these technologies with another **46%** planning to follow suit, for a total of **93%** when rounding is taken into consideration.

The eight-point swing among those respondents whose companies are already making use of AI and ML is particularly revealing.

This trend is even more marked within certain industries. For example, but perhaps unsurprisingly, **63%** of this year's respondents from IT, technology and telecom companies indicated that these leading-edge technologies have already found a home in their cybersecurity program.

Among the benefits attributed to these technologies, more than half (**56%**) of respondents from companies with some type of AI or ML technology in place said they had increased the accuracy of their threat detection; **48%** said their threat prevention efforts had improved, and **46%** noted that human error on the part of the cybersecurity team had been reduced.

The Cybersecurity Budget Gap Is Small But Significant

One reason why some companies have been slow to deploy cybersecurity systems and develop a cybersecurity strategy has been **budgetary limitations**. When asked what portion of their company's IT budget was allocated to cyber resilience versus how much should be allocated, the respondents, on average, indicated that 14% of their organization's IT budget was set aside for cybersecurity but that a 17% allocation would be optimal.

This discrepancy was much greater in some countries. In South Africa, for instance, the average IT budget for cyber resilience was only 12% when, according to respondents there, a 21% allocation was needed. In certain sectors, on the other hand, there is very little stinting on cybersecurity. Respondents from the IT and tech sector, for example, said that on average 18% of the IT budget goes toward cyber resilience, which they consider the full allocation that's required. In other words, when it comes to cybersecurity, the shoemaker's children are getting all the shoe leather they need.

While a 3% under-allocation may not seem like much, this year's SOES respondents with a budget shortfall were nearly united (**95%**) in agreeing that their organization's cyber resilience has been impaired as a result. Missing out on new technology innovations such as AI (**49%**), and improvements to existing cybersecurity solutions (**49%**), as well as lack of investment in cybersecurity training for staff (**46%**) were cited as the most common consequences.

There is cause for optimism, however. Several recent industry surveys have found that **many companies are planning to increase their cybersecurity budgets this coming year.** A November '21 study by the Neustar International Security Council, for instance, found that 81% of organizations are planning to add to their cybersecurity budgets in 2022—with nearly one out of four (24%) anticipating very large increases of 31% to 50%.[10] A slightly more modest forecast was issued by PwC, which projects that **69%** of organizations will up their cybersecurity spending in the year ahead.[11]

95%

of this year's SOES respondents with a budget shortfall were nearly united (95%) in agreeing that their organization's cyber resilience has been impaired as a result

Government Mandates Driving a New Environment

Many respondents are also hoping that their efforts to bolster their organization's cyber resilience will soon carry the weight of a government mandate.

In the U.S., for example, the Biden administration has issued an executive order that requires federal agencies and many private companies to meet new standards for cybersecurity. Similarly, in Europe, recent legislation will require many companies to certify that their cybersecurity measures meet certain minimal standards. Similar developments are also occurring in the Asian-Pacific region, where many countries are implementing data privacy and security requirements modeled after the European Union's General Data Protection Regulation (GDPR).

Nearly three out of four SOES respondents (**73%**) believe that these mandates and others like them will lead to high or moderate levels of improvement in their organization's level of cyber preparedness. They also think (**72%**) government requirements will induce senior management to take cyber resilience more seriously.

There is a downside, however, as **two-thirds of the respondents also say that such mandates will increase their costs** (69%) and limit their freedom to take the best course of action on behalf of their business (64%) to a high or moderate extent.

But even the best, most carefully calibrated cyber resilience strategy will fall short if the company's employees are unprepared to respond to an attack, and at many organizations a dearth of cyber awareness training is the biggest chink in their armor.

Most respondents are warily embracing government cybersecurity mandates.

PART FIVE:

Security Awareness Training: AN ACHILLES HEEL

Cyberattacks that spread from one infected employee to others are on the rise. **More than 8 out of 10** SOES participants report that in the past year their organization was the victim of such an attack. Moreover, this was fully 10 points higher than before (83% this year vs 73% in the 2021 survey) and well above the levels seen over the six years since the annual SOES study began.

When asked to name the worst security mistakes made by their organization's employees that would contribute to this spread, 83% of respondents called out poor password hygiene, 81% pointed to misuse of personal email and 76% identified use of collaboration tools. When asked what they expected their biggest security challenges to be in the coming year, **40%** of the respondents said one of their biggest concerns was employee naivete.

These anxieties are **backed up by Mimecast research**, which shows that more than 90% of security breaches involve some degree of human error. But that same research shows that in most cases it is both unfair and unreasonable to blame the people who committed those errors. The real issue, as demonstrated time and again by numerous studies, is whether those employees were properly prepared to deal with an attack. One example: Employees who receive consistent cyber awareness training are **five times more likely** to spot and avoid clicking on malicious links.

