Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **April 2021**
Sponsored by **Mimecast**

Assessing Organizational Readiness to Deal With Increased Employee Cyber Awareness

Executive Summary

This research looks at the flow-on effects of cybersecurity awareness training and other mechanisms of engaging and empowering users to recognize cyberthreats. Specifically, it addresses how organizations assess whether email messages reported by employees as suspicious are malicious or benign, and if the former, how security teams investigate them. Many organizations rely on human analysts in an IT or security role for this task, along with manual or partially automated processes. Not many organizations appear to employ dedicated email analysts with the expertise and specific tooling to undertake this work.

Removing as many threats from email as possible is essential to a heightened email security posture. However, few organizations have an end-to-end automated toolkit and approach in which they have high confidence to assess and remediate malicious messages across the organization. Those organizations that do are able to determine whether a message is malicious much faster than others, and employees respond in turn to the faster feedback loop by reporting a greater number of messages on average than organizations without the processes or disciplines in place.

Few organizations have an end-to-end automated toolkit and approach in which they have high confidence to assess and remediate malicious messages.

KEY TAKEAWAYS

These are the key takeaways presented in this paper:

- **Dealing with Emails Reported as Suspicious by Employees is a Distraction**
  Over half of the respondents in this research felt strongly that IT and security staff dealing with emails reported as suspicious by employees is a task that diverts them from more important tasks.
- **Infrequent Training Results in Lower Engagement by Employees**
  Almost half of organizations provide cybersecurity awareness training quarterly or less frequently. Organizations that train less frequently gain lower engagement with employees, who report fewer suspicious emails.
- **Few Dedicated Email Analysts with Professional Training and Tooling**
  Many organizations rely on staff in the IT department to address potential cybersecurity threats in email. Few organizations employ dedicated email security analysts with the professional training and tooling to tackle the job quickly and effectively.
- **Few Organizations Analyze All Reported Emails**
  The majority of organizations do not analyze all of the emails reported as suspicious by employees. However, for those organizations that do, employees are almost three times as engaged in identifying cybersecurity threats by email.

ABOUT THIS WHITE PAPER

We surveyed 300 cybersecurity professionals in the United States and the United Kingdom on the impact of the cybersecurity solutions deployed and used at their organization, including cybersecurity awareness training. All respondents worked at organizations with at least 1,500 employees, and virtually all of the organizations offered cybersecurity awareness training.

This white paper is sponsored by Mimecast. Information about Mimecast is provided at the end of the paper.

Email as a Threat Vector

Email is the dominant channel for internal and external communication and coordination across the world and all organizational types. Given its widespread adoption offering easy access to hundreds of millions of people for minimal cost, email has also become a primary vector for carrying cybersecurity threats into the hearts of organizations.

Email has consistently been a threat vector in recent years, for example:

- **Phishing is a Significant Threat**
  Verizon's 2020 *Data Breach Investigations Report* found that phishing was the top threat channel used by threat actors in 2019, and that 22% of data breaches involved phishing attacks. Verizon noted an increasing use of phishing and credential theft attack types.[1]
- **Business Email Compromise in 2019 at $1.7 Billion**
  The FBI reported a total of almost 33,000 complaints about business email compromise (BEC) scams in 2019, at a total cost of $1.7 billion.[2] BEC scams represented almost half of the value of total Internet crime losses in 2019.
- **Fewer Business Email Compromise Scams in 2020 But Higher Losses**
  The FBI's numbers for 2020 indicate fewer BEC scams in comparison to 2019, but at a higher per scam average and total overall cost. There were 19,300 complaints in 2020, with a total cost of $1.8 billion.[3]
- **More Than Two Million Domains Detected in 2020 Tied to Phishing Attacks**
  In 2020, Google detected 2.1 million domains tied to phishing attacks, up from 1.7 million detected domains the year before.[4] Phishing is implicated as the majority root cause for malicious breaches, and in the age of stringent data protection regulations (GDPR, CCPA, CPRA, etc.), the potential consequences of data breaches are significant.
- **Internal Phishing is a Growing Problem**
  Attackers compromise the account credentials for an email account belonging to a target organization, and then use those credentials to run phishing campaigns inside the organization against "colleagues" and "co-workers." The intent is to gather additional credentials and an increasing set of access privileges to data sources and trusted networks.
- **Phishing Attack, Credential Compromise, Business Email Compromise**
  In August 2020, hackers gained access to an email account at a construction company working for a school district in the United States, most likely the result of a phishing attack. The hackers sent new payment details for an invoice to the school district in a business email compromise attempt, which resulted in a $334,000 payment going to an account under the hacker's control.[5]
- **Cost of BEC Scams Increased in 2020**
  The average amount requested in a BEC scam attempt increased from $48,000 to $75,000 from Q3 to Q4 in 2020.[6] One successful email resulted in a $75,000 payoff to the cybercriminal! Specific instances of BEC scams are often for much higher amounts, e.g., the fake $388,000 invoice paid by the bookkeeper of a high-profile investor for a real estate renovation in early 2020.[7]

Email has become a primary vector for carrying cybersecurity threats into the hearts of organizations.

