Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **May 2024**
Commissioned by **OPSWAT**

2024 Report: Email Security Threats Against Critical Infrastructure Organizations

Executive summary

Organizations in critical infrastructure sectors operate under heightened warnings of cyberattack due to their control of physical infrastructure that wreaks havoc on economic, financial, and health systems when compromised. While warning levels are increasingly high, efficacy at protecting the most common attack vector—email—is low. Most organizations have been breached in the past 12 months (multiple times), half lack confidence in their current protections, and most know their approach is not best in class. With the level of threat posed by email attacks expected to increase over the next 12 months, critical infrastructure organizations intent on strengthening their email security posture must take a dramatic approach that emphasizes prevention and preclusion of email-borne threats. The data in this survey is drawn from a global audience of organizations in critical infrastructure sectors.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Up to 80% of organizations in critical infrastructure sectors have been the victim of an email security breach in the past 12 months**
  Per 1,000 employees, the organizations in this research experienced 5.7 successful phishing incidents per year, 5.6 account compromises, and 4.4 incidents of data leakage, among other types of email security breaches. Organizations in critical infrastructure sectors are highly attractive to cyberthreat actors and are under constant attack.
- **Email is the primary cybersecurity attack vector in critical infrastructure sectors**
  A median of 75% of cybersecurity threats against organizations in critical infrastructure sectors arrive via email. For two out of three organizations, the share of cybersecurity threats arriving by email ranges from 61% to 100%.
- **Success metrics for email security are low**
  48% of the critical infrastructure organizations in this research are not confident that their current email security protections are sufficient against email-borne attacks. Only 34.4% are fully compliant with the email-related regulations that apply to them, e.g., GDPR and other privacy regulations. And 63.6% are not confident that their approach to email security is best in class.
- **Threat levels for all types of cybersecurity attacks are expected to increase, with phishing, data exfiltration, and zero-day malware attacks leading the way**
  Over 80% of organizations expect threat levels of all email attack types to increase or stay the same over the next 12 months.
- **Most organizations do not approach email as malicious by default**
  More than half of the critical infrastructure organizations in this research operate from the assumption that messages and files are benign by default or attempt to operate from the flawed assumption that they are both benign by default and malicious by default. Many more firms need to embrace zero trust approaches for email security.
- **Organizations aspire to be dramatically better—and rapidly, too**
  While current email security efficacy metrics are low, aspirations run high for a dramatic and rapid shift. Achieving this requires a substantial uplift in capability.

Critical infrastructure organizations intent on strengthening their email security posture must take a dramatic approach that emphasizes prevention and preclusion of email-borne threats.

ABOUT THIS WHITE PAPER

The survey and white paper were commissioned by OPSWAT. Information about OPSWAT and details on the survey methodology are provided on page 20.

Importance of email security for critical infrastructure organizations

In this section, we look at the importance of email security to organizations in critical infrastructure sectors.

EMAIL SECURITY IS MORE IMPORTANT FOR ORGANIZATIONS IN CRITICAL INFRASTRUCTURE SECTORS

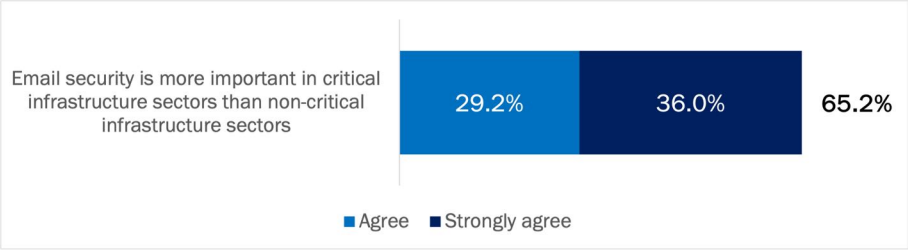
Organizations in critical infrastructures are bound together by a set of common attributes. These attributes make cybersecurity in general, and email security in particular, of high importance.

- **IT and OT systems manage physical infrastructure, not just data**
  Organizations in critical infrastructure sectors manage physical infrastructure and the network of devices and controllers that enable these to operate. Energy networks, nuclear power plants, food supply chains, transportation systems, and water management are all examples. Successful attacks affect actions in the physical world, not merely data, and attacks that begin on the IT network are often in pursuit of more disruptive effects on the OT network.
- **Attractive targets for nation-state actors to undermine national security consciousness and wreak havoc**
  When organizations in critical infrastructure sectors are successfully attacked, normal life is disrupted for all affected. This makes such attacks highly attractive to nation-state actors that want to disrupt the sense of security and normalcy in a target country, putting both governments and citizens on notice.
- **Negative health and wellbeing effects for citizens**
  When cyberattacks disrupt normal operations in healthcare organizations, water and wastewater treatment plants, and large food and agricultural providers and supply chains, citizens face immediate negative effects to health and wellbeing. In the healthcare sector, this could go as far as patient deaths due to systems being inaccessible after a ransomware incident. Attacks on water treatment facilities, too, threaten health levels for thousands.

Attacking critical infrastructure organizations is a key focus for nation-state actors since it disrupts the sense of security and normalcy for citizens.

For the organizations in this research, 65.2% were in high agreement that email security is more important to organizations in critical infrastructure sectors than those in non-critical infrastructure sectors. See Figure 1.

Figure 1
Email security is more important for organizations in critical infrastructure sectors than organizations in non-critical infrastructure sectors
Percentage of respondents



Source: Osterman Research (2024)

LOW CONFIDENCE IN CURRENT EMAIL SECURITY PROTECTIONS

For the organizations in critical infrastructure sectors in this research, 48% are not confident in the email security protections they have currently deployed to stop email security threats. This is shockingly high for a sector where successful security attacks rapidly amplify harm to physical infrastructure and distress to the people who rely on the same. See Figure 2.

Figure 2
Lack of confidence that current email security stack protects critical infrastructure organizations against email-borne attacks
Percentage of respondents indicating low confidence

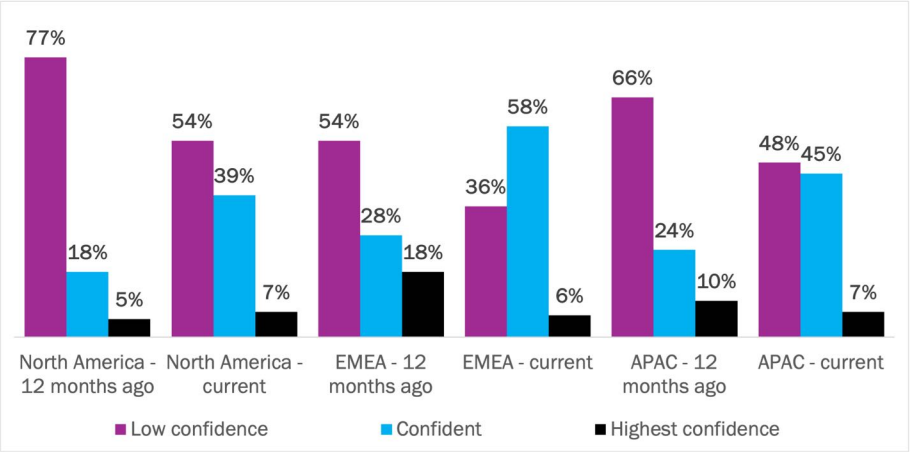
Source: Osterman Research (2024)

The percentage of organizations that have low confidence in their current email security protections has dropped over the past 12 months, from a high of 68% to 48% currently. While this as a trend is directionally correct, too many organizations in critical infrastructure sectors remain susceptible to damaging cyberattacks by email.

