February 2023

MARKET REPORT

2023 email security trends

The prevalence, impact, and cost of email-based cyberattacks on organizations around the world »

Barracuda
Your journey, secured.

aws PARTNER

- Public Sector
- Authority to Operate
- AWS Marketplace Seller
- AWS GovCloud (US) Delivery
- Security Software Competency

Contents

Introduction

Email attacks: enduring, diverse, and disruptive

Email is a top target for cyberattack. These attacks continue to evolve, harnessing machine learning to take advantage of the trust between colleagues and companies and to bypass basic security measures. Barracuda's research team has identified 13 email threat types that companies need to defend against.

Our international survey into email trends provides an overview of the prevalence, impact and costs associated with email attacks in the last 12 months.

Overall, 75% of the organizations surveyed had fallen victim to at least one successful email attack in the last 12 months. The impact of those attacks was wide ranging but invariably disruptive and costly, including downtime and business disruption (affecting 44% of those surveyed), the loss of sensitive data (43%) and damage to brand reputation (41%).

Different industries were affected in different ways. Financial services organizations lost valuable data and money to the criminals, while for healthcare the costs of quickly restoring systems were significant. Manufacturing was particularly affected by the disruption of business operations. Companies with more than half their employees working remotely faced higher levels of security risk and attack costs.

For 82% of respondents, the costs associated with an email attack have risen over the last year and now stand at more than $1 million on average for the most expensive attack.

Many of the organizations surveyed felt they were not fully prepared to deal with top security threats such as malware/viruses (34%), ransomware (27%) and even simple threats like spam (28%).

But it is not all bad news. The survey also found that 26% overall had increased their email security investments, and 89% felt their systems and data are more secure than 12 months ago. Growing awareness and understanding of email risks and the need for robust protection is a positive starting point for email security in 2023.

Methodology

Barracuda commissioned independent market researcher Vanson Bourne to conduct a global survey of IT managers and technical IT professionals, senior IT security managers, and senior IT and IT security decision-makers. There were 1,350 survey participants from a broad range of industries, including agriculture, biotechnology, construction, energy, government, healthcare, manufacturing, retail, telecommunications, wholesale, and others. Survey participants were from the U.S., Australia, India, and Europe. In Europe, respondents were from the United Kingdom, France, DACH (Germany, Austria, Switzerland,) Benelux (Belgium, the Netherlands, Luxembourg,) and the Nordics (Denmark, Finland, Norway, Sweden). The survey was fielded in December 2022.

The report references Barracuda-commissioned research published in 2019. That market research included responses from 660 executives, individual contributors, and team managers serving in IT security roles in the Americas, EMEA, and APAC.

FINDING #1

Most organizations have experienced a successful email attack

Email is arguably the most important communication tool in business today. An estimated 333 billion emails or more were sent and received daily in 2022. It's not unusual for an average employee to have dozens of emails go in and out of their inbox daily. Unfortunately, familiarity with the tool leads to complacence and misplaced trust in email as a safe and secure communication channel.

Cybercriminals understand this well and leverage email in their attacks. As a result, email is one of the top threat vectors faced by organizations today because anyone can send an email to anyone else from anywhere in the world.

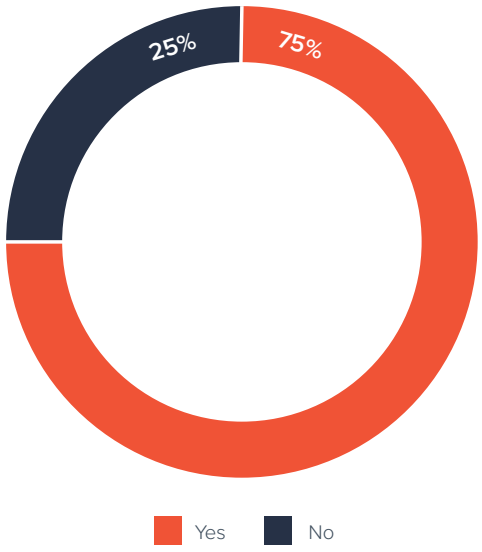
Email is not only an accessible and inexpensive tool for cybercriminals to use but also an incredibly effective one. Of the organizations surveyed in our study, 75% reported being the victim of at least one successful email attack in the last year.

> 3 out of 4 organizations have been a victim of a successful email attack.

These numbers are pretty consistent regardless of the size of their organization or the proportion of remote workers.

Has your organization faced any successful email-based security attacks in the past year?

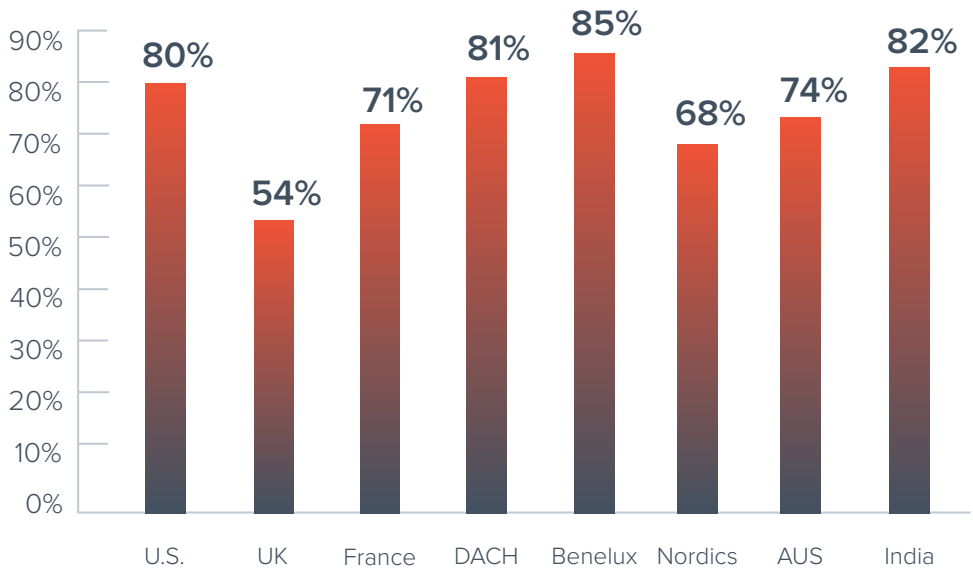
(n=1,350)



However, there are some significant variations by country, with the UK and the Nordic countries (54% and 68%) reporting lower levels of successful attacks. In comparison, organizations in India and the Benelux countries experienced rates above average (82% and 85%, respectively).