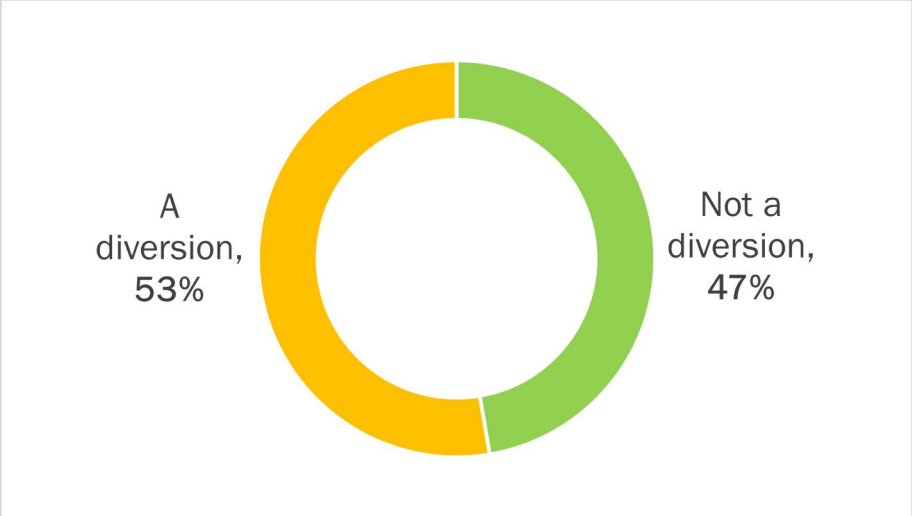
Research Findings

This research investigated the use and effects of employee engagement and empowerment to reinforce cybersecurity awareness training in organizations with more than 1,500 employees across the United States and the United Kingdom. As briefly explored above, email has become a significant threat vector for organizations, and remediating the threats in email is essential.

DEALING WITH EMPLOYEE REPORTED EMAILS VIEWED AS A DIVERSION

Over half of the respondents in this research felt strongly that IT and security staff dealing with emails reported as suspicious by employees is a task that diverts them from more important tasks. See Figure 1.

Figure 1
Dealing with Reported Emails as a Diversion
Percentage of respondents



Source: Osterman Research (2021)

Dealing with emails reported as suspicious by employees is viewed as a diversion from more important tasks by over half of respondents.

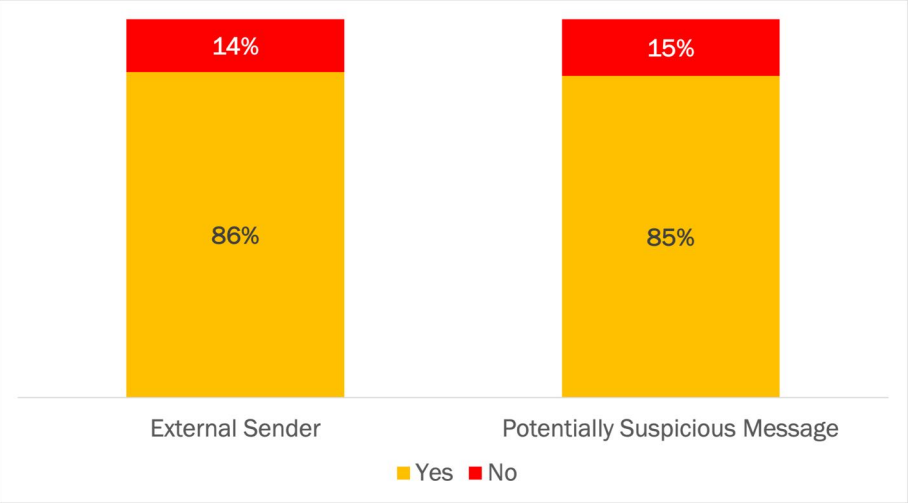
A common finding from the responses to the questions in this survey was the high degree of reliance on human analysts in the task of analyzing reported messages to ascertain maliciousness. Given the availability in the market of automated tools to analyze reported messages without requiring human analysts to do so, it is unsurprising that many felt continued reliance on human analysts was a diversion. For the 53% of respondents who said it was a diversion, we correlated their answer with their use of automation and human analysts and human intervention in the analysis task. We found that:

- 87% of respondents who said it was a diversion relied on human analysts or human intervention.
- 12% of respondents who said it was a diversion relied on fully automated tooling.
- Only 1% of respondents who outsourced the task to a third party viewed the task as a diversion.

MOST ORGANIZATIONS ADD WARNING SIGNALS TO EMAILS

Most organizations are seeking to engage their users in the fight against malicious email messages by automatically adding warning signals to emails in the form of message banners. Messages flagged as coming from outside the organization—from an external sender—bring the obscured technical facts of the message to the foreground, thereby aiding in addressing impersonation threats (e.g., when a threat actor is using impersonation to attempt to trick a targeted user into taking a particular action). Such banners also provide message-by-message coaching alerts to remind users to beware of unsolicited messages from outside the organization. See Figure 2.

