Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **February 2020**
Sponsored by **IRONSCALES**

Robust Email Security Requires Alignment Between Security Practitioners and Decision Makers

Executive Summary

Phishing is the leading concern among security decision-makers and influencers, and the vast majority of phishing comes through the email channel in most organizations. Underscoring just how serious email phishing has become are the following data points:

- Research for the Verizon *2019 Data Breach Investigations Report* found that 32 percent of the data breaches that occurred in 2018 were the result of some form of phishing activity, but more than 90 percent of cyber attacks begin with a phishing email[i].
- The same report found that "phishing was present in 78% of Cyber-Espionage incidents and the installation and use of backdoors."
- The FBI's Internet Crime Complaint Center (IC3) received 467,361 complaints during 2019 totaling $3.5 billion in losses, an increase of 30 percent compared to 2018. Business Email Compromise (BEC) comprised more than half of 2019's losses ($1.77 billion) despite constituting *only* 23,775 of the total complaints to the IC3[ii].

KEY TAKEAWAYS

Here are the key takeaways from the research conducted for this white paper:

- On some issues, we found that there is a serious disconnect between the perceptions of decision makers and practitioners. For example:
  - Decision-makers are four times more likely than practitioners to consider phishing to be the highest priority for their organizations.
  - Practitioners are more focused on the technical details of phishing and may consider that they have somewhat of a handle on the issue, while decision-makers are focused more on the "bigger picture" of the business risk that is a consequence of phishing.
- The need to address phishing is of significant concern to mid-sized and large organizations, with decision-makers considering it to be a higher priority than do practitioners. Interestingly, respondents in the UK were about three times more likely to report phishing as their "highest priority", despite the fact that US organizations reported receiving significantly more phishing attacks.
- There is a critical need for real-time threat intelligence to more thoroughly address phishing – there is a significant gap between current use of threat intelligence in the context of phishing and where use of it should be.
- Most organizations have been victimized by phishing, the most common impact being an infection with non-ransomware malware.
- Security teams spend significant amounts of time and effort dealing with phishing. We found that just the labor component of dealing with phishing would cost a 5,000-user organization nearly $8,900 per month.
- Three-quarters of organizations cannot act on phishing intelligence automatically in real time, while nearly 90 percent cannot orchestrate phishing intelligence from multiple sources in real time in the context of their overall email security solution(s).
- It takes a substantial amount of time for most organizations to detect, investigate and remediate phishing emails: 30 percent take from six to 30 minutes to identify a phishing attempt after it enters the network and another 14

Phishing is the leading concern among security decision-makers and influencers.

percent take from 31 to 60 minutes. Sixty-five percent of organizations take more than five minutes to detect the typical phishing email.

- However, 70 percent of organizations take more than five minutes to remove it from corporate mailboxes, but the average time-to-click on a phishing email is only 82 seconds.
- Most organizations are using several tools to combat phishing, secure email gateways being the most common approach to doing so. However, most organizations are not using all of the tools that could be brought to bear on phishing – the result is that most analysts can handle no more than four phishing threats per day.
- Nearly three in five organizations train their users on proper email security protocols no more than twice per year, while only 19 percent – one-third of this number – do so much more frequently (at least monthly or continuously).
- The security skills shortage is having an impact on security teams' ability to deal with phishing properly.
- More than 70 percent of organizations use only manual processes for reviewing user-reported phishing emails, making it far too labor-intensive.

ABOUT THE SURVEY

The survey conducted for this white paper was conducted with 252 individuals in the United States and the United Kingdom. In order to qualify for the survey, respondents had to a) work for an organization that has at least 500 employees, b) have a security-focused role, and c) had to be knowledgeable about how their organization deals with phishing emails. Respondent organizations serve a wide range of industries. Moreover, we segmented the survey audience into "decision-makers" (CIOs, CISOs and directors of information security) and "practitioners" (email administrators, information security analysts, IT managers/directors, security architects and SOC analysts) to better understand the differences in views and perceptions between these two groups.