Has your organization faced any successful email-based security attacks in the past year?

(n=1,350)



FINDING #2

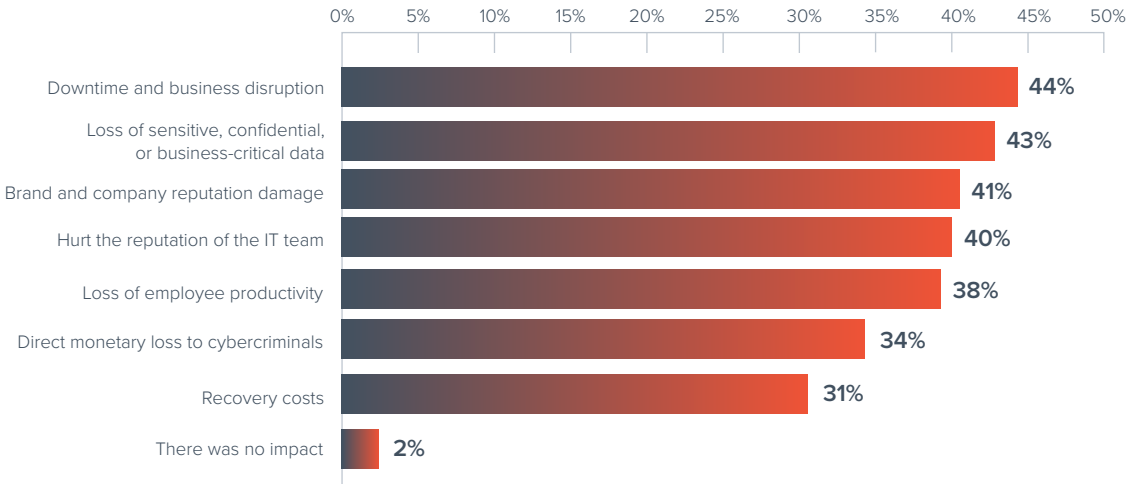
The impact of email attacks is becoming more noticeable

Practically every affected organization felt the impact of these email attacks. Only 2% said that email attacks did not affect their organization. This is a dramatic change from 26% of organizations reporting no impact in 2019, suggesting that attacks are becoming more successful and their impact is more noticeable within organizations.

Email security attacks on organizations bear many consequences, with the most severe effects being the most widely reported, including downtime/business disruption (44%), loss of sensitive data (43%), and reputation damage (41%).

What was the impact of these successful email security attacks on your organization?

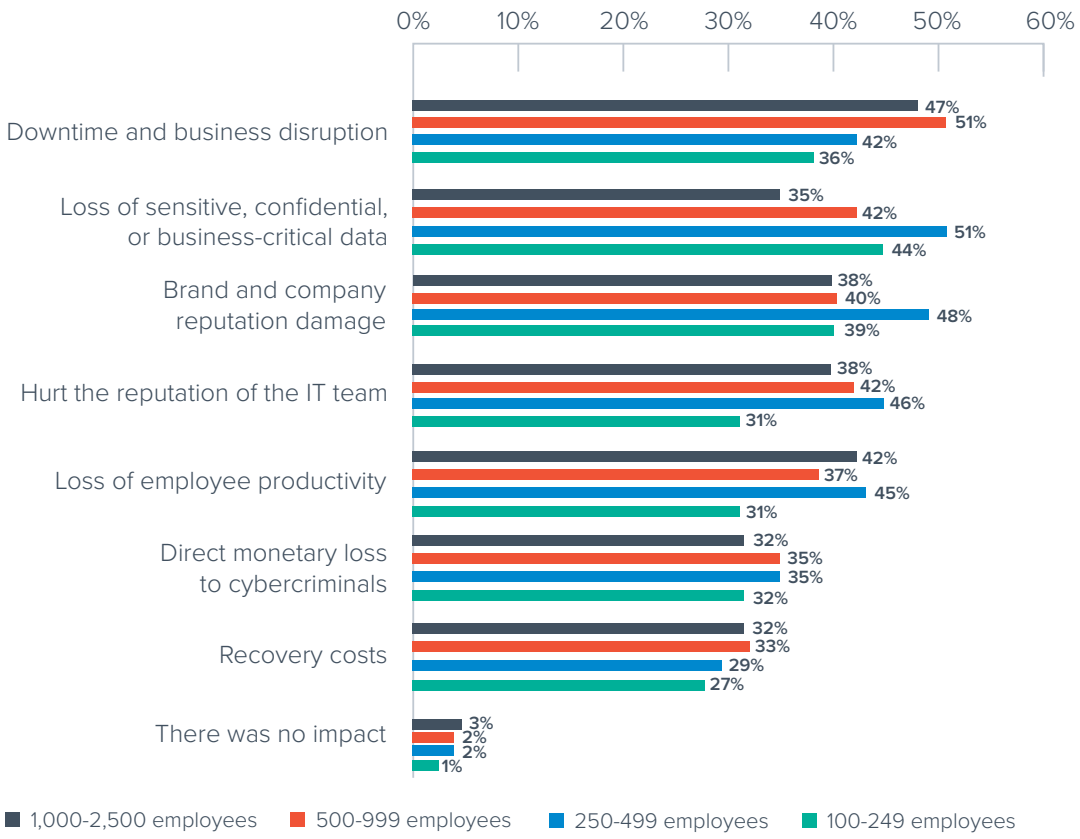
(n=1,012)



For the smaller companies surveyed, the most likely impact was the loss of sensitive or critical data (44% for those with fewer than 250 employees and 51% for those with 250 - 499 employees), followed by brand reputation damage (39% and 48%, respectively).

What was the impact of these successful email security attacks on your organization?