Figure 2
Warning Banners Added to Email Messages
Percentage of respondents



Source: Osterman Research (2021)

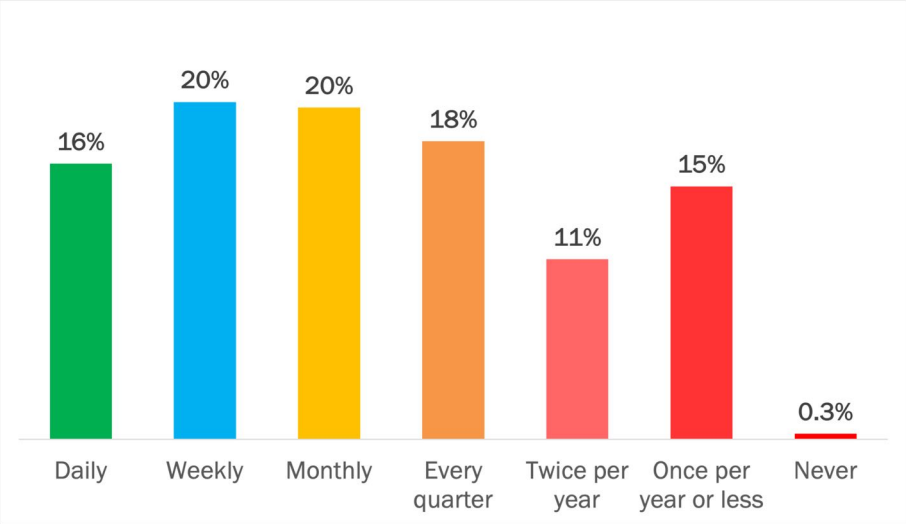
Most organizations also add a banner to messages to warn of potentially suspicious content. These banners are added as a way of dealing with the false positive problem: what to do when a message possesses some but not all of the warning signals used to rule it as malicious. Instead of blocking or quarantining such potentially suspicious messages that can disrupt valid communication events, the message is still delivered but with a warning added to enlist the intended target in the process of making the final determination on the malicious status.

Most organizations seek to engage their users in the fight against malicious email messages by automatically adding warning signals to email messages.

ONE HALF OF ORGANIZATIONS ARE TRAINING FREQUENTLY ON CYBERSECURITY THREATS

In our research, just over one half of organizations provided cybersecurity awareness training at least monthly (56% in total). The remaining 44% provide cybersecurity awareness training quarterly or less frequently, with 15% of the overall population of respondents training only once per year or less. In our view, given the seriousness of cybersecurity threats, cybersecurity awareness training should be offered on at minimum a monthly cadence. See Figure 3.

Figure 3
Frequency of Cybersecurity Awareness Training
Percentage of respondents



Source: Osterman Research (2021)

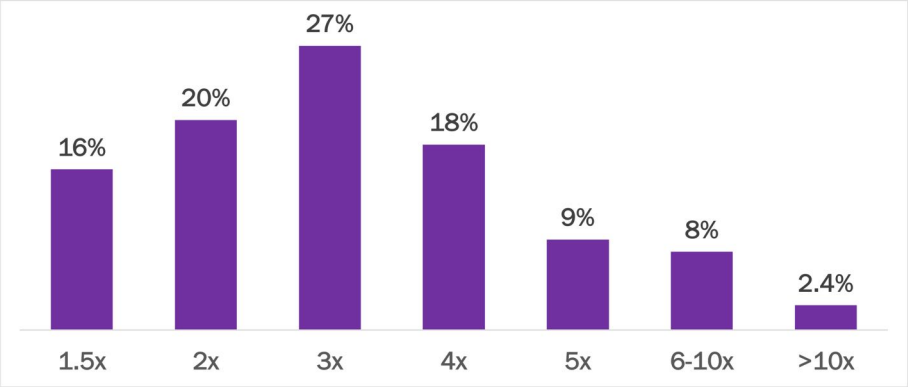
Providing cybersecurity awareness training on a daily basis is worth a mention. In our research, 16% of respondents indicated this cadence. Examples of daily training include a daily email alert on some aspect of cybersecurity, a warning poster in an elevator, or a pull-up display reminding employees not to leave USB sticks on their desk. When cybersecurity awareness training is embraced with the fervor of an internal marketing campaign, daily touchpoints are common.

Almost half of organizations provide cybersecurity awareness training quarterly or less frequently.

SUSPICIOUS MESSAGES REPORTED MORE FREQUENTLY AFTER TRAINING

Cybersecurity awareness training has an impact on the number of emails reported as suspicious by users, with 80% of respondents indicating an increase in the number of reports submitted. For almost two thirds of organizations, the rate of increase was between 1.5 and three times as many messages reported after cybersecurity awareness training began than the baseline number. See Figure 4.