In this report we differentiate between "decision-makers" and "practitioners". We have included in the former category CIOs, CISOs and directors of information security; practitioners, on the other hand, include email administrators, information security analysts, IT managers/directors, security architects, and SOC analysts. In short, the key differentiator between decision-makers and practitioners is that the former are higher level roles, while the latter are "in the trenches" and making more hands-on, day-to-day decisions about phishing issues.

Respondents in the UK were roughly three times more likely to report phishing as their "highest priority".

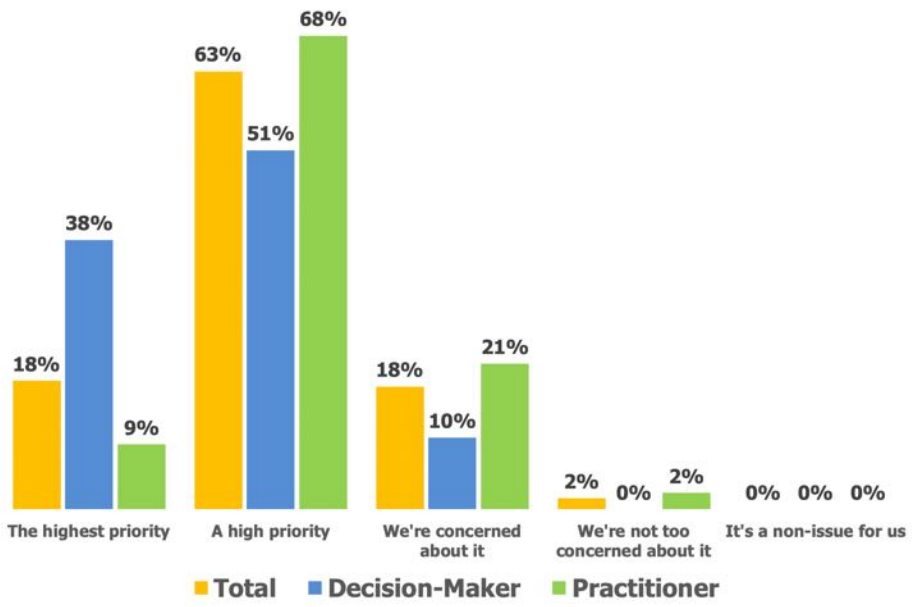
Survey Findings

ADDRESSING PHISHING IS A HIGH PRIORITY

Not surprisingly, our research found that phishing, in the context of all of the other security issues with which security have to contend, is a high priority. As shown in Figure 1, 18 percent of those surveyed consider phishing to be the "highest priority" for their organizations, while more than three in five consider phishing to be a "high" priority. We found that respondents in the UK were roughly three times more likely to report phishing as their "highest priority", despite the fact that US organizations reported receiving significantly more phishing attacks.

These results are consistent with another Osterman Research survey conducted in 2019[iii] that found phishing was the leading concern among security-focused decision-makers and influencers – 74 percent of those surveyed reported that they were "concerned" or "extremely concerned" about phishing attempts.

Figure 1
Priority of Phishing Relative to Other Security Issues



Source: Osterman Research, Inc.

Interestingly, however, decision-makers are four times more likely than practitioners to consider phishing to be the highest priority for their organizations. Moreover, when the "highest" and "high" priorities for phishing are summed, decision-makers are significantly more concerned than practitioners about the issue – 89 percent to 77 percent.

This difference may be due to the fact that practitioners are more focused on the technical details of phishing and may consider that they have somewhat of a handle on the issue, whereas decision-makers are focused not only on the technical aspects of phishing, but are seeing the "bigger picture" of the business risk that is a consequence of phishing.

BAD THINGS HAPPEN AS A RESULT OF PHISHING

As shown in Figure 2, slightly more than one-half of organizations report that as a result of users interacting with a phishing link or attachment of some kind, their organizations experienced some sort of non-ransomware infection, while nearly two in five experienced a ransomware outbreak. Data breaches are also a common occurrence as a result of users interacting with a phishing email – mentioned by more than one-quarter of organizations as a consequence of phishing (organizations in the UK were more than three times likely to report that a data breach occurred as a result of a successful phishing attack than their US counterparts). Account takeovers are also common, cited by more than one in five organizations.