(n=1,012)



However, for the mid-size (500 - 999 employees) and large (1,000 - 2,500) organizations surveyed, the most common impacts were downtime/business disruption (51% and 47%, respectively) and loss of employee productivity (42% for those with more than 1,000 employees), and data loss and damage to the IT team's reputation (both 42% for those with 500 - 999 employees). This could suggest that larger organizations have more established brands and reputations that can withstand an attack, but they are hit harder in terms of business continuity.

FINDING #3

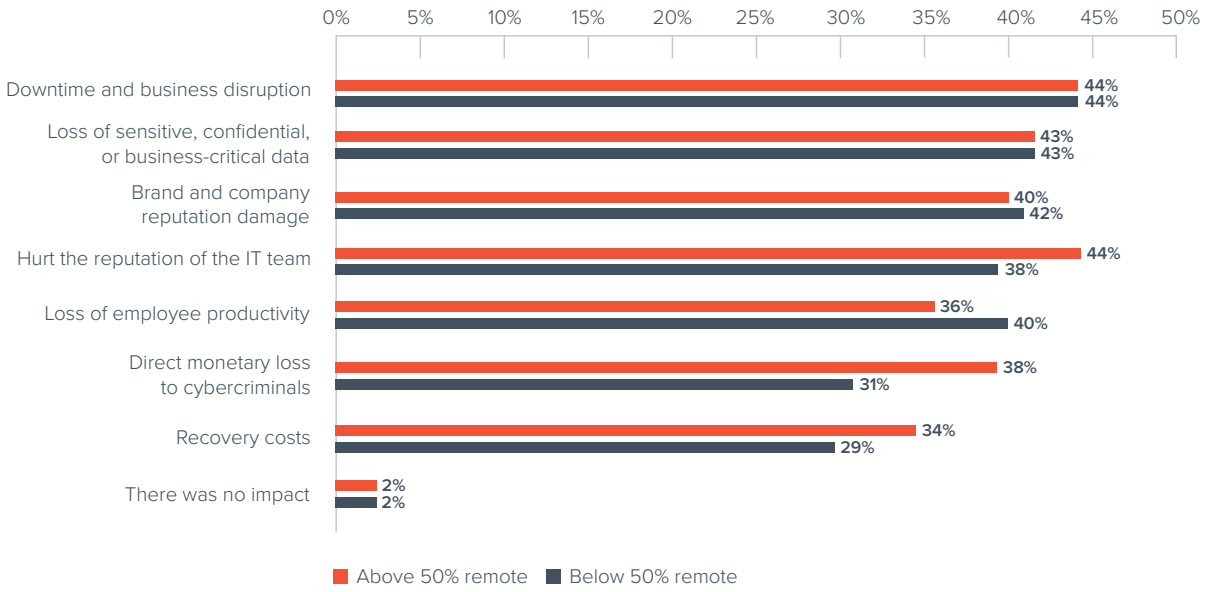
Remote work is contributing to higher monetary losses and recovery costs

Companies with more than 50% of employees working remotely are more likely to report monetary loss as an impact (38% vs. 31% for those with less than half working remotely) and higher recovery costs overall (34% vs. 29%).

The flexibility of remote work comes with increased risks. Organizations can't consistently enforce security policies on remote workers to ensure maximum protection. They have to allow remote access to business applications and critical data for employees to carry out their day-to-day jobs. A lot of the time, this access is even allowed from employees' personal devices. This not only increases the attack surface available to cybercriminals, but it can also significantly delay detection, response, and recovery from cyberattacks.

What was the impact of these successful email security attacks on your organization?

(n=1,012)



FINDING #4

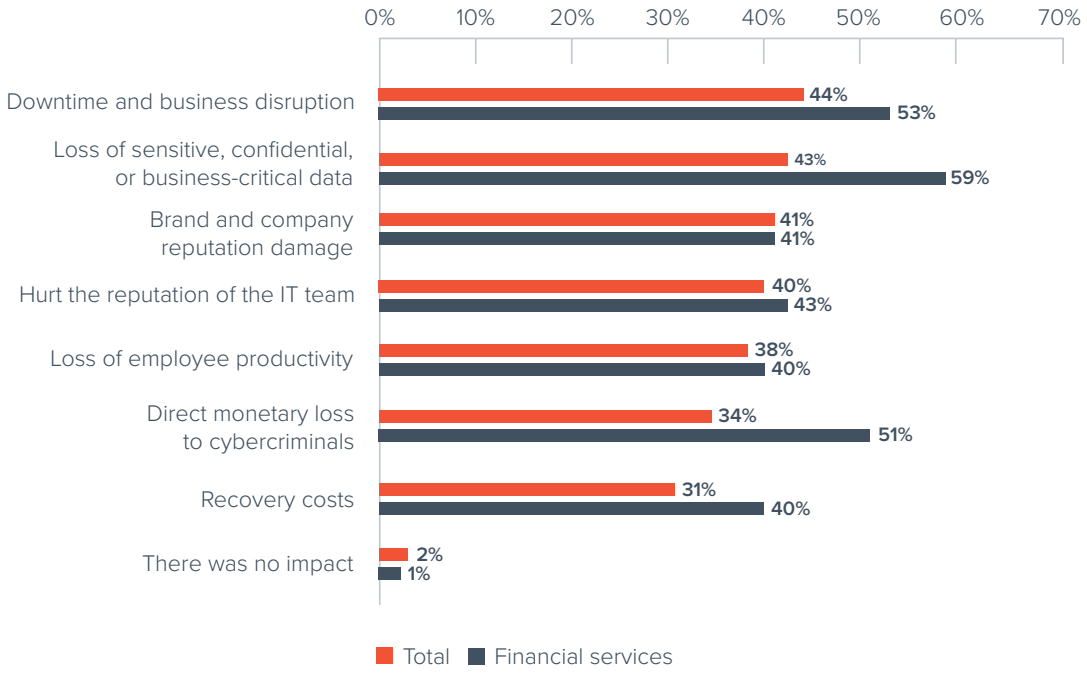
The impact of email attacks varies greatly by industry

Financial services

Financial services organizations hold two of the most valuable assets that cybercriminals are after — data and money. And that's exactly where most of the impact is felt. For example, 59% of the financial services organizations that have faced an email attack reported data loss, and 51% reported direct monetary loss to cybercriminals — think of all those fake wire transfers and deposits. Their recovery costs are also higher than average because of potential damage to their reputation, and the loss of customer trust may take a long time to rebuild.