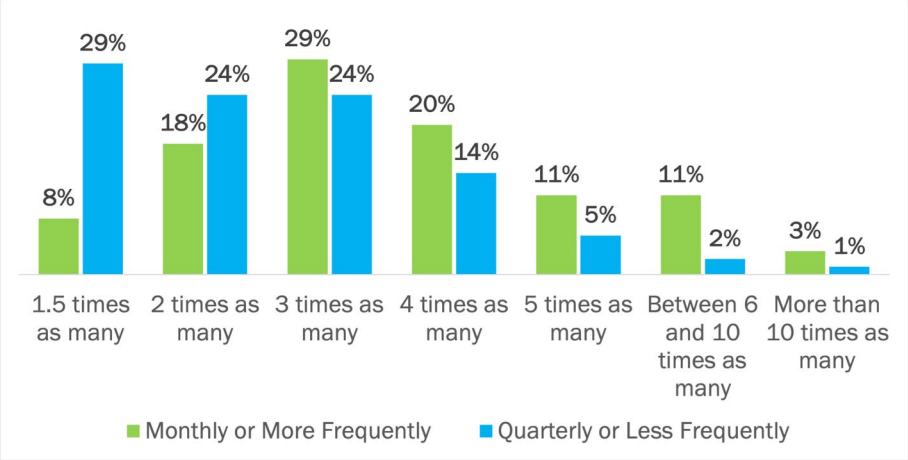
Figure 4
Rate of Increase in Messages Reported as Suspicious
Percentage of respondents



Source: Osterman Research (2021)

The frequency of training has an impact on the rate of increase in reporting suspicious messages. For organizations offering cybersecurity awareness training less frequently—which we interpreted as quarterly or less—77% of respondents indicated the increase in reporting volume was three times at most. For organizations offering cybersecurity awareness training on a daily, weekly or monthly cadence, the rate of increase was greater, with 74% of respondents indicating a rate of increase between three and 10 or more times. See Figure 5.

Figure 5
Correlating Training Frequency with Reporting Increase
Percentage of respondents



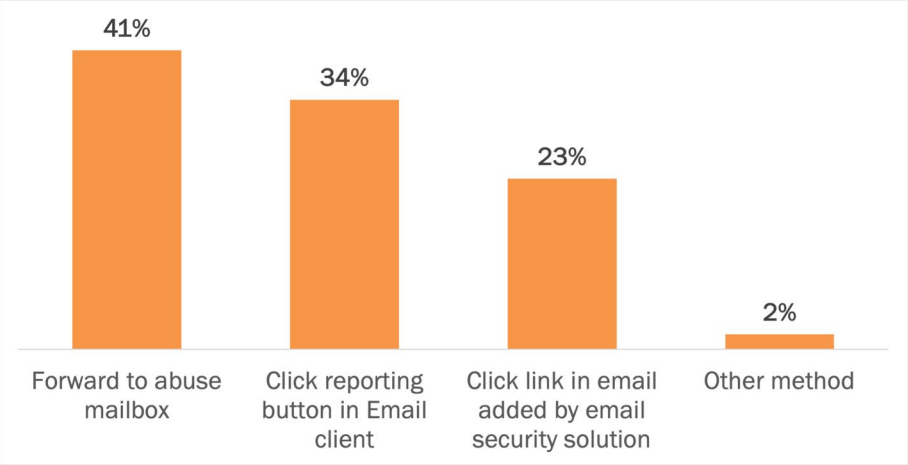
Source: Osterman Research (2021)

80% of respondents indicated an increase in the number of reports submitted after cybersecurity awareness training.

REPORTING SUSPICIOUS MESSAGES FOR FURTHER ANALYSIS

Over half of organizations are making it very easy to report messages as potentially suspicious. Almost three-fifths of organizations make use of either a button in the email client to click (34%) or a link in an email message to click (23%) for submitting reports. Both methods decrease the friction involved in reporting a message to a single click. By comparison, forwarding a message to an abuse mailbox involves at least the additional step of typing or selecting the correct destination email address. From an organizational perspective, forwarding a message to an abuse mailbox has a higher likelihood of requiring a human analyst to review and remediate the suspicious message, rather than being able to rely on automated security controls as with the other two. See Figure 6.

Figure 6
Method of Reporting Suspicious Email Messages
Percentage of respondents

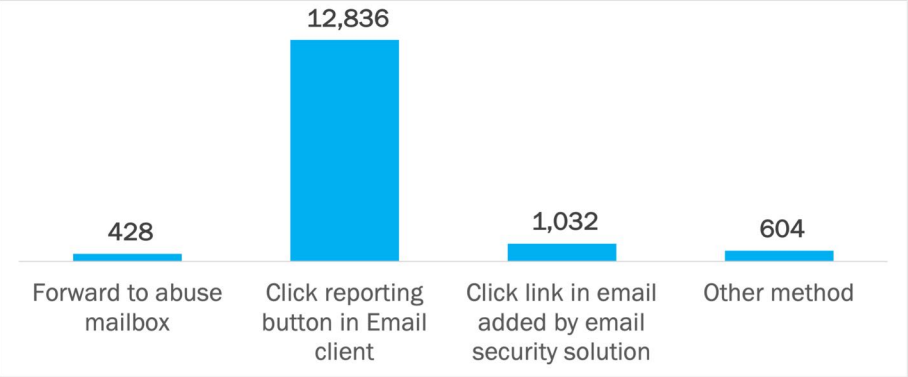


Source: Osterman Research (2021)

Over half of organizations are making it very easy to report messages as potentially suspicious.