Data breaches are a common occurrence as a result of users interacting with a phishing email.

Figure 2
Incidents That Have Occurred as a Result of Users Clicking on a Link, Being Asked to Wire Funds, Handing Over Their Credentials, or Opening an Attachment in a Phishing Email

Incident	Total	Decision-Makers	Pract-itioners
One or more endpoints was infected with malware other than ransomware	51%	56%	49%
One or more endpoints was infected with ransomware	38%	43%	35%
We experienced a data breach	27%	35%	23%
We had one or more accounts taken over by bad actors	21%	16%	23%
We fell victim to BEC	17%	17%	17%
Other	11%	9%	12%

Source: Osterman Research, Inc.

Overall, we found that practitioners are somewhat less likely to report negative consequences from users interacting with phishing emails in the context of ransomware, non-ransomware malware and data breaches than their decision-maker counterparts. However, practitioners are somewhat more likely to report that account takeovers have occurred as a result of phishing. Here again, decision-makers are more focused on the business consequences of security incidents, and so are more attuned to issues like data breaches than are their more technically focused practitioner counterparts.

PHISHING CONSUMES LOTS OF SECURITY TEAM TIME

Phishing emails consume a great deal of security teams' time. As shown in Figure 3, 30 percent of security teams "frequently" or "very frequently" deal with phishing emails that include or link to non-ransomware malware, 23 percent spend this level of effort on issues surrounding credential theft, and more than one in five are spending this much time on account takeovers.

Phishing emails consume a great deal of security teams' time.

Figure 3
Frequency With Which Security Teams Deal With Phishing Emails
Percentage Responding "Frequently" or "Very Frequently"

Type of Phishing Email	Total	Decision-Makers	Pract-itioners
Malware other than ransomware	30%	36%	27%
Credential theft	23%	31%	19%
Account takeover attempts	21%	27%	19%
Ransomware	19%	29%	15%
BEC	15%	24%	11%
Threats other than those listed above	12%	19%	8%

Source: Osterman Research, Inc.

Here again, decision-makers seem to be overestimating the amount of time that their security teams are spending on various types of threats – practitioners who are directly dealing with these issues estimate lower levels of effort required to deal with malware, credential theft and other threats. Clearly, there is a misalignment between the perception of when a threat is "dealt with" and when it is truly dealt with.

PHISHING TAKES A LONG TIME TO DETECT IN MANY CASES

The good news: our research found that 12 percent of organizations can identify and remove a phishing email within one minute of it entering the network, while 33 percent can do so within five minutes, as shown in Figure 4. Organizations in the UK reported slightly longer detection and remediation times for phishing attacks than their US counterparts, but a significantly greater proportion of respondents in the US told us that they did not know how long it took for identification and remediation of these threats.

The bad news: 67 percent of organizations take six minutes or longer to identify and remove a phishing email. What makes this especially bad news is the fact that eight percent of users will click on a phishing email within 30 seconds of receiving it, while this figure jumps to 30 percent within the first 60 seconds[iv]. That means that the vast majority of organizations cannot identify – and certainly cannot remediate – phishing emails before a large proportion of their users will potentially click on a phishing email that enters the network. This points to the critical need for real-time threat intelligence.

Figure 4
Elapsed Time Between the Typical Phishing Email Entering the Network and its Removal From Company Mailboxes

Time	Total	Decision-Makers	Pract-itioners
Less than one minute	12%	12%	12%
Up to five minutes	21%	17%	22%
Six to 30 minutes	30%	30%	29%
31 to 60 minutes	18%	23%	15%
Several hours	14%	15%	14%
Several days	2%	1%	2%
Weeks or longer	0%	0%	0%
I really don't know	4%	1%	5%

Source: Osterman Research, Inc.