What was the impact of these successful email security attacks on your organization?

(n=97)

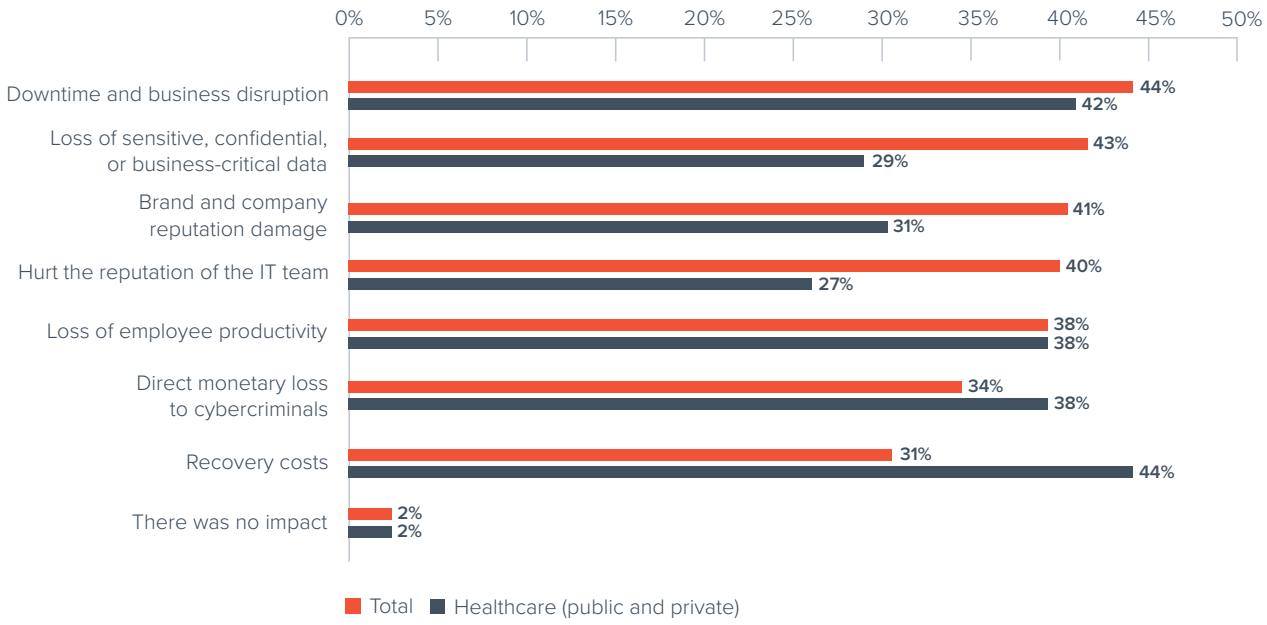


Healthcare

Healthcare institutions are under constant threat of cyberattacks — ransomware in particular. There have been many high-profile attacks on healthcare institutions over the years, and such attacks accelerated during the COVID-19 pandemic. This unfortunate experience led to healthcare becoming one of the best prepared industries to deal with the impact of cyberattacks. The recovery cost is high because healthcare infrastructure needs to be up and running again fast, as human lives literally depend on it. But they are a lot less likely to suffer from data loss (29% vs. an average of 43%) or reputational damage (31% vs. 41%). They are likely well prepared with exceptionally stringent policies around sharing, storing, and backing up all valuable medical data and other PHI (Protected Health Information).

What was the impact of these successful email security attacks on your organization?

(n=48)

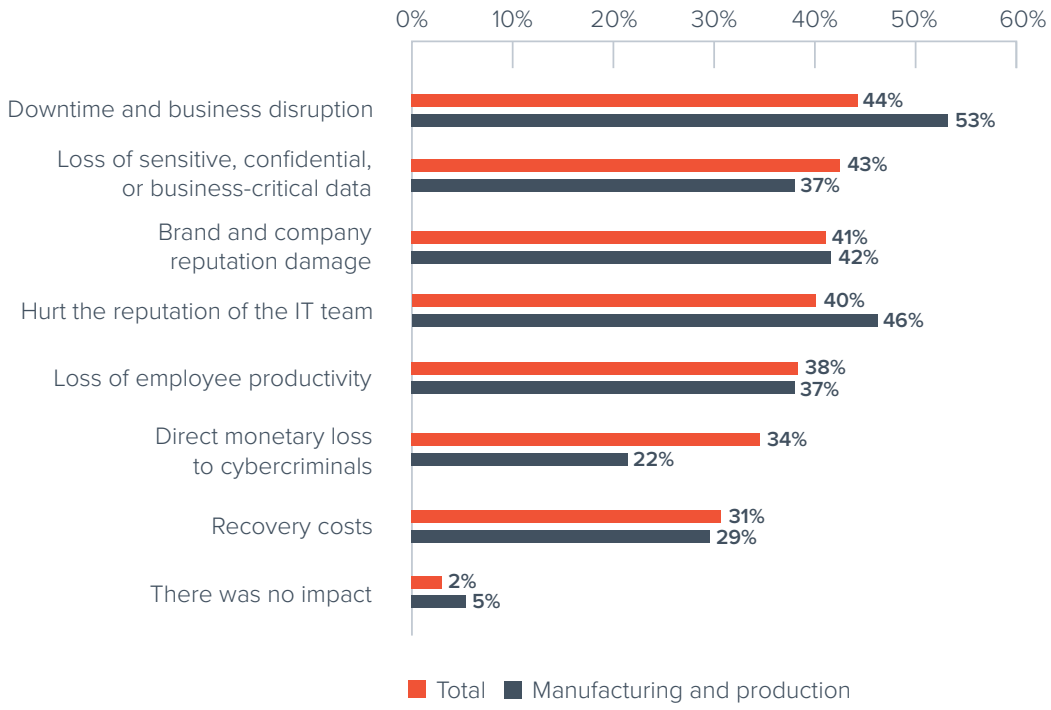


Manufacturing and production

Modern manufacturing depends on technology and automation, so it's not surprising that 53% of respondents in this sector said they experienced downtime and business disruption due to an email attack. However, direct monetary loss (22%) or loss of data (37%) were below average. This is because manufacturing doesn't hold the same amount of valuable data as financial services or healthcare; therefore, this kind of impact is not as noticeable.