The two easiest methods of reporting suspicious messages lead to higher numbers of reports being submitted. The button in the email client results in the most. See Figure 7.

Figure 7
Average Suspicious Messages Reported by Reporting Method Used
Percentage of respondents

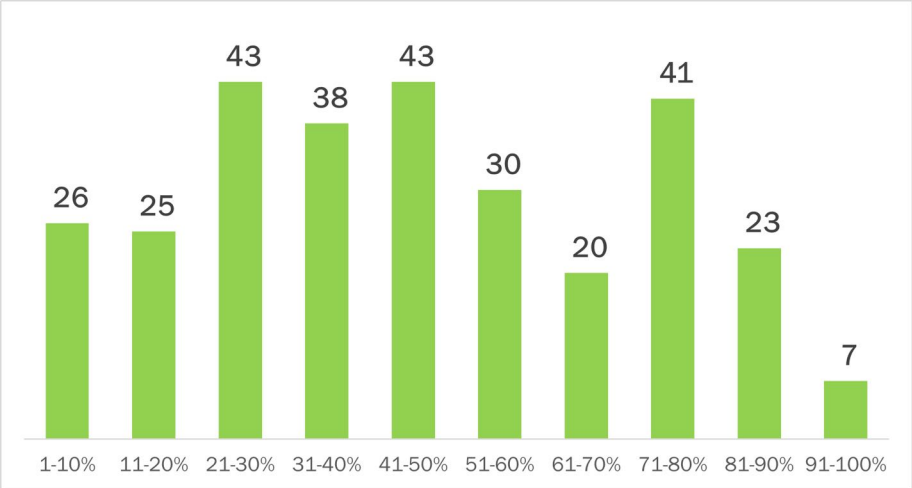


Source: Osterman Research (2021)

RESPONDENTS HAD WIDELY VARYING RESULTS ON BENIGN VS. MALICIOUS MESSAGES

We asked respondents what percentage of messages that are reported as suspicious by employees end up being benign (or "not malicious") after investigation. The results varied widely, and there was no clear or discernable pattern in the answers given. See Figure 8, where we report the count of benign messages in 10 grouped percentage bands.

Figure 8
Percentage of Reported Messages That Are Not Malicious
Count of respondents



Source: Osterman Research (2021)

From the above chart, the following observations (and speculations) can be made:

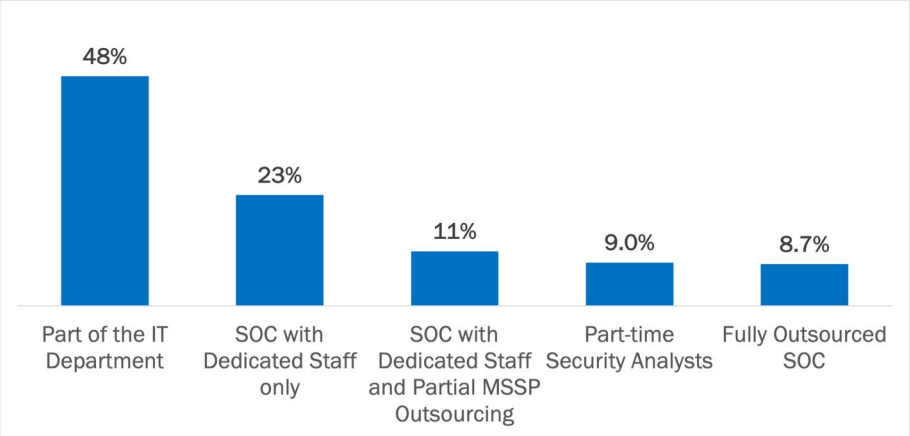
- The data shows that only seven out of almost 300 respondents who answered this question with a valid response found that almost all reported messages were benign.[8] That is, for the vast majority of organizations, employees are reporting messages that are indeed malicious.
- While different organizations will face a different profile of malicious vs. benign messages, we would expect to see a clearer grouping across an aggregated set of data. One explanation could be that organizations lack the tooling to accurately record malicious vs. benign messages, and thus respondents speculated on the result set.

At most organizations, employees are reporting messages that are indeed malicious. On average, almost half are benign.