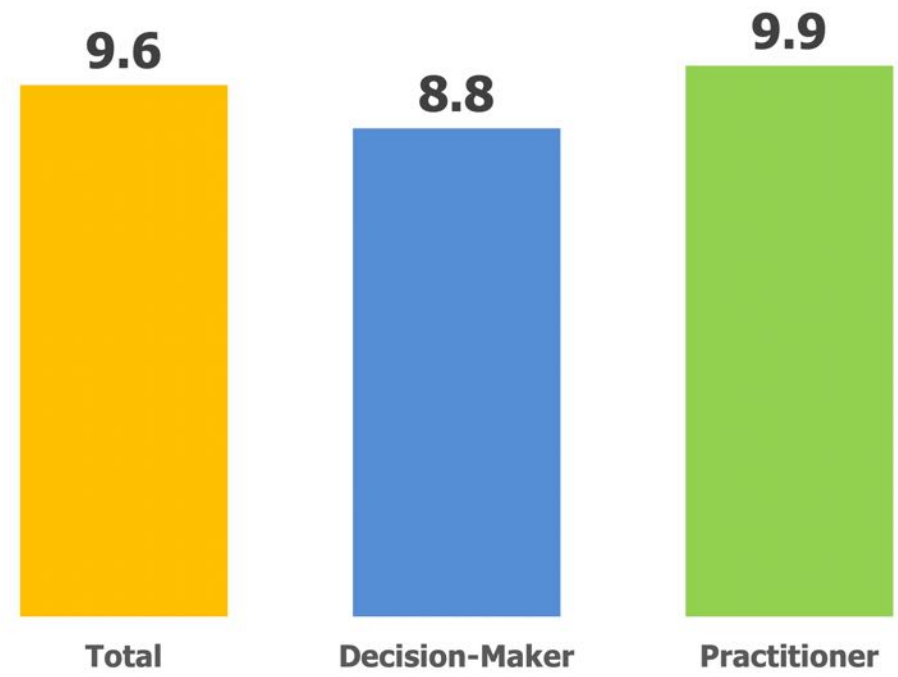
67 percent of organizations take six minutes or longer to identify and remove a phishing email.

DEALING WITH PHISHING IS TIME-CONSUMING

The organizations we surveyed, on average, spend 9.6 person-hours per 1,000 employees per week investigating, detecting or remediating phishing emails, as shown in Figure 5. Interestingly, decision-makers' estimates are significantly lower than practitioners' estimates of the time investments required to deal with phishing attempts through their lifecycle, and significantly so – decision-makers' estimates are about 11 percent less than those of practitioners, those who are "in the trenches" dealing with phishing issues. We also found that the time investments for UK-based organizations is slightly lower (9.2 person-hours per 1,000 hours per week) than for their US counterparts (9.9).

What this means in that a typical workweek of 40 hours, 24 percent of the security team's time is spent just investigating, detecting or remediating phishing emails – more than one day per week! It's also important to note that some phishing emails go undetected, resulting in time not spent in dealing with them due to a lack of visibility and intelligence about phishing activities.

Figure 5
Time Spent During a Typical Week by the Security Team Investigating, Detecting or Remediating Phishing Emails
Person-hours per 1,000 employees



Source: Osterman Research, Inc.

This is a significant finding, particularly for smaller security teams that simply do not have the resources to devote to investigating, detecting and remediating phishing emails. For example, in a 500-seat organization, these activities would consume more than 10 percent of a security team's (often just a one-person function) time.