When we look at the pattern of confidence across regions, two realities stand out. First, across all regions, the number of those indicating low confidence in the efficacy of email security protections declines from 12 months ago to currently (in alignment with the general trend). Second, there is a general pull-back from assigning the highest level of confidence across the two timeframes. See Figure 3.

48% of organizations in critical infrastructure sectors are not confident that their current email security stack is effective against email-borne attacks.

Figure 3
Confidence in current email security stack to protect critical infrastructure sector organizations against email-borne attacks: Regional variations
Percentage of respondents

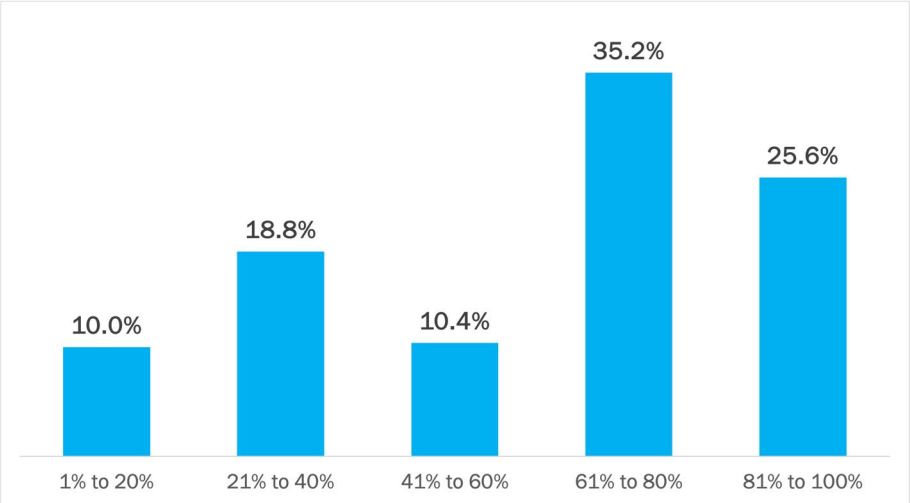


Source: Osterman Research (2024)

LOW CONFIDENCE IN PROTECTIONS IS A PROBLEM BECAUSE EMAIL SECURITY THREATS ARE THE PRIMARY ATTACK VECTOR FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS

Email is the primary attack vector used by cyberthreat and nation-state actors when targeting organizations in critical infrastructure sectors. For the critical infrastructure organizations in this research, a median of 75% of total cybersecurity threats arrive via email (the average is 63%). See Figure 4, where 60.8% of the organizations in this research indicated that the share of cybersecurity threats posed by email ranged from 61% to 100%.

Figure 4
Email threats as a percentage of all cybersecurity threats against organizations in critical infrastructure sectors
Percentage of respondents



Source: Osterman Research (2024)

For organizations in critical infrastructure sectors, email is a critical communications channel that must be secured against cybersecurity threats, particularly since IT networks and OT (operational technology) networks are increasingly linked. Significantly fewer OT networks are still airgapped, and the digital transformation activities of the past decade has resulted in OT networks being connected to the Internet. What this means is that a successful cyberattack by email can spread to the organization's OT network to cause damage and initiate new attacks from inside the OT network.

Successful cyberattacks by email can spread to the organization's OT network to cause damage and initiate new attacks from inside the OT network.

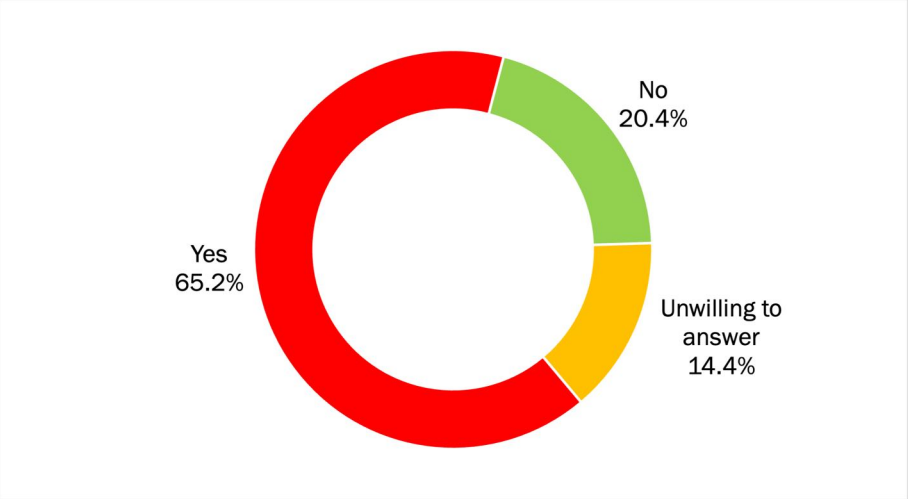
MOST CRITICAL INFRASTRUCTURE SECTOR ORGANIZATIONS ARE SUFFERING FROM EMAIL-RELATED SECURITY BREACHES

Two out of three organizations in this research have been the victim of an email-related security breach in the previous 12 months, such as a phishing message that resulted in account compromise, an email that linked to a ransomware threat that encrypted an endpoint, or a zero-day malware infection.

An additional 14.4% of respondents were unwilling to indicate whether they had been the victim of an email-related security breach. At Osterman Research, we normally interpret this answer as an unofficial "yes," rather than an unofficial "no." If this is the case, 79.6% of the organizations in this research have been compromised by an email-related security breach in the previous 12 months.

See Figure 5.

Figure 5
Email-related security breaches in previous 12 months
Percentage of respondents



Source: Osterman Research (2024)

Between 65% and 80% of organizations in critical infrastructure sectors have been the victim of an email-related security breach in the previous 12 months.