What was the impact of these successful email-security attacks on your organization?

(n=79)



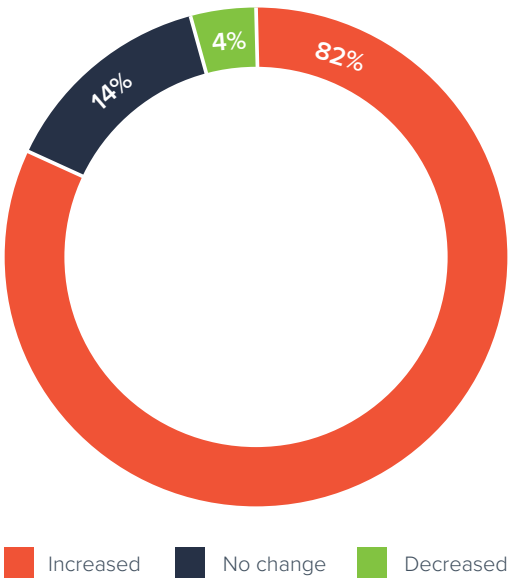
FINDING #5

The cost of an email security breach is rising

With rising costs in many areas of business, it is also no surprise that over 8 in 10 (82%) organizations that have experienced email security breaches report that these incidents cost them more than they did 12 months ago. Almost a quarter of these organizations (23%) have seen a dramatic cost increase.

How has the total cost of email security breaches changed over the past 12 months?

(n=1,012)



Compared to security spend

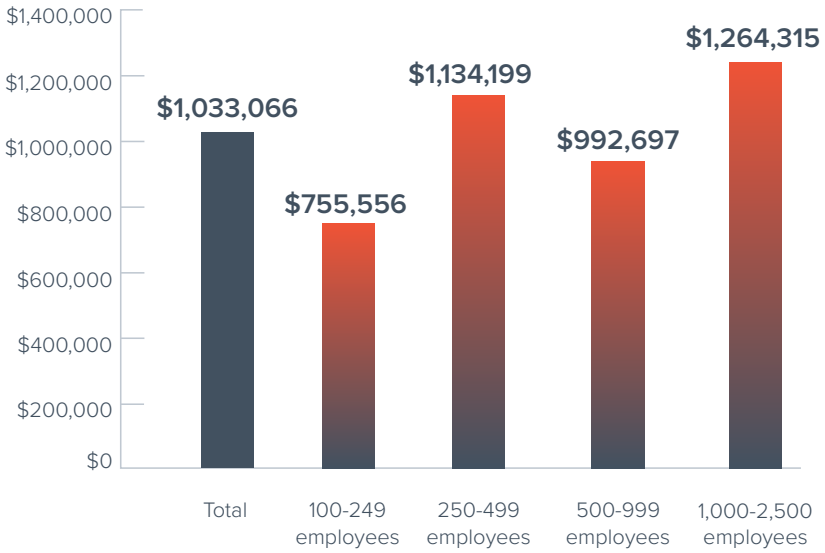
Organizations that say they invested more in email security in the past 12 months were more likely to report that the cost of attacks has increased. 93% of organizations spending more on security said the cost of attacks has increased. In comparison, 78% of organizations spending less on security felt the same. This suggests that the increased spending is a response to these rising costs and a way to mitigate the potential impact.

Organizations reported that the average cost of the most expensive email attack was over $1 million. This figure includes not only direct monetary loss, but also the cost of downtime, lost productivity and data, and reputational damage.

Costs associated with email attacks were more significant for larger organizations, but this kind of cost can have a disproportional impact on smaller businesses. According to public reports, 60% of small businesses that are victims of cyberattacks will go out of business within six months. Therefore, it's critical for all organizations to be prepared for cyberattacks and to plan ahead to minimize the impact and potential costs associated with a security breach.

Average cost of the most expensive email attack organizations experienced in the past 12 months

(n=1,012)



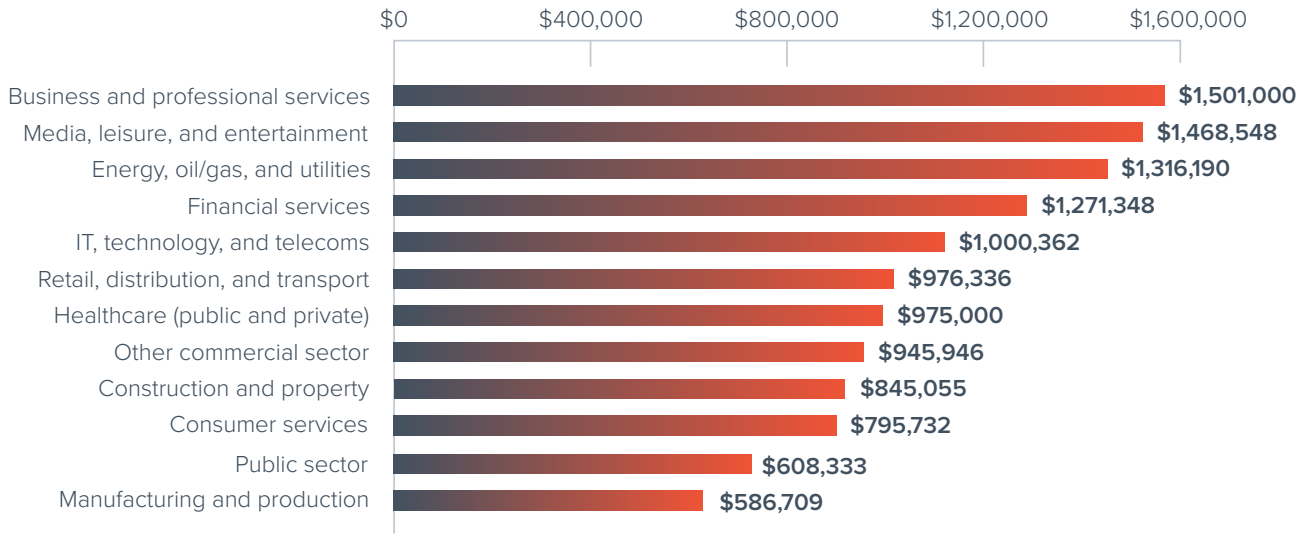
Industry variations

Organizations in industries that reported higher impact from direct monetary losses to cybercriminals and higher recovery costs (such as financial services and business and professional services) reported a higher than average total cost of email attack.