LACK OF PROFESSIONALS WITH EXPERTISE AND TOOLING IN EMAIL SECURITY THREATS

Few organizations employ dedicated email analysts with professional training and tooling in threat identification and mitigation for email-borne threats. At almost half of organizations, the security response function is just part of the general IT department. Even for organizations with a dedicated Security Operations Center (SOC) internally or as part of an outsourcing arrangement, while it is more likely that greater expertise and tools can be brought to bear on email threats specifically, it depends on the design of the department or the terms of the outsourcing agreement. See Figure 9.

Figure 9
Organizing the Security Response Function
Percentage of respondents



Source: Osterman Research (2021)

Dedicated analysts with specific training and the right tooling for email analysis are necessary for prompt and effective resolution. Areas for focus and tooling include:

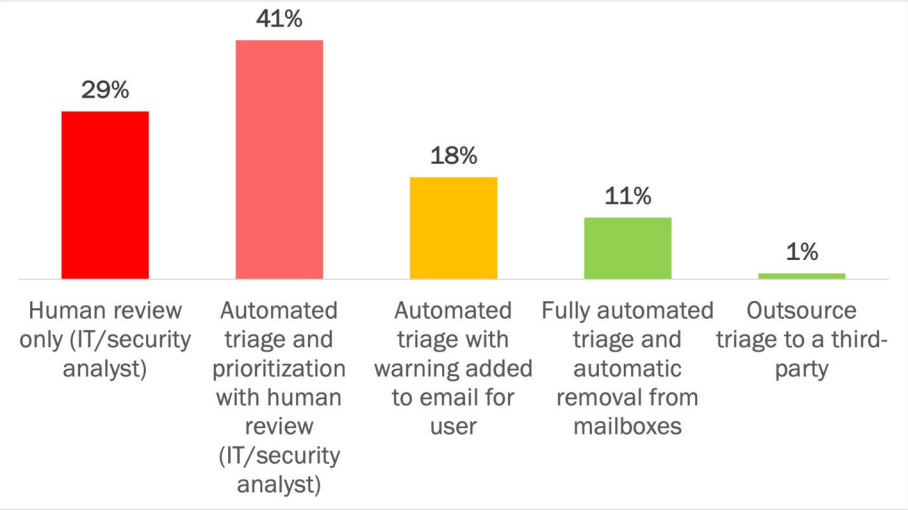
- The insight and tooling to determine whether a suspicious message is malicious or not.
- The tooling to locate and remediate other exact copies of a malicious message across all mailboxes in the organization, along with other messages that have similar characteristics.
- The tooling to update filters, machine learning models, and other methods of pre-delivery analysis for suspicious and malicious indicators in email messages, links, and attachments.

Few organizations employ dedicated email analysts with professional training and tooling in threat identification and mitigation for email-borne threats.

FEW ORGANIZATIONS HAVE THE RIGHT TOOLING

Only 11% of organizations have the right tooling in place to automatically triage email messages reported as suspicious and also enable the fully automatic removal from mailboxes of messages subsequently determined to be malicious. Almost one-third of organizations have no tooling available and rely completely on human analysts in an IT or a cybersecurity role. Three-fifths of organizations use automation plus human review—41% on automation plus human review by an IT or cybersecurity analyst, and 18% on automation plus subsequent human review by the end user. These results demonstrate the blended approach that is necessary given the complexity of the problem. Without human intervention to make a definitive decision, remediating a suspicious email can result in false positives. See Figure 10.

Figure 10
Determining Whether a Suspicious Message is Malicious
Percentage of respondents



Source: Osterman Research (2021)

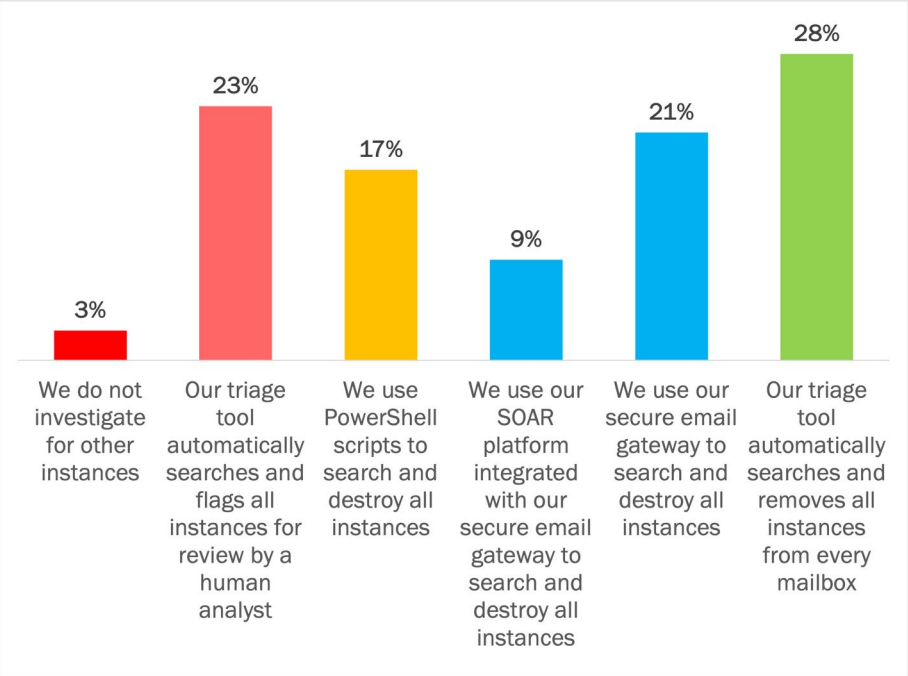
The lack of automation also extends at some organizations to removing (remediating) malicious messages from users' mailboxes. Remediation is triggered in 28% of respondents' secure email gateways, and another 13% of respondents use the SOAR platform integrated with their security email gateway. Sixteen percent are reliant on PowerShell scripts, and at 6% of organizations, users are told to delete the message manually from their mailbox.