MANY CRITICAL INFRASTRUCTURE ORGANIZATIONS ARE NOT COMPLIANT WITH COMPLIANCE REGULATIONS

Only 34.4% of the organizations in this research believe they are fully compliant with the compliance regulations that apply to them. The most common regulations that the organizations in this research were subject to are:

- GDPR (applicable to 59.2% of organizations in this research)
- Industry-specific privacy regulations (58.8%)
- Country-specific privacy regulations (54.0%). The report drew on a global audience of critical infrastructure organizations, and hence these regulations varied depending on where respondents were located.
- Email marketing regulations (46.0%)

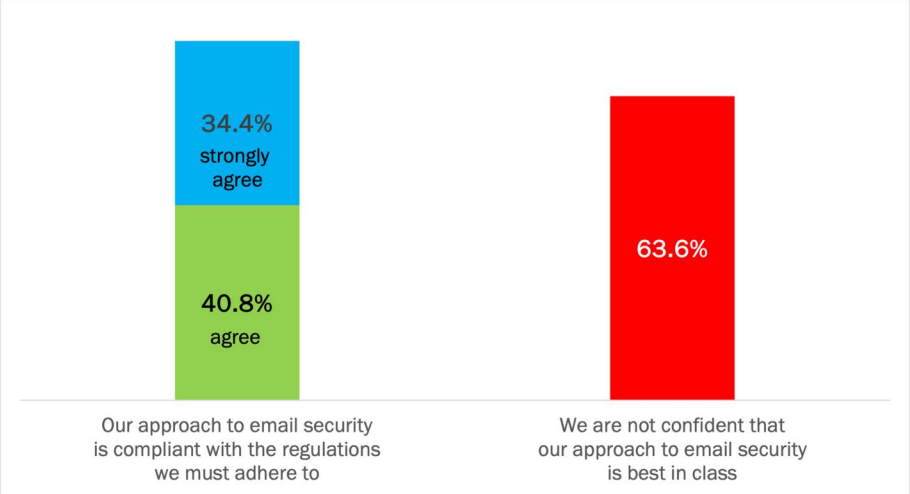
These are not optional regulations that organizations can embrace if they choose. They represent significant areas of business and operational risk if an organization is not compliant and carry detrimental financial consequences for non-compliance.

In addition, 63.6% acknowledge that their approach to email security is not best in class. This means that the majority are readily aware that more needs to be done to achieve best-in-class status.

See Figure 6.

By their own admission, 63.6% of organizations in critical infrastructure sectors rely on email security that is not best in class.

Figure 6
Level of agreement with statements about email security
Percentage of respondents



Source: Osterman Research (2024)

For the organizations in this research, there is clear alignment between the current state of email defenses and the consequences:

- 63% of total cybersecurity threats arrive via email.
- 63.6% of organizations are not confident that their approach to email security is best in class.
- 65.2% acknowledge one or more email security breaches over the past 12 months.

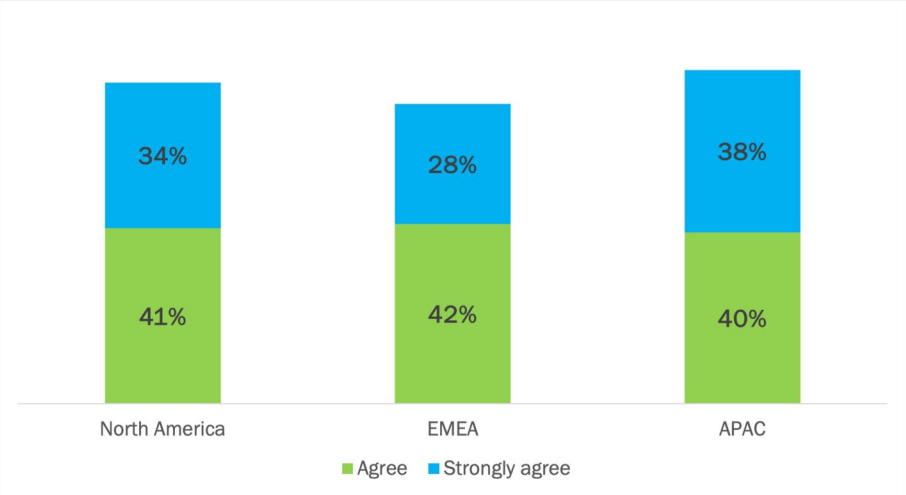
REGULATORY COMPLIANCE: THE REGIONAL PERSPECTIVE

The pattern of regulatory compliance varies to some degree across the three regions surveyed in this research. The question asked in the survey is whether the approach to email security is compliant with the regulations each organization must adhere to. Of the three regions, respondents in APAC most strongly agree that their approach is compliant, followed by those in North America and the EMEA cohort.

While those stack rankings are a true reflection of the data, the data is also a major red flag. For organizations in EMEA—where GDPR casts a significant shadow on business practices for data protection and security—only 28% of the critical infrastructure organizations in this research indicate they are fully compliant. It is slightly higher in the United States, which lacks a cohesive country-wide regulation akin to GDPR, but rather has a burgeoning set of broadly similar state-level regulations that organizations must contend with.

See Figure 7.

Figure 7
Compliance of email security to regulations: The regional perspective
Percentage of respondents



Source: Osterman Research (2024)

Only 28% of the critical infrastructure organizations in EMEA indicate they are fully compliant with their regulatory obligations.

With most organizations facing increasing regulatory pressure—especially those in critical infrastructure sectors—a dramatic change in security posture, in alignment with current and anticipated regulatory obligations, is critical.

Quantifying the dynamics of email security

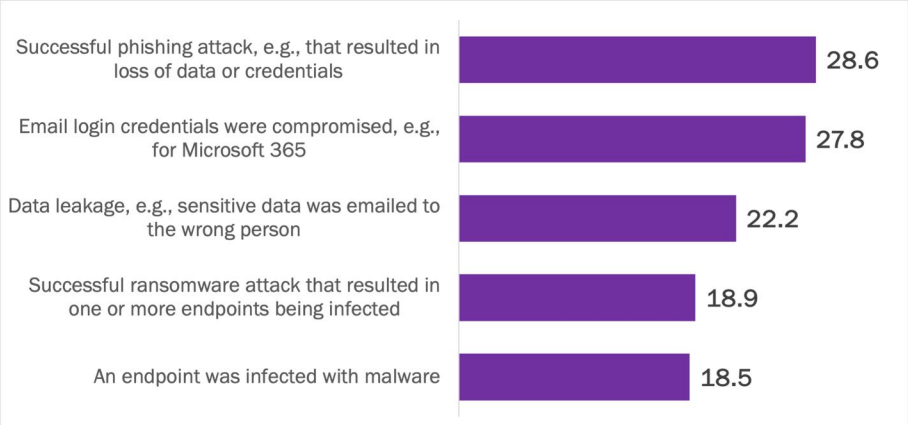
We look at the number and growing severity of email security breaches in this section.