When asked to name the worst security mistakes made by their organization's employees

83% called out poor password hygiene

81% pointed to misuse of personal email

76% identified use of collaboration tools

Training Is Headed Sideways

Under these circumstances, it would be reasonable to expect companies to be stepping up the amount of cyber awareness training they provide to their employees, and by some measures this appears to be the case. Fully **99%** of the SOES respondents indicated that their company provides some form of training to help their workforce spot and respond to a cyberattack.

But in other respects, these efforts appear to be going in the wrong direction. When asked if their company provides certain types of cybersecurity training — such as group training sessions, formal testing, email prompts, interactive videos and one-on-one sessions with experts — for each category fewer respondents answered in the affirmative than the year before. In most cases, the percentage was the **lowest it has been** for the past four years.

Counterintuitively, this was especially true for the highly vulnerable healthcare and public sectors. For instance, while **54%** of respondents overall said their company offers group training sessions to employees, only **50%** from healthcare organizations and just **44%** from the public sector said the same. Likewise, while **39%** of all survey respondents indicated that their company offers one-on-one security training sessions to employees, this was true for only **35%** of healthcare sector respondents and a mere **26%** of those from the public sector.

On the bright side, those **organizations with a cyber resilience strategy in place are faring better**. For example, while fewer than one in four (23%) of the SOES survey takers said that their company provides cyber awareness training on a regular, ongoing basis, the number rose to more than a third (36%) for those from companies with a cyber preparedness strategy.

Fewer than one in four (23%) of the SOES survey takers said that their company provides cyber awareness training on a regular, ongoing basis

The number rose to more than a third (36%) for those from companies with a cyber preparedness strategy

Companies want more cyber-aware employees, but they haven't stepped up to train them.

PART SIX:

Brand Spoofing: Another Thorn in the Side

Online brand spoofing and impersonation remains a persistent danger. Among SOES 2022 participants, nearly half (46%) reported an upswell in this type of fraud year-over-year.

Respondents said their companies had experienced an average of **10** such attacks during the past year, although this was even higher for some countries and industries. In Germany, for instance, the average number of spoofing attempts reported was 16, while for both the healthcare and financial services sectors it was 12, and for the energy sector it was 13.

Just how seriously companies take this threat is evidenced by the number that have an in-house or third-party service in place to detect instances of brand mimicry and counterfeit websites. More than three-fourths of respondents (**76%**, up from 72% the previous year) said their organization was already making use of such a service, and that number rises to a nearly unanimous **98%** of all respondents when organizations that are currently rolling out or planning to roll out a monitoring service are included.

Companies have also readied themselves to deal with attacks that spoof their email domains. Fully **95%** of respondents said their organization is at least somewhat prepared to cope with this type of threat, and nearly a third (32%) consider their company fully prepared. For companies that are less than fully prepared, the chief reasons cited were insufficient resources (40%) and inadequate technology (43%).

Making Use of DMARC

Companies are also making use of Domain-based Message Authentication, Reporting and Conformance (DMARC) to protect their brands.

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

Approaching nine out of 10 respondents (**89%**) say their organization is either already making use of, in the process of implementing or considering implementing DMARC within the next 12 months, well up from the 85% that indicated this in the year-ago survey.

Online brand impersonation and mimicry **is on the rise**

PART SEVEN:

Top 10 TAKEAWAYS

Stepping back, what can we conclude from this year's survey results? Ten important lessons stand out:

1. There's no other way to say this: The cyber threat landscape is dire.

Most companies are bracing for an email-based attack that could cause them considerable harm. Nearly three out of four respondents report that the already sky-high level of email-related cyber threats is continuing to rise, and the majority say these attacks are becoming increasingly sophisticated.

2. Everyone has a phish tale — and they're all true.

During the past year, virtually every company surveyed was the target of a phishing attack, with the majority reporting that these are occurring more frequently. And while phishing is the most common email-borne threat, data leaks and business email compromise attacks are not far behind: More than 9 out of 10 respondents acknowledge that their organization has been subjected to these types of incursions.

3. The data thieves are winning.

In 2020, per the SOES respondents, fewer than two in three companies suffered a ransomware attack; during 2021, it was 3 out of 4. As a result of these attacks, nearly half (48%) of these companies were out of business for a week or more. Worse still, to recover their data, nearly 2 out of 3 were forced to pay the ransom.

4. Companies are more awake to the need for cyber defense

There is heightened awareness that a lack of cyber preparedness is a major risk factor. Virtually all respondents (96%) report that their organization either already has or is well into the process of developing a strategy for cyber defense. Nevertheless...

5. Too many companies are still cyber-unprepared

While nearly every company surveyed is at least thinking about the need for a cyber resilience strategy, only a little more than a third actually have one in place. In the meantime, a large group of respondents attribute a host of ills to their organization's lack of preparedness, from lost data and lower employee productivity to financial losses and business disruptions.