There have been a number of costly, high-profile data breaches involving critical infrastructure such as oil and gas. Colonial Pipeline ended up paying over $4 million in 2021 following a ransomware attack that began with a compromised password.

Average cost of the most expensive email attack organizations experienced in the past 12 months

(n=1,012)

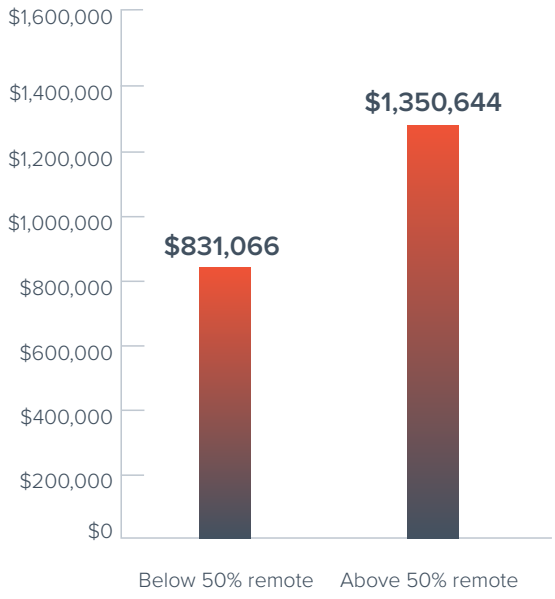


Proportion of remote workers

Costs are also significantly higher for organizations with a larger remote workforce. For example, those with 50% or more remote employees reported higher recovery costs (34%) and higher than the average direct monetary loss to cybercriminals (38%) — all of which contribute to the high cost of email attacks. IBM drew similar conclusions in their recent research — the cost of a data breach is higher for organizations with a larger remote workforce.

Average cost of the most expensive email attack organizations experienced in the past 12 months

(n=1,012)



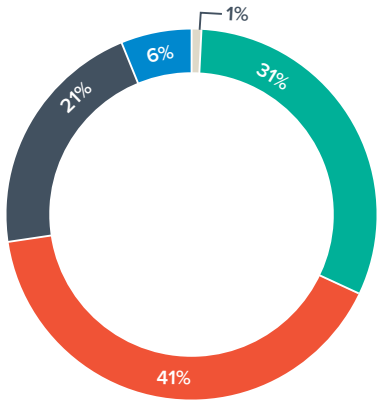
FINDING #6

COVID-19 has left organizations more concerned about email security

Concerns about email-based threats have been rising steadily over the years, and they accelerated during the COVID-19 pandemic. The early days of the pandemic in 2020 saw a 667% rise in COVID-related phishing attacks. A full 72% of organizations surveyed in our study reported that they are more concerned about email-based threats since the COVID-19 pandemic.

How did the COVID-19 pandemic change your organization's concerns about the email-based threats?

(n=1,350)



- Significantly more concerned now than before the pandemic
- Slightly more concerned now than before the pandemic
- About the same concerned now than before the pandemic
- Slightly less concerned now than before the pandemic
- Significantly less concerned now than before the pandemic

FINDING #7

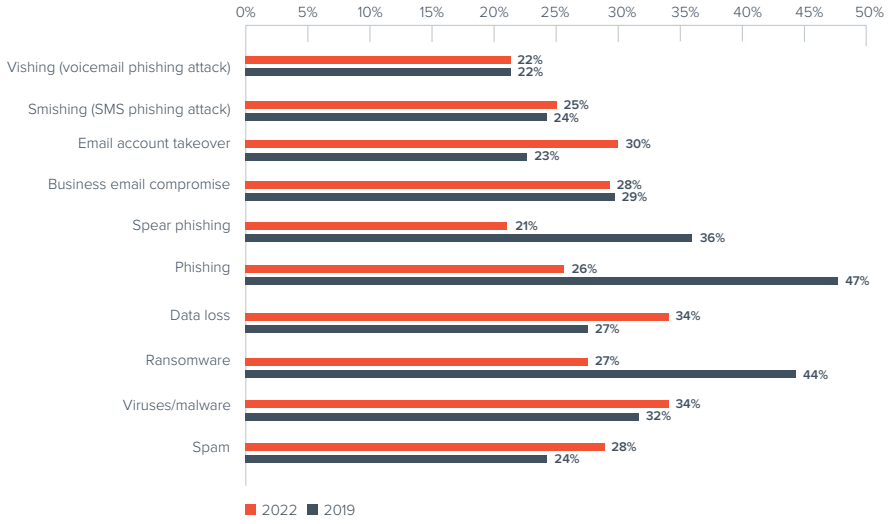
Organizations feel they are not fully prepared to deal with email-based threats

Nearly all respondents (97%) feel underprepared to deal with some of the most prevalent cyberthreats. Around a third (34%) feel poorly prepared to deal with data loss or malware, and over a quarter (27%) say the same about ransomware. In fact, 28% feel they are not even prepared to deal with less complex threats such as spam.

The good news is that, overall, organizations feel better prepared to deal with some of the more advanced threats like phishing, spear phishing, and ransomware than they did three years ago. However, they feel less prepared to deal with account takeover and data loss. Both security risks, unlike many others, require not only prevention but very robust detection and recovery strategies.

Which of the following security risks are you concerned that your organization is NOT fully prepared to deal with?

(n=1,350)



For example, while organizations may feel better equipped to prevent phishing attacks, they are not as prepared to deal with account takeover, which is usually a by-product of a successful phishing attack. Account takeover is also a bigger concern for organizations with the majority of their employees working remotely — 34% of such organizations are not fully prepared to deal with this threat.