ORGANIZATIONS IN CRITICAL INFRASTRUCTURE SECTORS EXPERIENCE REGULAR EMAIL SECURITY BREACHES

For the critical infrastructure organizations in this research, email security breaches are a common occurrence. Over the previous 12 months, organizations have suffered multiple incidents across multiple security breach types. These are attacks that resulted in a security incident, where existing email security protections were bypassed and the employee also engaged with the malicious email.

Phishing attacks that resulted in the loss of data or account credentials were the most common, at a rate of 5.7 incidents per 1,000 employees. Compromise of Microsoft 365 account credentials was close behind, at a rate of 5.6 incidents per 1,000 employees. Data leakage—where an employee misdirects sensitive data to the wrong person—occurred at a rate of 4.4 incidents per 1,000 employees. See Figure 8.

Figure 8
Email-related security breaches in the previous 12 months
Number of breaches per 1,000 employees



Source: Osterman Research (2024)

Email security breaches are a common occurrence for organizations in critical infrastructure sectors.

This is the rate per 1,000 employees, so as the number of employees changes, so does the number of email-related security breaches. See Figure 9.

Figure 9
Email-related security breaches in the previous 12 months
Number of breaches

Type of email-related security breach	500 employees	2,500 employees	5,000 employees
Successful phishing attack	2.9	14.3	28.6
Email login credentials compromised	2.8	13.9	27.8
Data leakage	2.2	11.1	22.2
Ransomware infection	1.9	9.5	18.9
Malware infection	1.8	9.2	18.5

Source: Osterman Research (2024)

THREAT LEVELS ARE EXPECTED TO INCREASE

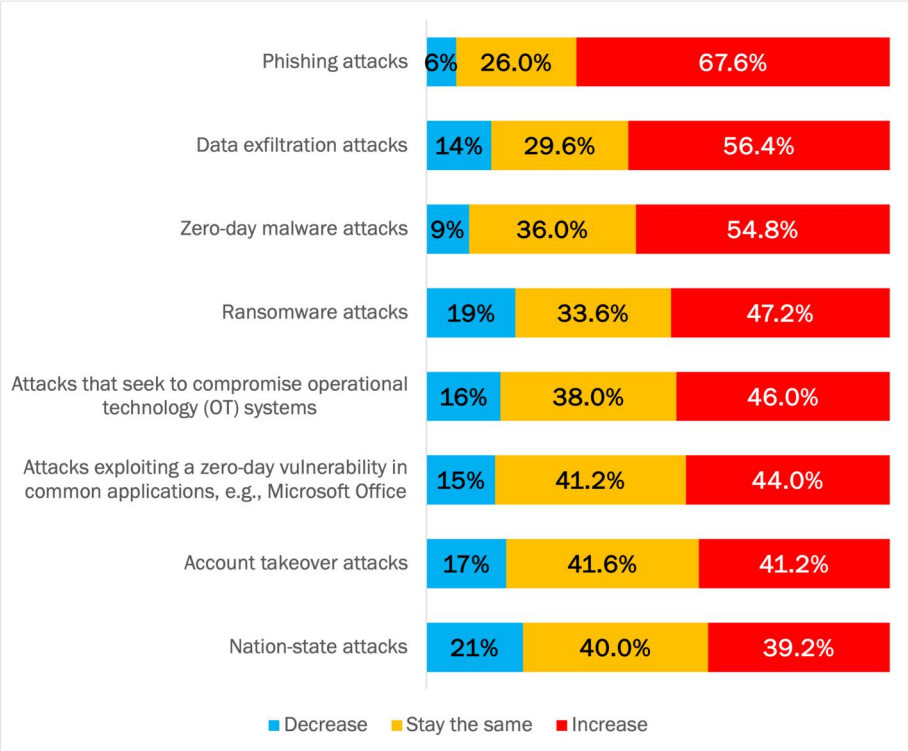
Cyberthreat and nation-state actors continually invest in new approaches to compromising targets in the critical infrastructure sector. Over the past 12 months, QR code phishing attacks became more commonplace, ransomware gangs continued to focus on data exfiltration as a more guaranteed path to profitable extortion than unwanted encryption, and threat actors have made increased use of malicious AI services to craft more believable phishing emails. Some critical infrastructure sectors have seen increased activity by nation-state actors, leading to warnings from government agencies to be better prepared, e.g., water and wastewater treatment plants.[1]

The organizations in this research do not expect cyberthreat and nation-state actors to suddenly cease and desist over the next 12 months. On average, half expect the threat level posed by all types of email attacks to increase over the coming 12 months, while 35% expect threat levels to remain unchanged. Apart from account takeover attacks and nation-state attacks, the largest proportion of respondents believe that the threat level will increase for all types of email attacks.

See Figure 10.

On average, 50% of organizations believe the threat posed across multiple email threat vectors will increase over the next 12 months.

Figure 10
Anticipated change in the threat of email attacks over the next 12 months
Percentage of respondents



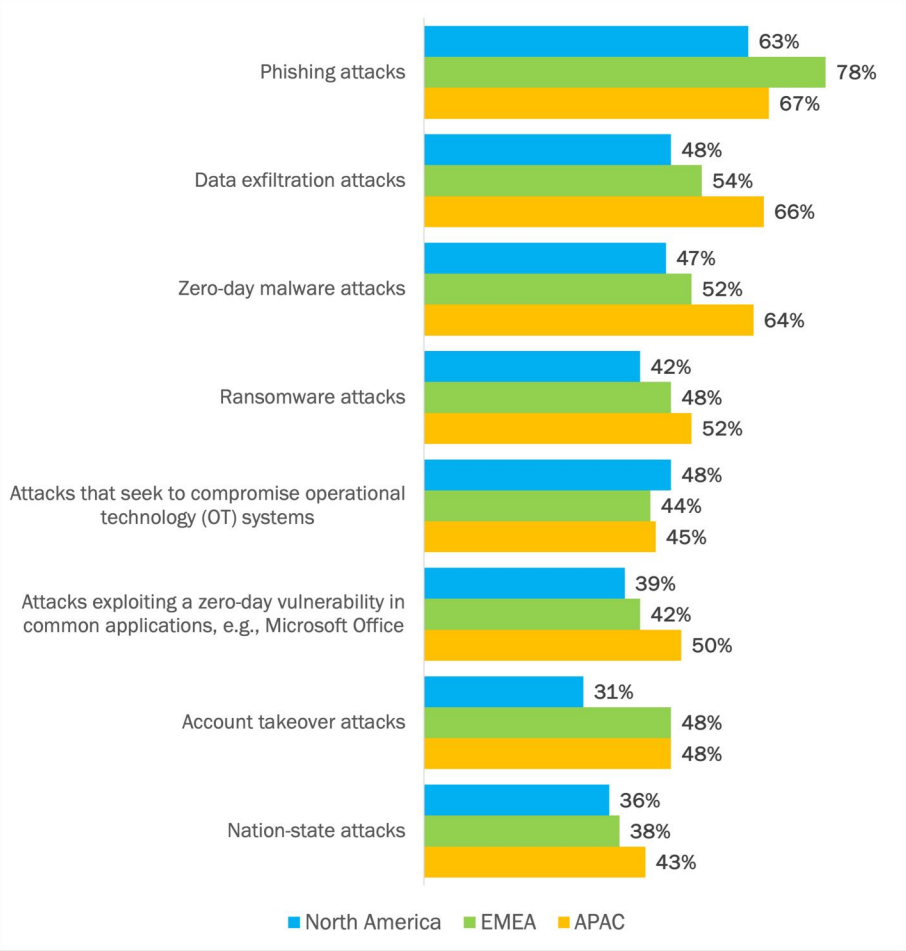
Source: Osterman Research (2024)