Only 11% of organizations have the right tooling in place to automatically triage email messages and automatically remove malicious messages from mailboxes.

MOST ORGANIZATIONS RELY ON HUMAN ANALYSTS TO PERFORM WIDER DISCOVERY

Determining that a suspicious message is actually malicious is only the first step in remediating the threat posed. A critical step after making the malicious determination is to remove the message from the mailbox of the employee who submitted the report in the first place, and a second critical step is to remove any other instances from other mailboxes across the organization. Just under one-third of organizations rely on their triage tool to automatically search and remove all instances from every mailbox. There is a high degree of reliance on human analysts at other organizations to do the same. See Figure 11.

Figure 11
Wider Discovery of Malicious Messages
Percentage of respondents



Source: Osterman Research (2021)

Three percent of organizations do not investigate for other instances at all—not by PowerShell, SOAR platform, secure email gateway, or a triage tool. Failing to look for other instances is a dangerous approach when threat actors unleash targeted phishing attacks on an organization.

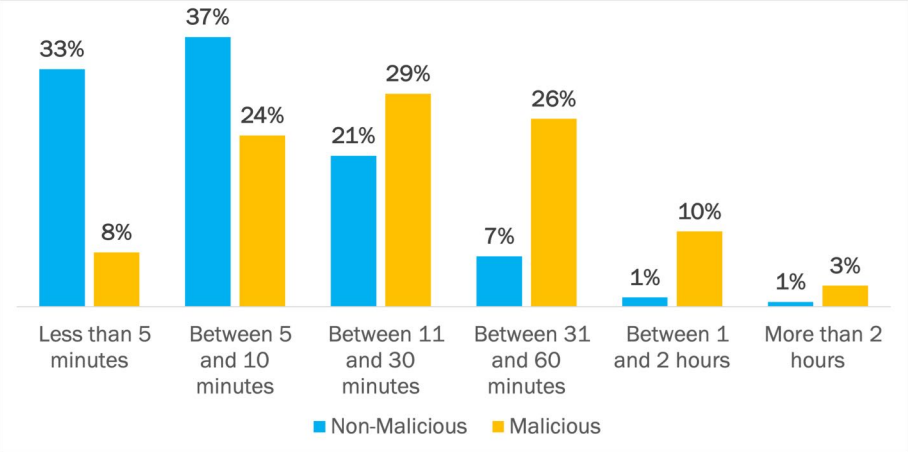
Interestingly 23% of respondents use a triage tool to automatically identify and flag all instances but stop short of automatically removing those instances. These organizations require a human analyst to review the identified list of instances before deleting them. This could indicate a low level of confidence in current triage tools to accurately identify other instances, or that it is still early days for using a triage tool and a fully automated search-and-destroy approach has not yet been deployed.

Most organizations rely heavily on human analysts to perform wider discovery for other instances of malicious messages.

TIME TAKEN TO DETERMINE WHETHER A MESSAGE IS MALICIOUS

For non-malicious email messages, 70% of organizations are able to analyze each email and close the incident in less than 10 minutes. For malicious email messages, the time taken is longer—with 79% of organizations saying it takes between five and 60 minutes per message. It is taking organizations longer to rule out all possible malicious factors than to judge a message as clear of such factors. See Figure 12.

Figure 12
Determining Maliciousness and Closing Each Incident
Time taken by percentage of respondents



Source: Osterman Research (2021)