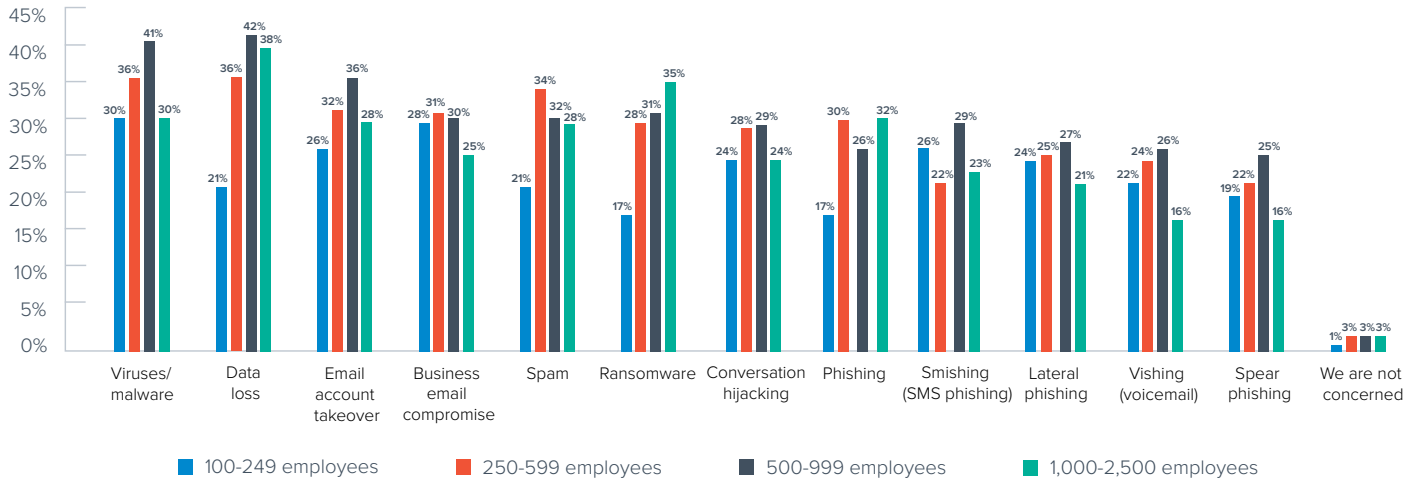
Company size variations in preparedness

Larger organizations feel less prepared to deal with most threats across the board. These businesses will have a lot of dispersed data and employees. Therefore, identifying all instances of attacks, estimating the scope of impact, and managing the recovery can be challenging.

Organizations with fewer than 250 employees feel particularly underprepared for viruses/malware (30%) and business email compromise attacks (28%). For most organizations, regardless of their size, one of the top concerns is data loss, closely followed by viruses/malware. Data is arguably the most valuable asset for most businesses today. Data loss will have a significant impact on productivity, reputation, and business continuity.

Which of the following security risks are you concerned that your organization is NOT fully prepared to deal with?

(n=1,350)



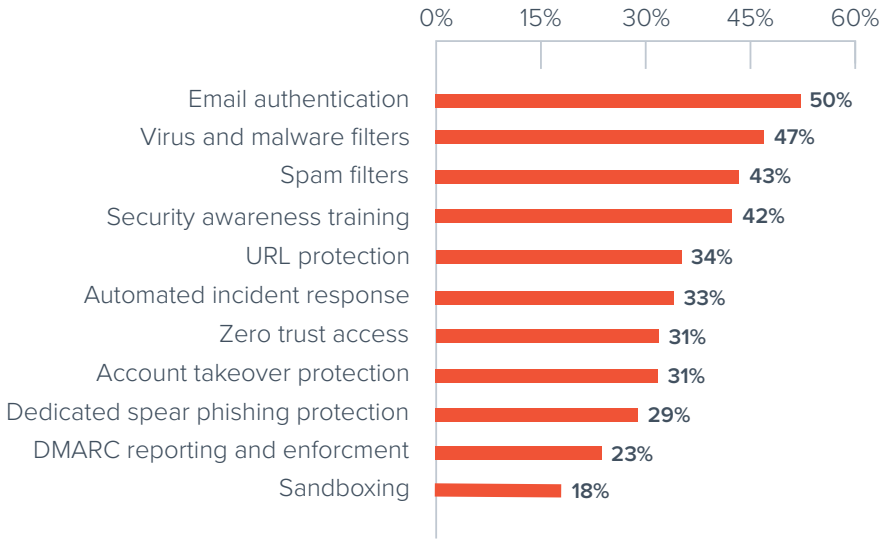
FINDING #8

Adoption of advanced email security tools is low

Organizations invest their email security budgets in a variety of technologies and tools to help protect their users. Email authentication (50%), malware/virus (47%), and spam protection (43%) are at the top of the list. These are usually part of email gateways that help block large-scale attacks from getting into users' inboxes. These widely adopted tools are closely followed by security awareness training (42%) to turn employees into a strong line of defense.

Which of the following types of email security technology does your organization have in place today?

(n=1,350)



Fewer organizations focus on protecting account access with account takeover protection (31%) or Zero Trust Access (31%), so it is not surprising that many businesses (30%) reported that they are not fully prepared to deal with account takeover. More advanced technologies — such as spear-phishing protection (29%), DMARC enforcement (23%), or sandboxing for zero-day attacks (18%) — that are used to detect targeted threats show low adoption. Organizations cannot fully protect themselves against these modern threats without investing in advanced security solutions. Smaller organizations are particularly vulnerable as they demonstrate the lowest adoption of all email security tools across the board.