THREAT LEVELS EXPECTED TO INCREASE: REGIONAL COMPARISON

We looked at how respondents from the three geographical regions covered by this survey assessed the likelihood that the threat level of email attacks would increase over the next 12 months. For all three regions, phishing claimed top place for the expected increase in threat level, although in the APAC region, this only just edged out the threat of data exfiltration attacks. On a regional basis (see Figure 11):

- **North American firms were the least likely to anticipate increasing threat levels**
  Apart from attacks that seek to compromise OT systems, where the North American respondents ranked highest, for every other type of email attack, the expected level of increase was lower than respondents in the other two regions.
- **EMEA firms most concerned about phishing attacks**
  Firms in EMEA were much more likely to indicate that phishing attacks would increase over the next 12 months versus the others.
- **APAC firms generally exhibited the highest expectation of increasing threat levels**
  For five of the eight email threat types, respondents in APAC exhibited the highest expectation that threat levels would increase. For a sixth, they tied in first place with the EMEA respondents.

Figure 11
Anticipation of increasing threat level of email attacks over the next 12 months: Regional comparison
Percentage of respondents



Source: Osterman Research (2024)

Organizations in APAC are much more likely to expect increasing threat levels from a range of email attacks over the next 12 months.

MANY CRITICAL INFRASTRUCTURE ORGANIZATIONS ARE CONFUSED ON FUNDAMENTAL EMAIL SECURITY PRINCIPLES

We asked respondents to rank the importance of four principles of email security to their organization:

- Email messages are assumed benign until proven otherwise.
- Files coming into our organization are assumed benign until proven otherwise.
- Email messages are assumed malicious until proven otherwise.
- Files coming into our organization are assumed malicious and must be sanitized before being made available to our users.

With the elevation of threats against critical infrastructure organizations and the significant negative impacts that accrue after an email breach, the principle that aligns best with the threat landscape is the assumption of maliciousness by default.

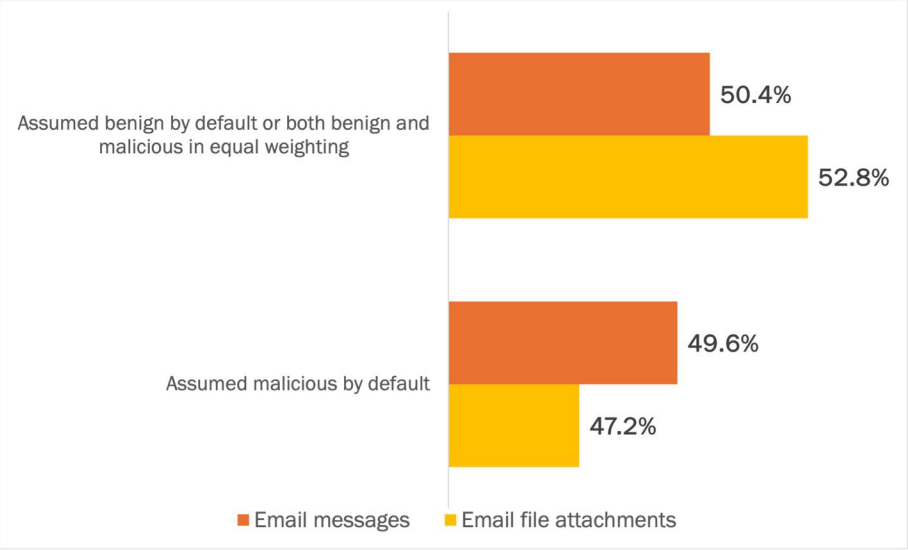
We analyzed the responses and grouped the answers on email messages and email file attachments into two buckets: those where the assumption of maliciousness was higher than the assumption of being benign, and those where the benign assumption was higher or where both ratings were the same.

Among the organizations surveyed for this research, more than half operate from the assumption that messages and files are benign by default or attempt to operate from the assumption that they are both benign by default and malicious by default. The latter approach of equivalent assumptions does not make sense, because the two principles are diametrically opposed and mutually exclusive.

See Figure 12.

More than half of organizations in critical infrastructure sectors approach email messages and email file attachments as benign by default or both benign and malicious by default—a confused and flawed position.

Figure 12
Importance of email security principles
Percentage of respondents



Source: Osterman Research (2024)

If the respective principles of malicious by default and benign by default are fully embraced, they will have a significant impact on the selection decision for email security solutions.

For example:

- **When email messages and files are assumed to be benign**
  Organizations that take a benign-by-default stance will settle for email security solutions that focus on a pre-delivery assessment for obvious malicious signals by looking for a match against known malicious signatures, along with post-delivery detection of malicious activity in email messages or files. The benign-by-default assumption is more likely to result in email-related security breaches.

- **When email messages and files are assumed to be malicious**
  Organizations that take the malicious-by-default stance, by comparison, will invest in an email security solution with deep pre-delivery checks and balances to assess for malicious intent and behavior, the creation of threat-free email messages and file attachments that can be safely delivered to a user's inbox, and continual real-time analysis of behavioral attributes in email messages and attachments as users engage with them. This emphasis requires features such as content disarm and reconstruction (CDR), anomaly detection in email communication patterns, and time-of-click assessment of links in email messages and file attachments to counteract post-delivery weaponization.

It is logically impossible for an organization to hold both assumptions in equal measure. The baseline assumption of building an email security stack must be driven by a belief either that email messages and email file attachments are benign, or that they are malicious. The two are mutually exclusive.

When we crosstabbed the survey data:

- **The malicious-by-default approach was more frequently correlated with high confidence in current email security protections**
  Organizations approaching both email messages and files as malicious by default were more likely to have a high level of confidence in their current email security stack compared to those organizations that did not take the malicious-by-default stance for one or both.
- **The absence of the malicious-by-default approach was overwhelmingly correlated with low confidence in current email security protections**
  Organizations that did not approach either email messages or files as malicious by default were overwhelmingly more likely to have low confidence in the efficacy of the protections afforded by their current email security stack.

