October 2025

Market report

The Email Security Breach Report 2025

The experience and impact of email security breaches on organizations worldwide

Barracuda®
Your business, secured.

Contents

Introduction

This report explores the experience and impact of email security breaches on organizations around the world in the previous 12 months. It draws on the findings of an international survey of 2,000 IT and security decision-makers undertaken by Barracuda and Vanson Bourne. The results were largely consistent across all the countries and industries surveyed, so this report focuses on overall and size-related findings.

The findings show that email security breaches affect most organizations. They highlight how an increasingly complex email threat landscape and internal challenges such as skills gaps and a lack of automated incident response make it difficult for organizations to rapidly detect, respond to and recover from a breach.

Delayed response times can leave organizations vulnerable to other attacks, such as ransomware, and more widespread damage.

The impacts of an email security breach are far-reaching, ranging from downtime to reputational damage and lost business. The recovery costs hit smaller businesses especially hard.

The purpose of this report is to help organizations better understand the risks and implications of email-based security threats, and to highlight areas where they may be vulnerable.

Methodology

Barracuda commissioned independent market research company Vanson Bourne to conduct a global survey of 2,000 senior security decision-makers in IT and business roles in organizations with between 50 and 2,000 employees from a broad range of industries in the U.S., UK, France, DACH (Germany, Austria, Switzerland), Benelux (Belgium, the Netherlands, Luxembourg), the Nordics (Denmark, Finland, Norway, Sweden), Australia, India, and Japan. The fieldwork was conducted in April and May 2025.

Key findings

78%

of organizations experienced an email security breach in the previous 12 months

71%

of organizations that experienced an email security breach were also hit with ransomware during the year

41%

suffered reputational damage, and many lost new business opportunities, harming growth

50%

detected the breach within an hour

47%

say advanced evasion techniques are the main obstacle to rapid incident response

44%

say the lack of automated incident response delays the detection, containment and removal of threats

$217,068

is the average cost of responding to and recovering from an email security breach

Most businesses experience an email security breach

The survey found that 78% of respondents had experienced an email security breach in the previous 12 months.

Victims were hit with a broad range of attack types, including phishing and spear phishing (experienced by 27% of victims), business email compromise (experienced by 24%) and account takeover (22%).

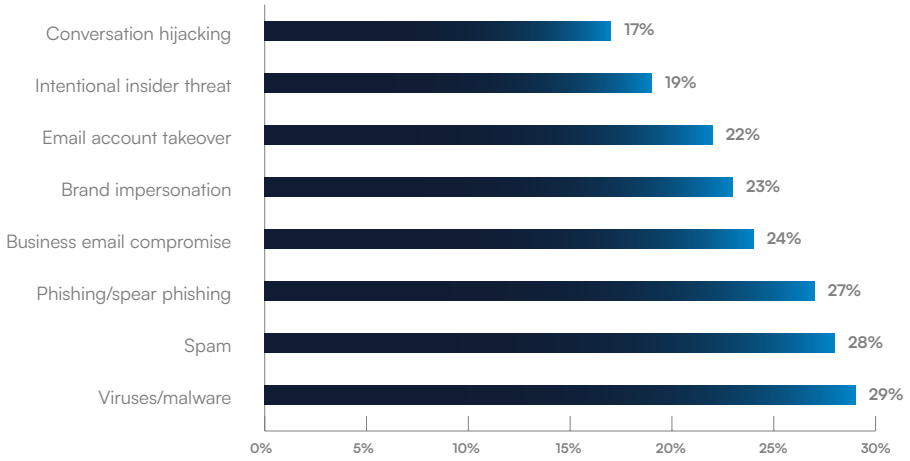


FIGURE 1

Which of the following email-based attack types has your organization been successfully breached by in the last 12 months?

The email threat landscape is further complicated by the fact that many email attack types are interrelated. Understanding these relationships is key to building effective defenses.

For example, phishing often acts as the initial breach point, opening the door to more advanced threats like business email compromise (BEC), account takeover and ransomware. Once credentials are stolen, attackers can impersonate internal users to make their emails appear more trustworthy and increase the likelihood of further compromise. Spoofing techniques enhance the effectiveness of phishing and BEC by mimicking trusted senders. Meanwhile, malware introduced through phishing can automate the attack process, harvesting additional credentials and spreading across the network.

BEC is a targeted and financially motivated threat. Attackers impersonate trusted individuals or entities to trick employees into transferring money or sensitive information. Malware and ransomware delivery are facilitated through phishing emails containing malicious attachments or links.