FINDING #9

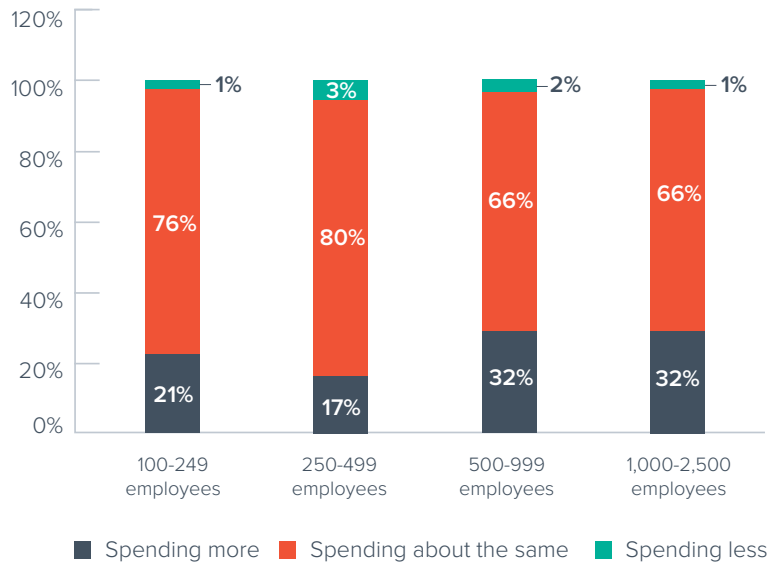
Many organizations are starting to invest more in email security

As email attacks are becoming more sophisticated and harder to detect, organizations are investing more in security to prevent and respond to such threats. A full 26% of organizations have increased their budgets regarding email security spending, and those that did say they feel more secure.

Larger organizations are more likely to have invested more in email security compared to the previous year. This is because they feel more exposed to email threats having a larger potential attack surface. Larger organizations also have more resources to invest in additional layers of security.

How does your organization's current spending on email security compare to last year?

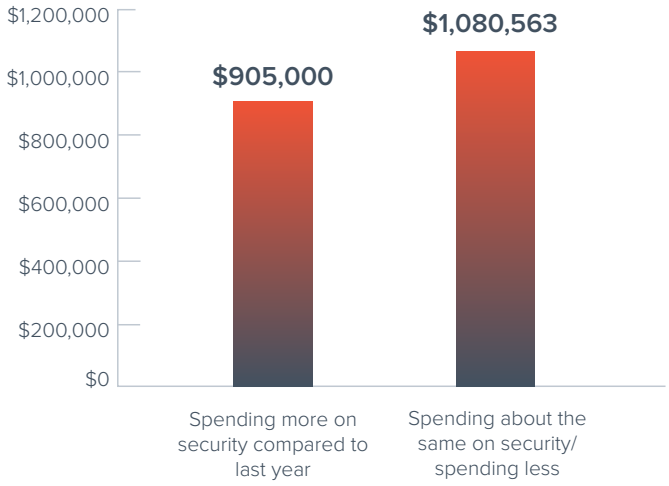
n=(1,350)



The survey also suggests that investing in advanced layers of protection can minimize the risk of a security breach and mitigate the cost of a breach should any data, accounts, or infrastructure be compromised. In fact, organizations that have invested in email security in the past 12 months reported lower costs associated with email attacks compared to those that have kept their spending the same or reduced.

Average cost of the most expensive email attack organizations experienced in the past 12 months

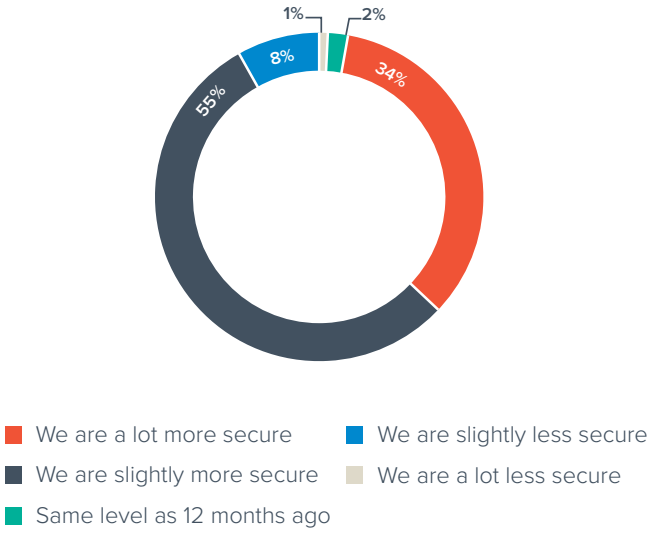
(n=1,012)



A total of 89% of organizations also feel that their systems and data are more secure than 12 months ago.

How secure do you feel your organization's systems and data are compared to 12 months ago?

(n=1,350)



Conclusion

As email remains a top vector for cyberthreats, IT and security professionals need to stay focused on the evolution of phishing, ransomware and other security threats. Here are the top five cyber security best practices that all organizations should put in place regardless of their industry to minimize their risk and exposure to cyberthreats and the impact of an attack:

- **Deploy multilayered email security.** Many organizations around the globe have reported that they feel underprepared to deal with even the simplest threats, such as spam and malware. Most organizations today will have robust spam and malware filters in place, however, they are not always properly configured to block malicious messages effectively. IT teams need to regularly perform a 'health check' on their email gateway settings to ensure optimal performance.

  As threats evolve, so should your protection. Scammers are adapting email tactics to bypass gateways and spam filters, so it's critical to have a solution in place that detects and protects against targeted phishing attacks. Supplement your gateways with machine learning technology that doesn't solely rely on looking for malicious links or attachments.

- **Protect users' access.** Protecting access and your users' accounts should be an integral part of your cybersecurity strategy. Start using multifactor authentication (MFA), which will provide an additional layer of security above and beyond username and password, such as an authentication code, thumb print, or retinal scan. Today, organizations should consider a more advanced Zero Trust strategy in which organizations continuously verify and only allow the right users to access the right resources. Deploying Zero Trust Access technology will protect access and reduce your exposure to lateral attacks.

- **Automate incident response.** An automated incident response solution will help you quickly clean up any threats found in users' inboxes, making remediation more efficient for all email messages going forward.

- **Improve cyber security awareness.** Educate users about spear-phishing attacks by making it a part of security awareness training. Ensure employees can recognize these attacks, understand their fraudulent nature, and know how to report them. Use phishing simulation for emails, voicemail, and SMS to train users to identify cyberattacks, test the effectiveness of your training, and evaluate the users most vulnerable to attacks.

- **Secure and back up all data.** Many organizations highlighted data loss as one of the biggest impacts of an email attack. Your data needs to be properly secured, isolated, and backed up. You also need to make sure that your data backup will allow you to restore data in a reasonable time frame. Make sure you run drills and test your data back up regularly to ensure you are fully prepared.

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-first, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level.

Get more information at barracuda.com.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and Their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit vansonbourne.com.

Barracuda
Your journey, secured.