The baseline assumption of building an email security stack must be driven by either a belief that email messages and email file attachments are benign—or that they are malicious.

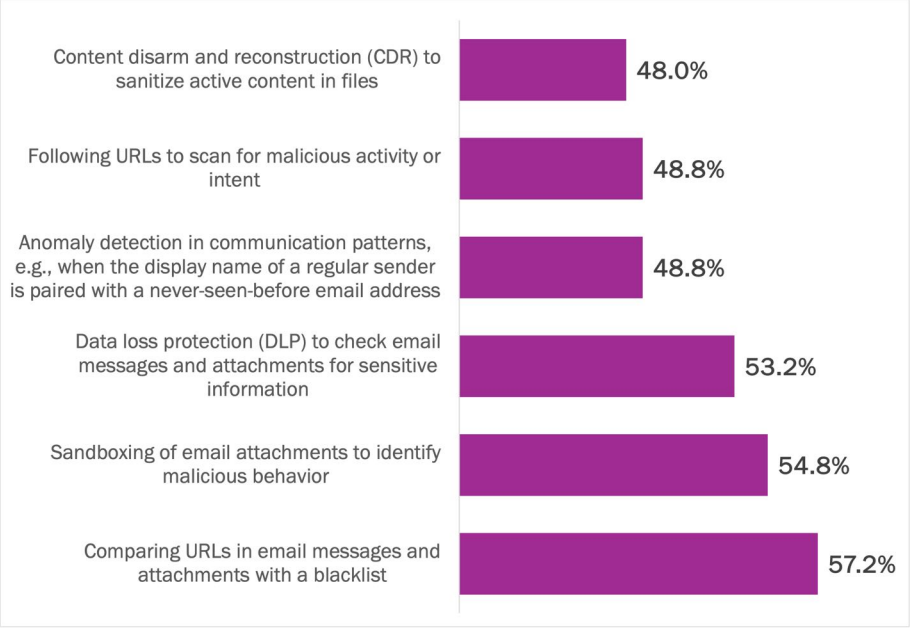
TOO FEW ORGANIZATIONS ARE USING EMAIL SECURITY CAPABILITIES THAT PRECLUDE THREATS BY DESIGN

Many of the organizations in this research are lacking advanced email security capabilities that preclude and prevent email security threats from reaching users' inboxes. See Figure 13. Many of the capabilities that are not being used align with the malicious-by-default principle of email security. For example:

- **Content disarm and reconstruction to sanitize active content in files (48%)** CDR takes the original file as delivered and performs a deep and recursive assessment to break the file into its constituent parts and then reassemble it without any of the potentially malicious components that were included in the original, e.g., macros or code. The reconstructed and sanitized file is delivered to the intended recipient. It should work with full fidelity to the original, sans the threats.
- **Following URLs to scan for malicious activity or intent (48.8%)** A security approach that assesses URLs for malicious signals every time the URL is clicked or opened to counteract post-delivery weaponization. It is a newer and more sophisticated approach than comparing URLs against a blacklist. Any email security solution that performs only an on-delivery check of a URL creates significant risk for the organizations using that solution.
- **Anomaly detection in communication patterns (48.8%)** Analysis of the technical signals available in an email message for anomaly detection, such as when the display name of a regular sender is linked with a brand-new email address. While such a communication may be valid, it is more likely to represent an impersonation attempt. Anomaly detection is driven by artificial intelligence models that automatically create and maintain baseline communication patterns for all employees.

Many of the organizations in this research are not leveraging advanced email security capabilities that preclude and prevent email security threats from reaching users inboxes.

Figure 13
Email security capabilities lacking at critical infrastructure organizations
Percentage of respondents



Source: Osterman Research (2024)

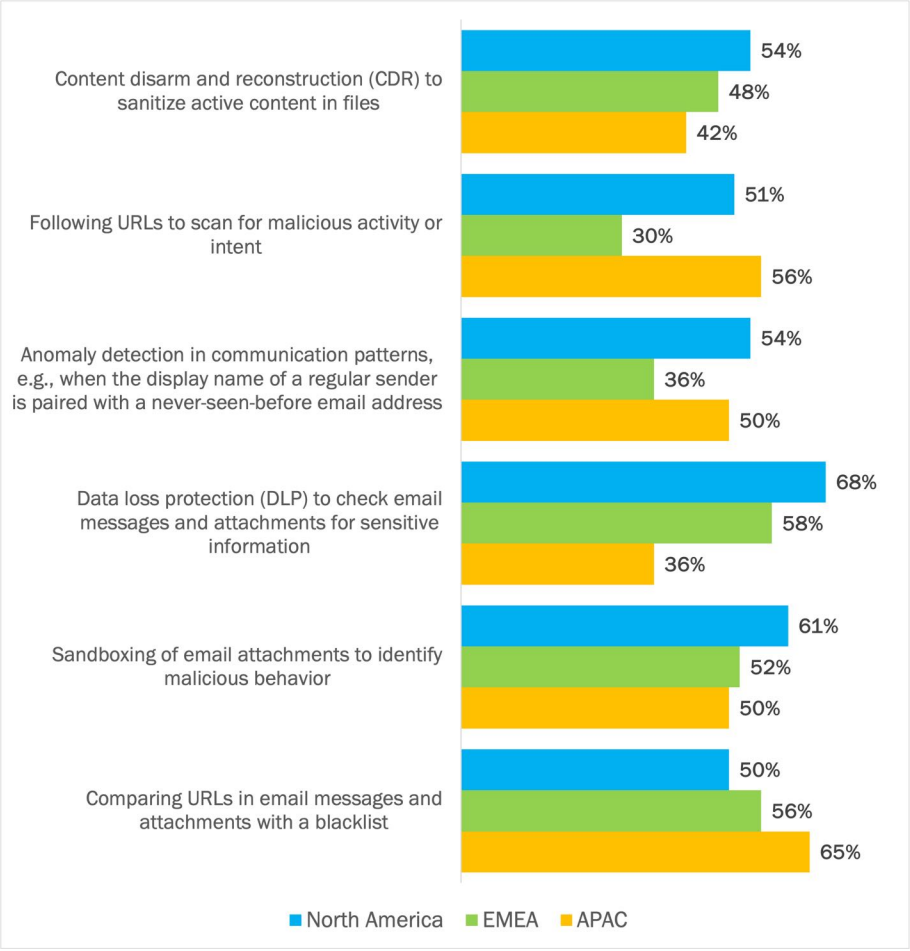
ADOPTION OF EMAIL SECURITY CAPABILITIES THAT PRECLUDE THREATS BY DESIGN: REGIONAL COMPARISON

Across the three regions we surveyed, adoption patterns of email security capabilities that preclude threats by design differ. For example (see Figure 14):

- **North American firms lagging behind others in three areas**
  Respondents from organizations in critical infrastructure sectors in North America were least likely to have three of the six capabilities we asked about—CDR (at 54% of respondents), DLP (68%), and sandboxing of email attachments (61%). They were more likely than the other regions to rely on ineffective email security approaches, such as comparing URLs in email messages to a blacklist.
- **EMEA firms more likely to use two preclusion technologies**
  The EMEA cohort is more likely than the others to follow URLs to scan for malicious activity or intent (only 30% not doing so) and anomaly detection (only 36% not doing so). They are in the middle of the pack for most others.
- **APAC firms have a big opportunity to strengthen URL analysis**
  Many firms in APAC are neither comparing URLs to a blacklist (65% not doing so) or following them to scan for malicious intent (56%). That is a risky approach.