Impersonation and spoofing are techniques used to deceive recipients into trusting the sender. These tactics are commonly employed in phishing, BEC and malware campaigns. Attackers may use display-name spoofing, domain spoofing or lookalike domains to mimic legitimate contacts, increasing the chances that their messages will be opened and acted upon.

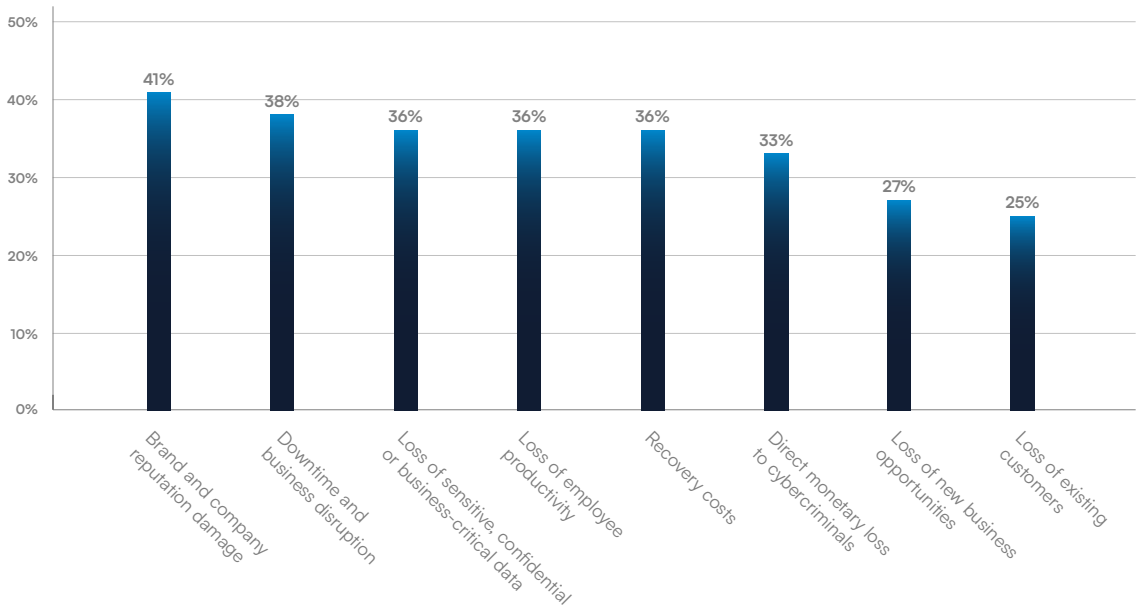
All types of email threats are growing in complexity, sophistication and reach. Many of the most widespread phishing campaigns are developed and delivered at scale by well-resourced platforms. **The damage these attacks can do is considerable.**

An email security breach harms business growth

According to the organizations surveyed, the most common consequence of an email security breach is brand and reputational damage (cited by 41% of respondents). This is followed by operational impact, including downtime and business disruption (affecting 38%), and reduced employee productivity (36%). Over a third (36%) lost sensitive data, and around a quarter lost new business (27%) and customers (25%).

FIGURE 2

What was the impact of email-based security breaches on your organization (overall)?



The consequences of reputational damage can extend far beyond short-term public perception and have a deep, lasting impact on an organization's financial health, legal standing and strategic direction.

The impact on business operations and productivity, as well as the financial losses, data loss (particularly if this leads to compliance and contractual breaches), theft of intellectual property, and erosion of trust can lead to a loss of existing customers and new business opportunities. This has a tangible impact on revenue growth.

It may be hard to put a number on the longer-term impact, but it is possible to quantify the cost of responding to and mitigating an email security breach.

The cost of fixing an email security breach hits smaller firms harder

An email security breach costs on average $217,068 to fix, with smaller businesses hit disproportionately harder.

The survey covered companies with 50 to 2,000 employees. The average mitigation cost incurred by companies with 50 to 100 employees was $145,921. For companies with 1,000 to 2,000 employees, the average mitigation cost was $364,132.

This means that the average recovery cost per employee for the smaller organizations (50 to 100 employees) is $1,946, compared to an average recovery cost per employee of just $243 for the larger organizations (1,000 to 2,000 employees).