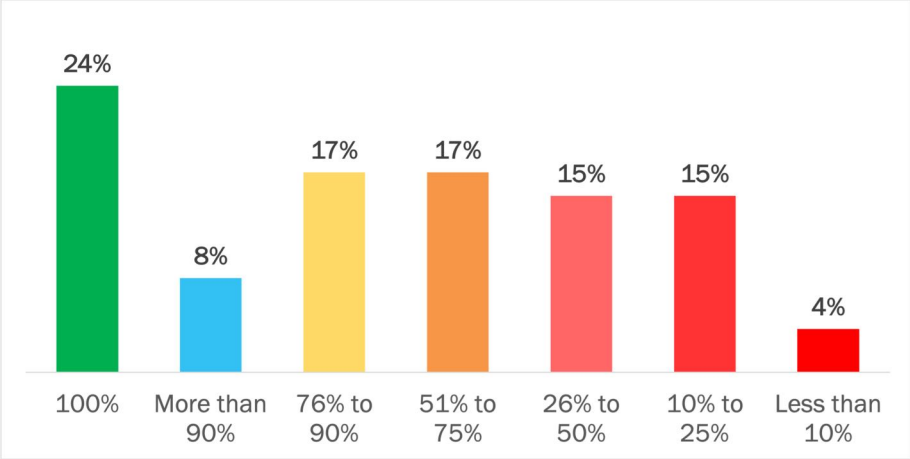
The time taken to make both determinations varies significantly with the approach taken at each organization. The most automated approach takes the shortest time for both types. Surprisingly, the automated approach that relies on human review takes the longest time—almost twice as long as human analysis only. This is perhaps because the automated tool hides the context that a human analyst needs to make a final determination.

Determining if a message is malicious takes between five and 60 minutes per message in most organizations.

MOST ORGANIZATIONS DO NOT ANALYZE ALL REPORTED EMAILS

The majority of organizations do not analyze all of the emails reported as suspicious to determine if they are malicious. The lack of coverage undermines the purpose of training employees to report suspected messages in the first place. More than two-thirds of organizations analyze 90% or fewer of reported emails. Only a quarter of organizations analyze the full 100% of reported messages. See Figure 13.

Figure 13
Reported Emails That Are Analyzed for Maliciousness
Percentage of respondents



Source: Osterman Research (2021)

There were several interesting correlations with answers to other questions in the survey, for example:

- Organizations relying on human analysts or human intervention to determine whether an email was malicious or not analyzed 100% of emails at about the same rate as organizations using a fully automated process. When human analysts are the dominant approach, there is a greater need to analyze the full complement of reported messages in order to ensure that no malicious messages slip through. With automated analysis, there is a greater ability to use similarity analysis to rule out the variations.
- Organizations relying on a fully automated triage tool or an outsourcing agreement analyzed an average of 71% of all reported messages. In comparison, organizations relying on human analysts or involvement in the analysis process analyzed 64%, or about 10% fewer messages.
- Organizations that analyze the full complement of reported email messages receive almost three times as many reports of suspicious messages. The feedback loop of analysis and remediation is essential to fostering ongoing involvement by employees in reporting messages. If many messages are not reported and no feedback is provided, employees fail to see the value in reporting messages and cease their engagement in the process. The net result is that a greater number of malicious messages are left unchecked and available to employees when the analysis process is not completed.

The majority of organizations do not analyze all of the emails reported as suspicious to determine if they are malicious.

Summary

People are an essential part of the security posture at an organization, and effective cybersecurity awareness training shows employees how to defend against security threats. Employee engagement through reporting suspicious messages for triage is an important aspect of their responsibilities, but this relies on having effective tooling, processes, and personnel in place to respond promptly and effectively. Many organizations still have a significant way to go to make such arrangements the common way of operating.

Sponsored by Mimecast

MIMECAST

Mimecast (NASDAQ: MIME) was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together. We are the company that built an intentional and scalable design ideology that solves the number one cyberattack vector—email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance, and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error, and technology failure, and to lead the movement toward building a more resilient world. Learn more about us at www.mimecast.com.

www.mimecast.com

@mimecast

UK/EUROPE
+44 (0) 207 847 8700
info@mimecast.com

NORTH AMERICA
+1 800 660 1194
+1 781 996 5340
info@mimecast.com

SOUTH AFRICA
+27 (0) 117 223 700
0861 114 063
info@mimecast.co.za

AUSTRALIA
+61 3 9017 5101
1300 307 318
info@mimecast.co.au

[1] Verizon Enterprise, 2020 Data Breach Investigations Report, May 2020, at https://enterprise.verizon.com/en-gb/resources/reports/dbir/

[2] FBI, 2019 Internet Crime Report Released, February 2020, at https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[3] FBI, FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics, March 2021, at https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

[4] Simon Chandler, Google Registers Record Two Million Phishing Websites in 2020, November 2020, at https://www.forbes.com/sites/simonchandler/2020/11/25/google-registers-record-two-million-phishing-websites-in-2020/

[5] Chelsea Sheasley, As Remote Learning Spreads, So Have Cyberattacks. Are Schools Ready?, November 2020, at https://www.csmonitor.com/USA/Education/2020/1103/As-remote-learning-spreads-so-have-cyberattacks.-Are-schools-ready

[6] Lindsey O'Donnell, How Email Attacks are Evolving in 2021, February 2021, at https://threatpost.com/email-security-attacks-bec/163869/

[7] Jordan Valinsky, Shark Tank Host Loses $400,000 in a Scam, February 2020, at https://edition.cnn.com/2020/02/27/business/barbara-corcoran-email-hack-trnd/index.html

[8] Three respondents did not provide an answer to the question. One respondent gave a percentage value of 150%, which was an invalid answer to the question.