Without advanced technologies to preclude threats by design, organizations in critical infrastructure sectors will continue to suffer costly attacks on the IT side and heightened risk of compromise on the OT side.

Figure 14
Email security capabilities lacking at critical infrastructure organizations: Regional comparisons
Percentage of respondents



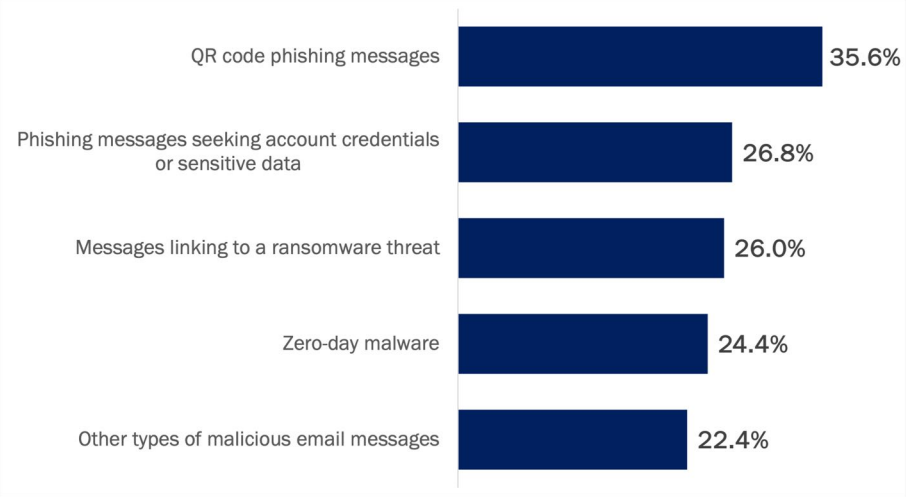
Source: Osterman Research (2024)

TRAINING APPROACHES ARE FAILING TO PREVENT ATTACKS FROM BECOMING INCIDENTS

Cybersecurity awareness training, particularly for email-related security attacks, is commonly advocated as a method for building a last line of defense to stop email attacks from becoming incidents. Under this approach, if an executive or employee doesn't click or open a malicious message because they recognize the malicious signals that the email security stack has missed, a security breach or incident has been avoided. At Osterman Research, we have regularly advocated that organizations must carry out effective cybersecurity awareness training for this very purpose.

While we advocate for the necessity of cybersecurity awareness training, we have never viewed it as a panacea nor as being independent of the email security technology being used. For many of the organizations in this research, undetected email threats became costly incidents when employees clicked a link, scanned a QR code, downloaded a ransomware threat that encrypted their endpoint, or lost their account credentials after falling for a phishing threat. This was true for just over one quarter of organizations across a range of email attacks. See Figure 15.

Figure 15
Cybersecurity training doesn't prevent email attacks from becoming incidents
Percentage of respondents indicating training has low effectiveness



Source: Osterman Research (2024)

Cybersecurity awareness training is not a panacea nor independent of the email security technology being used.

What this means in light of the data from this research is twofold. First, organizations in critical infrastructure sectors need better email security technologies than they are currently using. These need to preclude and prevent email threats from being delivered to inboxes so that employees cannot activate them. Second, organizations experiencing a high number of incidents because employees are falling for email attacks must revisit the type of cybersecurity awareness training on offer, along with the frequency of that training to increase the effectiveness of training interventions.

What organizations in critical infrastructure sectors want for their email security

This section looks at what organizations in critical infrastructure sectors need.

CRITICAL INFRASTRUCTURE ORGANIZATIONS KNOW THEY NEED BETTER EMAIL SECURITY TECHNOLOGIES

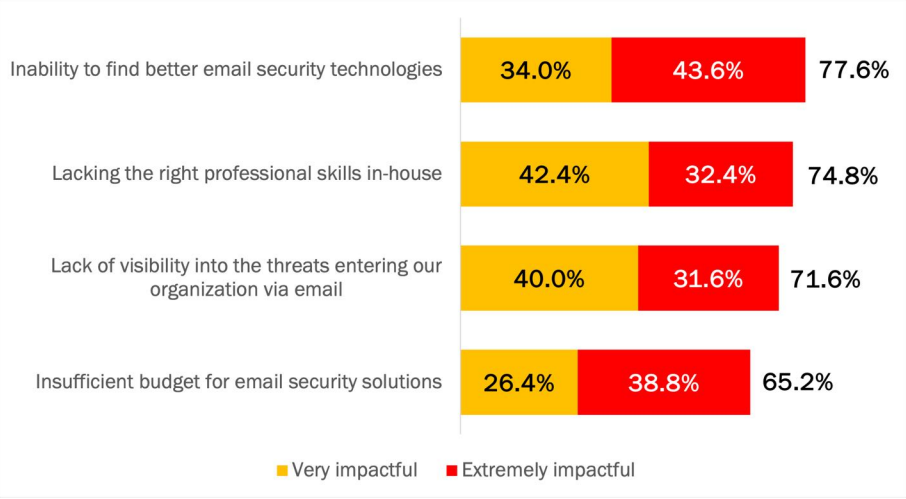
Organizations in critical infrastructure sectors know that they need to find better email security technologies to increase the efficacy of email security. This is the top-rated issue that hinders organizations in delivering the requisite level of email security (at 77.6% of organizations) and is the issue with the highest rating of "extremely impactful" (at 43.6%). See Figure 16. It would be beneficial if the email security vendor had deep experience and expertise in the critical infrastructure sector, as well as offering email security technologies that include the features previously discussed that enable email threats to be precluded, not merely detected.