	50-100 employees	101-250 employees	251-500 employees	501-1,000 employees	1,001-2,000 employees
Average cost per organization to mitigate the most expensive email security breach in the last 12 months	$145,921	$157,804	$155,804	$300,751	$364,132
Average cost per employee to mitigate the most expensive email security breach in last 12 months	$1,946	$898	$415	$400	$243

Larger organizations may have better defenses and more resources in terms of skills and staffing to detect and respond to security incidents. This makes them better equipped to handle breaches quickly and effectively, ensuring that each incident is less costly when compared to their overall size. Smaller organizations are far more exposed.

The ability to detect and respond quickly to security threats is critical for reducing risk exposure.

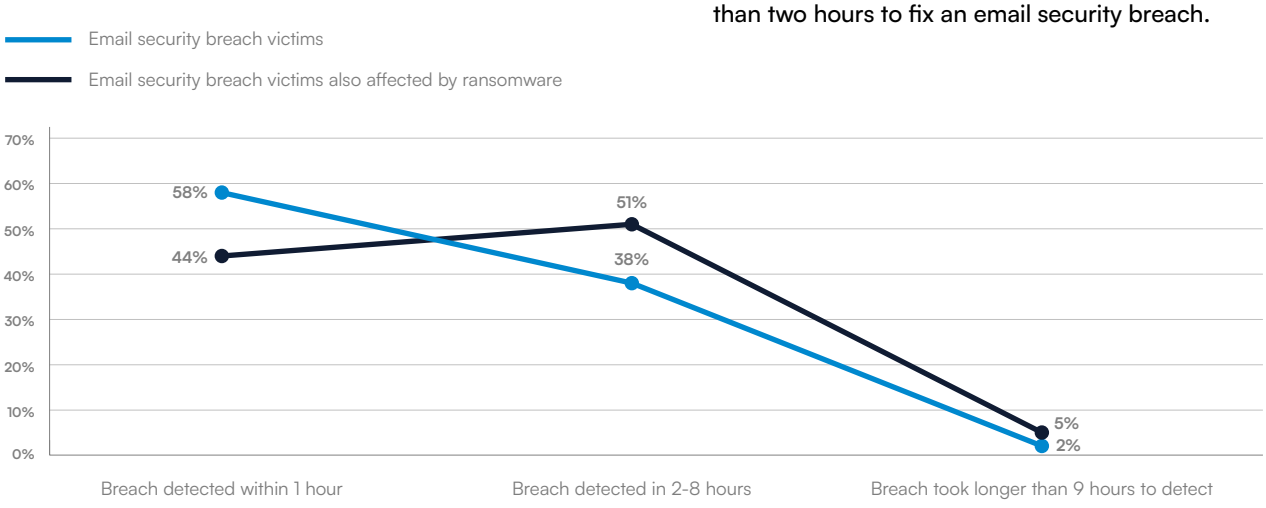
Delays in email breach detection and response times make ransomware more likely

There's a correlation between the time it takes an organization to detect and mitigate an email security breach and the chances of also being hit with a successful ransomware incident.

The research shows that 71% of organizations that experienced an email security breach report that they were also hit with ransomware in the last 12 months.

FIGURE 3

Average time taken to detect an email security breach



This could be because many ransomware attacks start with a seemingly innocuous phishing email that gives attackers a foothold — through stolen credentials or a compromised endpoint — and a channel to deliver ransomware and other malicious payloads through attachments and links.

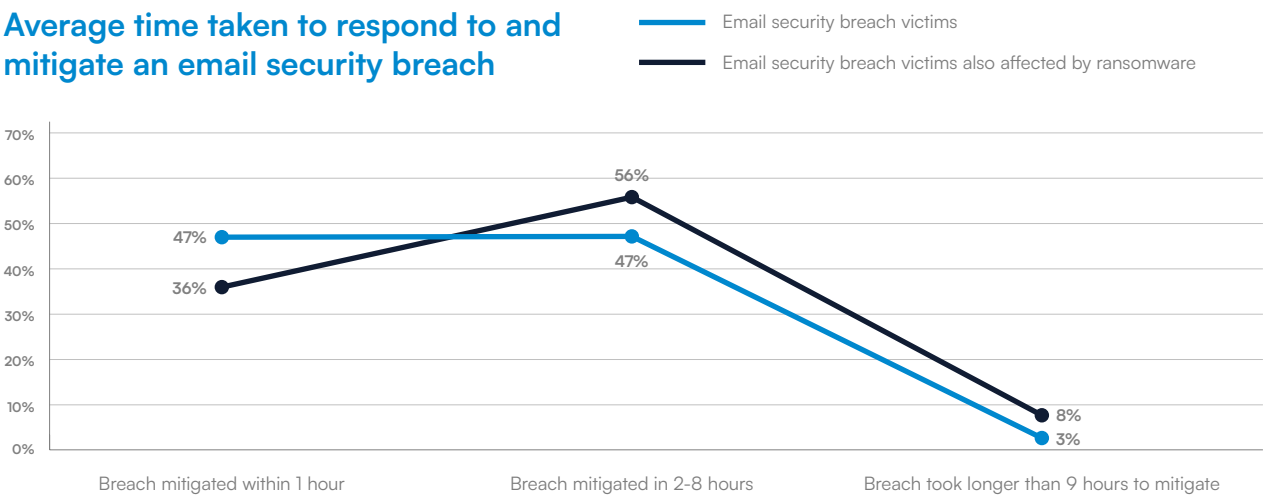
If an email security breach isn't detected and contained quickly and effectively, the attack chain has time to unfold, with the attackers able to steal data, encrypt files or establish persistent access to the network.