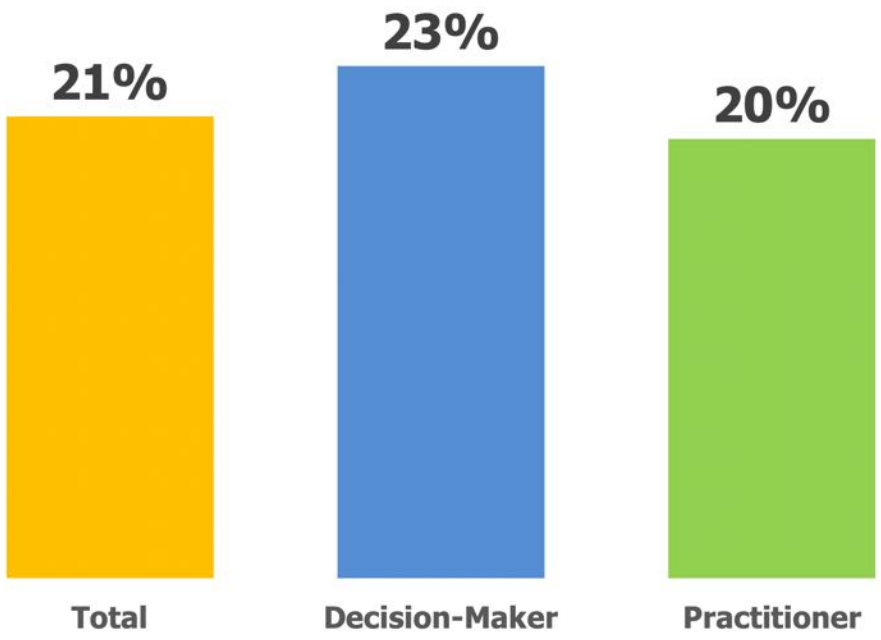
The fact that decision-makers, on average, underestimate the amount of time required by practitioners to deal with phishing is indicative of the fact that CIOs, CISOs and others are somewhat more removed from the minutiae of what is involved with dealing with all aspects of phishing. Decision-makers in many cases may underappreciate just how difficult current practices and processes are, as well as the gaps that exist in current anti-phishing defenses. In some organizations, that may make it more difficult for practitioners to get all of the budget and headcount support they need to address phishing threats.

Decision-makers, on average, underestimate the amount of time required by practitioners to deal with phishing.

PHISHING MANAGEMENT TAKES SUBSTANTIAL EFFORT

We found that slightly more than 20 percent of security analysts' time is spend on investigating and/or remediating phishing emails, as shown in Figure 6. The difference between decision-makers' estimates and practitioners' estimates in this regard were minimal.

Figure 6
Percent of Their Time During a Typical Week That an Analyst Spends on Investigating and/or Remediating Phishing Emails



Source: Osterman Research, Inc.

DEALING WITH PHISHING IS EXPENSIVE

If we assume that the average salary for a security analyst is $85,799 per year[v], using practitioners' estimates of the time required to investigate, detect or remediate emails as shown in Figure 5 works out to a total time expenditure of 515 person-hours per year per 1,000 employees, or a total cost of $21,235 per 1,000 employees. That works out to a labor-only cost of $1.77 per employee per month just to deal with the investigation, detection and remediation of phishing emails – an organization of 5,000 employees, therefore, will spend in excess of $106,000 annually on labor alone to address phishing emails.

An organization of 5,000 employees will spend in excess of $106,000 annually on labor alone to address phishing emails.

MOST USE SECURE EMAIL GATEWAYS TO DEAL WITH PHISHING

We found that about two-thirds of organizations use a secure email gateway solution to deal with phishing, although practitioners cited the use of this approach slightly more often than their decision-maker counterparts, as shown in Figure 7. Other solutions are also widely used, including Microsoft's Advanced Threat Protection (ATP) and Exchange Online Protection (EOP), largely as a result of the significant penetration of Office 365 into the business-grade email market (as of January 2020, there are more than 200 million users of Office 365[vi]). Only a tiny percentage of organizations report that they are not using any sort of anti-phishing solution. Organizations in the US are much more likely to use a secure email gateway solution (82 percent) than their UK-based counterparts (51 percent).