6. Companies are paying for cybersecurity — but need to pay more.

Most cybersecurity professionals are not pleading poverty. On average, SOES participants say there's only a small difference between the budget they need and the budget they have. Yet that discrepancy is having an outsized effect: This year's respondents overwhelmingly blame budgetary limitations for undermining their preparedness. Among the biggest casualties were sufficient funds for cyber awareness training and important new technologies such as AI.

7. Using MS 365 for email is not a cyber resilience strategy.

Will the security defenses that come with Microsoft 365 protect a company from email-borne cyberattacks? Not according to the 9 out of 10 SOES respondents who believe that additional safeguards are needed. Underscoring their argument, nearly as many said their company had experienced an MS 365 email outage this past year.

8. AI and machine learning are giving cybersecurity a big boost.

Nearly half of respondents have already incorporated some type of machine learning or AI into their cybersec defenses, and close to the other half are preparing to do so. Benefits ascribed to these technologies include better threat detection and fewer human errors.

9. Don't blame employees — give them better training.

Companies are aware that employees who aren't prepared to deal with a cyberattack pose a major threat to their security. More than 8 in 10 respondents said their companies fell victim to attacks that spread from one employee to another, and 4 in 10 consider employee naivete one of their greatest email security challenges for 2022. Yet when it comes to actually preparing their employees to identify and respond to cyberthreats, these organizations are only doing a so-so job. Although virtually all the SOES respondents said that their company provides some sort of cyber awareness training, most do not offer it on a regular, ongoing basis. Even more disconcerting, the number of companies offering various specific training initiatives — such as group training and one-on-one training sessions — have declined year-to-year.

10. No rest for the weary: Online brand impersonation is on the upswing.

Efforts to spoof companies' websites and email domains are on the rise, and respondents reported that their companies experienced an average of 10 such attacks this past year. But the response to this has been robust. Nearly every company surveyed is using or planning to use a service to monitor these threats, and the great majority feel at least somewhat prepared to deal with them. Nine out of 10 companies are also employing the DMARC protocol to protect their brands or looking to do so in the next 12 months.

PART EIGHT:

The BOTTOM LINE

No bank would ever dream of storing its cash and other valuables outside a timed vault with four-inch-thick steel walls, and no big box store would ever operate without security cameras. Yet today, even as we continue our gallop toward a digital economy, there are still companies that leave their digital assets unguarded. This reflects the old mentality that only things with tangible physical value need protection. But we live in a time when, every day, the digital intangibles count for more.

Bitcoins, account numbers, customer contact info and transaction data are the real wealth of today's society. Data, after all, is now called "the new oil," which explains why ransomware is such a big threat. And just like we recognize that an unlocked door or window is an open invitation to a thief, we need to realize that unmonitored email, unencrypted data and untrained employees are just as big an invitation to a cybercriminal who is after assets that are much more valuable.

Indications from the 2022 SOES report are that this awareness is finally taking hold, even though companies and institutions are still struggling to secure their digital wealth as diligently as their physical assets.

Our society needs to inoculate itself from digital threats — and, fortunately, the means to do so is at hand. But it's still up to organizations and individuals to take the cure.

About the Survey Results Included in this Report

For our 2022 report on the state of email security, Mimecast commissioned research firm **Vanson Bourne** to conduct a global survey of 1,400 information technology and cybersecurity professionals from 12 countries: the U.S., Canada, U.K., Germany, the Netherlands, Sweden, Denmark, Saudi Arabia, the United Arab Emirates, South Africa, Singapore and Australia.

Participants were surveyed between October and November of 2021 from companies ranging in size between 250 to 500 employees (14% of the total) and more than 10,000 employees (8% of the total). These companies were spread across 12 industrial sectors with healthcare (18%), the public sector and education (13%), financial services (11%), technology and telecommunications (10%), manufacturing (8%) and retail (8%) the most prominent among them.

Among the participants, CIOs, CTOs, CISOs, IT Directors and IT Security Directors comprised 63% of the total. The remainder included IT and SOC managers, as well as security architects and analysts.

1 "**Q3 First-Half Data Breach Analysis**," Identity Theft Resource Center

2 "**2021 Data Breach Investigations Report**," Verizon

3 *Ibid*

4 "**How to Reduce the Risk of Phishing and Ransomware**," Osterman Research

5 "**Extortion Payments Hit New Records as Ransomware Crisis Intensifies**," Palo Alto Networks

6 "**Insights to help you quantify security risk**," IBM

7 "**Cost of a Data Breach Report 2020**," IBM

8 "Gartner Press Release, "**Gartner Survey Finds 88% of Boards of Directors View Cybersecurity as a Business Risk**," November 18, 2021. **https://www.gartner.com/en/newsroom/press-releases/2021-11-18-gartner-survey-finds-88-percent-of-boards-of-directors-view-cybersecurity-as-a-business-risk**

9 "**Global Ransomware Damage Costs to Exceed $265 Billion by 2031**," Everyone's Internet News Presswire

10 "**Survey Results**," Neustar International Survey Council

11 "**2022 Global Digital Trust Insights Survey**," PwC

mimecast®

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.