The findings show that organizations that took longer to detect and mitigate an email breach had a higher likelihood of also being affected by ransomware:

- 58% of email breach victims unaffected by ransomware took less than an hour to detect the breach.
- Just under half (47%) of them mitigated the threat within an hour of detection.
- However, for those victims that also experienced a ransomware incident, detection and mitigation often took longer: 51% took between two hours and a full working day to detect the breach, and 56% took two to eight hours after detection to mitigate the threat.
- In short: 64% of ransomware victims take more than two hours to fix an email security breach.

FIGURE 4

Average time taken to respond to and mitigate an email security breach



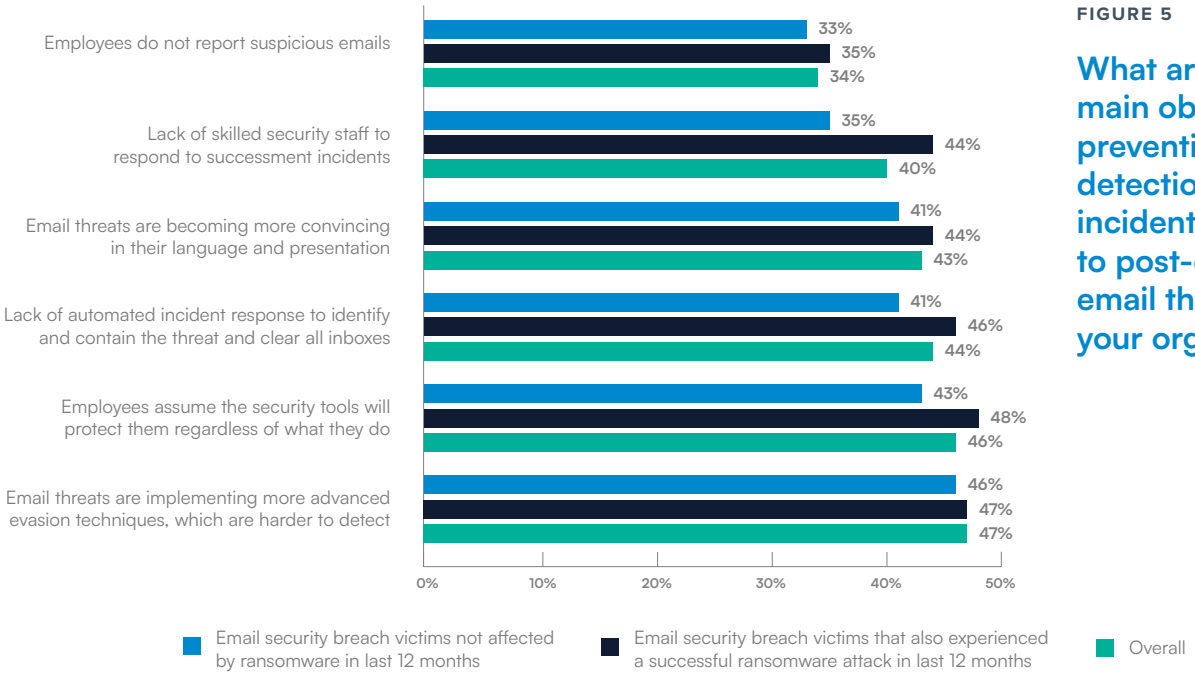
These findings underscore just how important effective email security, response and mitigation capabilities are in broader cyber defense strategies.

Responding to breaches is hampered by attack complexity, human factors and lack of automation

Responding quickly and effectively to an email security breach is not always easy, and the survey highlights obstacles that can get in the way. These can be broadly grouped into three areas: attack complexity, human factors and security tools.