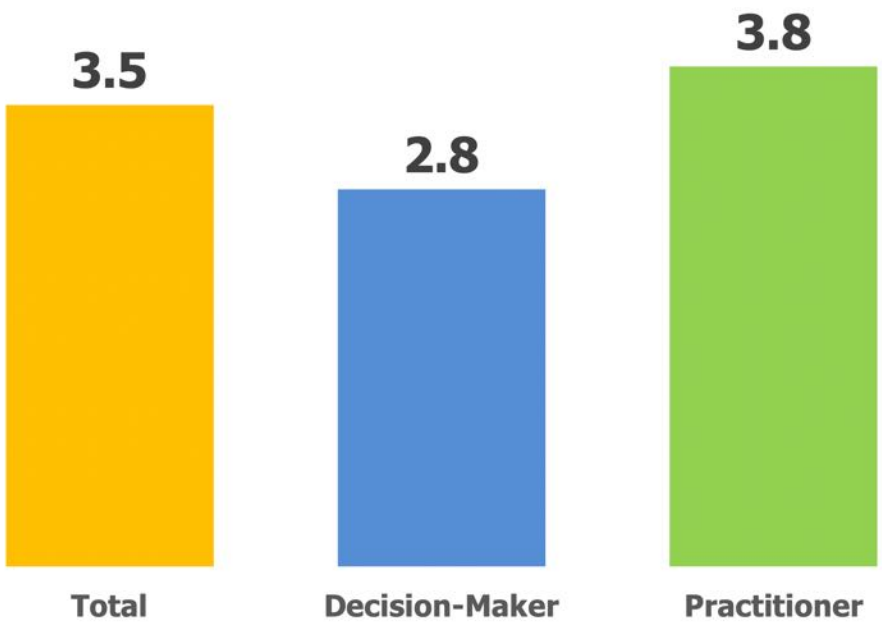
Figure 7
Anti-Phishing Solutions in Use

Solution	Total	Decision-Makers	Pract-itioners
A secure email gateway solution	67%	63%	68%
Microsoft ATP	48%	55%	45%
Microsoft EOP	33%	37%	31%
Google G Suite	32%	40%	28%
We are not using an anti-phishing solution	1%	0%	2%

Source: Osterman Research, Inc.

As shown in Figure 8, organizations report that they are using an average of 3.5 different tools to detect and respond to phishing emails, although decision-makers offered an estimate that is significantly lower than their practitioner counterparts. This reflects the fact that decision-makers are more removed from the process of phishing management in many organizations and may not fully appreciate everything that goes into dealing with the detection, investigation and remediation of phishing emails.

Figure 8
Number of Different Vendors' Tools Deployed to Detect and Respond to Phishing Emails



Source: Osterman Research, Inc.

Organizations report that they are using an average of 3.5 different tools to detect and respond to phishing emails.

ORGANIZATIONS REPORT SIGNIFICANT PENETRATION OF ADVANCED TECHNOLOGIES

As shown in Figure 9, nearly two in five organizations report that they use artificial intelligence as part of their anti-phishing defenses, while nearly one-half report that they use machine-learning and 71 percent use automation. Practitioners are somewhat less likely to report the use of an artificial intelligence and machine-

learning technologies to address their phishing problems, but are slightly more likely to report the use of automation. Organizations in the UK report somewhat greater use of machine-learning technologies to combat phishing, but US-based organizations report higher levels of automation.

Figure 9
Use of Various Technologies as Part of Anti-Phishing Defenses

Incident	Total	Decision-Makers	Pract-itioners
Artificial intelligence			
Yes, we use this	39%	46%	36%
No, we don't use this, but will do so	49%	44%	51%
No, we don't use this and have no plans to do so	12%	10%	13%
Machine-learning			
Yes, we use this	49%	55%	47%
No, we don't use this, but will do so	40%	36%	42%
No, we don't use this and have no plans to do so	10%	9%	11%
Automation			
Yes, we use this	71%	67%	73%
No, we don't use this, but will do so	26%	32%	23%
No, we don't use this and have no plans to do so	4%	1%	5%

Source: Osterman Research, Inc.