Three additional issues are seen as getting in the way of better email security:

- **Lack of the right professional skills in-house (74.8%)**
  Cybersecurity professionals with the right skills are needed to manage and operate an email security platform. This can be buttressed to some degree by working with a managed services partner. In addition, better tools that decrease the number of email security threats getting through to the inbox reduce the need for incident response skills.
- **Lack of visibility into email-borne threats (71.6%)**
  If you are unable to see the threats that exist, there will be low desire to do something different. Visibility leads to insight which ignites the drive to change.
- **Insufficient budget for email security solutions (65.2%)**
  Although organizations are covering the costs of frequent email security incidents, they appear less willing to invest in better email security solutions to preclude incidents from happening.

Organizations in critical infrastructure sectors are desperately looking for better email security technologies to increase the efficacy of email security.

Figure 16
Issues that get in the way of delivering the required level of email security
Percentage of respondents indicating "very impactful" or "extremely impactful"



Source: Osterman Research (2024)

ORGANIZATIONS EXPECT A RAPID AND SIGNIFICANT IMPROVEMENT IN PROTECTIONS AGAINST EMAIL-RELATED SECURITY ATTACKS

The organizations in this research hold aspirational goals of significantly improving their email security posture over the next 12 months. Given the current areas of low performance in email security among organizations in critical infrastructure sectors across the world, it is gratifying to see this intent.

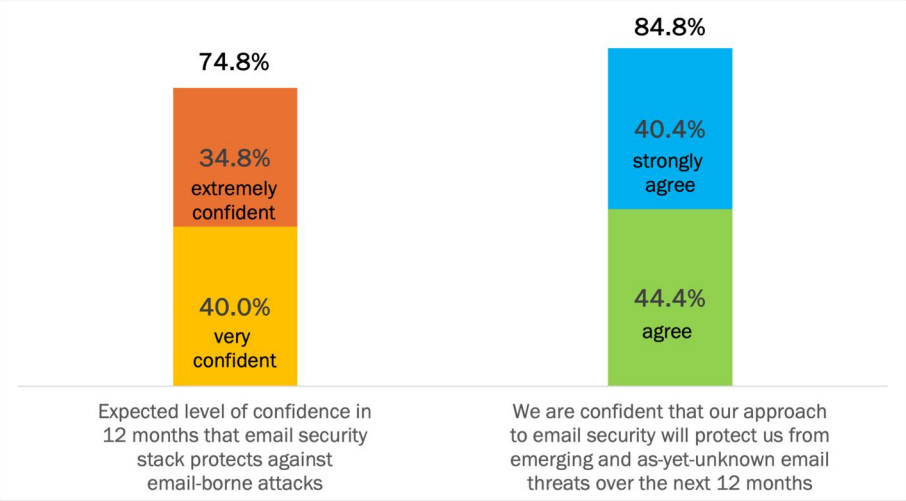
Two finding from this research highlight this intent:

- **A desire for five times higher confidence in email security protections**
  While only 52.0% of organizations are confident in their current email security protections (see discussion on page 4), it is the aspiration of 74.8% to reach this level within 12 months. In addition, organizations want the composition of confidence to change, too, with five times more wanting to be at the highest level of confidence compared to the current level (from 6.8% at the "extremely confident" level to 34.8%). With this highest level of confidence dropping over the previous 12 months, only those organizations taking a very different approach to email security protections have any chance of achieving this higher level—an approach that leverages zero trust technologies for email security such as leveraging multiple scanning engines, CDR, and other real-time methods of detecting phishing attacks and weaponized documents.
- **An aspiration to strengthen protections against emerging and as-yet-unknown email threats and unknown malware**
  In a similar vein, 84.8% of the organizations in this research aspire to be at a place where their approach to email security protects them from emerging and as-yet-unknown email threats over the next 12 months. With many organizations being the victim of multiple email-borne attacks over the previous 12 months, this requires a significant upleveling of email security capabilities and efficacy over the next 12 months.

See Figure 17.

Many more organizations want to achieve the highest level of confidence in their email security posture within the next 12 months.

Figure 17
Aspirations for email security protections in 12 months
Percentage of respondents



Source: Osterman Research (2024)

Conclusion

Organizations in critical infrastructure sectors are under frequent attack from cybercriminals and nation-state actors. Email is the primary vector of attack, and from multiple viewpoints, organizations know they need to be doing much better than they are at preventing these attacks from succeeding. The need to do much better is an acknowledgement that no one disagrees with. The question is whether critical infrastructure organizations will take the necessary actions to achieve such a dramatic and rapid uplift in posture—one that precludes threats by design, not by the hope of detection. This is particularly important due to the interlinkages between IT and OT networks, with threats that originate on the IT side (e.g., via email) pivoting to compromise the OT network.

About OPSWAT

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises the critical advantage needed to protect their complex networks and ensure compliance. Empowered by a "Trust no file. Trust no device™." philosophy, OPSWAT solves customers' challenges around the world with zero-trust solutions and patented technologies across every level of their infrastructure, securing their networks, data and devices, and preventing known and unknown threats, zero-day attacks and malware.

Discover how OPSWAT protects the world's critical infrastructure and helps secure our way of life; visit www.opswat.com.

OPSWAT.

www.opswat.com

@OPSWAT

+1 415 590 7300

Methodology

The survey research for this white paper was conducted by Osterman Research.

Two hundred and fifty (250) respondents in IT and security leadership roles were surveyed in March 2024. To qualify, respondents had to work at an organization in a critical infrastructure sector with at least 100 employees. The surveys were conducted in nine countries and across 16 critical infrastructure sectors. All respondents were directly involved in how their organization was dealing with email security strategies and approaches.

ORGANIZATION SIZE

100 to 499 employees	18.8%
500 to 999 employees	28.4%
1000 to 2,499 employees	31.6%
2,500 or more employees	21.2%

JOB ROLE

IT manager, director, or VP	30.8%
Director or VP of security or information security	28.0%
CISO	21.2%
CIO	20.0%

GEOGRAPHY

United States	34.0%
India	12.0%
Japan	12.0%
United Kingdom	10.8%
Australia	8.0%
Singapore	8.0%
Canada	6.0%
Nordics	5.2%
Netherlands	4.0%

CRITICAL INFRASTRUCTURE SECTOR

Chemicals	5.2%
Commercial facilities	6.4%
Communications	8.0%
Critical manufacturing	6.8%
Dams	5.2%
Defense industrial base	4.8%
Emergency services	6.8%
Energy, e.g., electricity, oil, natural gas	6.4%
Financial services	7.2%
Food and agriculture	7.2%
Government facilities	5.2%
Healthcare and public health	6.4%
Information technology	8.0%
Nuclear reactors, materials, and waste	2.8%
Transportation systems	8.0%
Water and wastewater	5.6%

[1] CISA, CISA, EPA, and FBI Release Top Cyber Actions for Securing Water Systems, February 2024, at https://www.cisa.gov/news-events/alerts/2024/02/21/cisa-epa-and-fbi-release-top-cyber-actions-securing-water-systems