FIGURE 5

What are the main obstacles preventing rapid detection and incident response to post-delivery email threats in your organization?



The most-cited obstacles paint a clear picture of the evolving complexity of email threats and the internal challenges organizations face in responding to them effectively once the attackers have broken through.

Attack sophistication

- The biggest obstacle to rapid incident response, cited by 47% of email security victims overall, is the evolving and increasingly evasive nature of email threats, making them harder to spot and remove from inboxes once they've successfully gained access.
- Compounding the issue is the increasing sophistication of phishing emails themselves. Attackers are crafting messages that are linguistically polished, contextually relevant and visually convincing — often mimicking internal communications or trusted brands. According to 43% of respondents, this makes it harder for both users and security tools to distinguish malicious emails from legitimate ones.

The human factor

- The findings suggest a level of complacency among employees, with 46% of respondents saying colleagues assume that security tools will protect them no matter what.
- Around a third (34%) say that employees do not report suspicious emails. This can also allow threats to persist in inboxes and may be a sign that employees don't know who to report suspicious emails to.
- Both these factors can be addressed through security awareness training, incentives, feedback, easy reporting mechanisms and by fostering a culture of proactive cybersecurity awareness.

Security tools

- The lack of automated incident response capabilities is a significant barrier for 44% of respondents. Without automated tools that can rapidly identify, isolate and remediate threats across user inboxes, security teams are forced into manual processes that are slow and prone to mistakes. This delay gives attackers more time to exploit the breach, escalate privileges or move laterally within the network.

Skills shortage

- A shortage of skilled security personnel is a challenge for 40% of respondents.
- This is the area where the gap between organizations that were also hit with a successful ransomware attack and those that were unaffected is greatest: 44% of organizations that fell victim to both types of attack reported this as a barrier, compared to 35% of those unaffected by ransomware. If organizations lack the expertise or capacity to respond effectively to a detected breach, this can lead to delayed containment or incomplete remediation, enabling attackers to remain in the network and further their attacks.

Conclusion

The broad range of email threats targeting organizations, the tangible impacts, significant costs and growing complexity of the cyberthreat landscape highlight the importance of making email security an integral part of platform-based cyber defense strategies.

A holistic approach to email security should combine advanced, AI-powered detection technologies with user education, automated response and a strong security culture.

The following recommendations may help:

Supporting employees

1. **Regularly train employees** to recognize phishing, social engineering and suspicious email behavior.
2. **Make it easy for employees to report suspicious emails**, and ensure reports are routed to the right team for investigation and rapid triage.
3. **Limit access to sensitive systems and data**, based on job roles. This minimizes the impact of credential theft and lateral movement following an email compromise.

Security tools

4. **Implement multifactor authentication (MFA)** for email and other critical systems. Even if credentials are stolen via phishing, MFA adds a strong layer of defense against unauthorized access.
5. **Deploy email security solutions that use AI/ML** to detect phishing, malware and impersonation attempts. These tools should be able to analyze sender behavior, message content and attachments in real time.
6. **Implement industry-standard email authentication protocols** such as SPF, DKIM and DMARC to verify sender identity and prevent spoofing. These protocols help ensure that only authorized senders can use your domain.
7. **Automate incident response** using tools that can automatically identify and quarantine malicious emails post-delivery, remove them from inboxes and initiate containment workflows. This reduces attacker dwell time and limits exposure.

Longer-term measures

8. **Leverage threat intelligence feeds** to stay updated on emerging email threats, malicious domains and attacker tactics. Integrate this data into your broader detection systems and security platform.
9. **Conduct periodic audits** of email security configurations and simulate attack scenarios (e.g., phishing, BEC) to test your detection and response capabilities.
10. **Understand and address regulatory demands** by ensuring you have the email security measures in place for robust detection, response and data protection. This will also help with cyber insurance requirements.

In today's dynamic and interconnected threat landscape, email security isn't just about stopping spam or phishing — it's about preventing the first domino from falling in a chain that could end in operational paralysis, data loss, reputational damage and longer-term business impacts.

About Barracuda

Barracuda is a leading global cybersecurity company providing complete protection against complex threats for all size business. Our AI-powered BarracudaONE platform secures email, data, applications, and networks with innovative solutions, managed XDR and a centralized dashboard to maximize protection and strengthen cyber resilience. Trusted by hundreds of thousands of IT professionals and managed service providers worldwide, Barracuda delivers powerful defenses that are easy to buy, deploy and use.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research in 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.