Are organizations really using this level of artificial intelligence, machine-learning and automation? No and yes. There are not a significant number of anti-phishing technologies that fully exploit all of the potential benefits of these technologies in detecting, investigating and remediating phishing emails. However, a number of leading solutions that are currently available actually do use artificial intelligence, machine-learning and automation to varying degrees, addressing at least a portion of their customers' phishing management requirements through the use of these approaches. Moreover, this points to the fact that there is not a universal definition of true "automation" or "artificial intelligence".

SECURE EMAIL GATEWAYS AND USER TRAINING ARE RELIED UPON TO DEAL WITH VARIOUS THREATS

The two primary methods that organizations use to deal with polymorphic/rotating email attacks, fake login pages/emails, and Business Email Compromise (BEC) attempts are secure email gateways and users who have been trained to deal with these threats, as shown in Figures 10, 11 and 12. In most cases, we did not discover significant differences between decision-makers and practitioners in terms of the tools they use to address these problems. This strongly suggests that security teams have a false sense of security about dealing with these threats, particularly as cloud-based emails become more commonly used. However, we did find that for all three types of attacks/threats, US-based organizations cite "trained users recognizing these threats" much more frequently than their UK counterparts.

It is also important to note, as shown in the following three figures, that the heavy reliance on scripts and tools, playbooks and YARA Rules strongly implies that not nearly as much *true* automation is actually in use as many security analysts believe. This is an important misconception that security-focused decision-makers should address with their teams.

Heavy reliance on scripts and tools, play-books and YARA Rules strongly implies that not nearly as much true auto-mation is actually in use as many security analysts believe.

Figure 10
Solutions and Processes Used by the Security Team to Deal With Polymorphic/Rotating Email Attacks

Solution/Process	Total	Decision-Makers	Pract-itioners
A secure email gateway using signature-based detection	62%	67%	59%
Trained users recognizing these threats	52%	55%	51%
Scripts and tools	50%	45%	53%
Playbooks	19%	26%	17%
YARA Rules	11%	14%	9%
Not familiar with this type of attack	10%	5%	12%
We cannot deal with these attacks	6%	10%	5%
Other	2%	1%	2%

Source: Osterman Research, Inc.

Figure 11
Solutions and Processes Used by the Security Team to Deal With Fake Login Pages/Emails

Solution/Process	Total	Decision-Makers	Pract-itioners
A secure email gateway using signature-based detection	69%	76%	66%
Trained users recognizing these threats	70%	69%	70%
Visual similarity detection (computer vision)	20%	26%	18%
Other	4%	0%	6%

Source: Osterman Research, Inc.

Figure 12
Solutions and Processes Used by the Security Team to Protect Against BEC Attempts

Solution/Process	Total	Decision-Makers	Pract-itioners
A secure email gateway using signature-based detection	69%	77%	65%
Trained users recognizing these threats	68%	72%	66%
Mailbox-level anomaly detection	34%	35%	34%
DMARC	14%	12%	15%
Other	2%	3%	2%

Source: Osterman Research, Inc.

Some important capabilities to manage phishing and other security issues are lacking.

KEY CAPABILITIES ARE SERIOUSLY LACKING

As shown in Figure 13, some important capabilities to manage phishing and other security issues are lacking. For example, while 55 percent of the organizations surveyed are using threat intelligence feeds and 47 percent have real-time visibility into zero-day phishing attacks, those that do not are 45 percent and 53 percent, respectively. Making matters worse is the fact that 25 percent of organizations cannot act on phishing intelligence automatically in real time, while 13 percent cannot

orchestrate phishing intelligence from multiple sources in real time in the context of their overall email security solution(s). We found relatively little difference between decision-makers and practitioners with regard to these data points. US-based organizations are more likely than their UK counterparts to make use of threat intelligence feeds (60 percent vs. 50 percent).

Figure 13
"Which of the following is true in your organization?"

Incident	Total	Decision-Makers	Pract-itioners
We make use of threat intelligence feeds	55%	58%	53%
We have real-time visibility into zero-day phishing attacks	47%	48%	46%
Our threat intelligence feeds generate too many false positives	26%	29%	25%
We can't act on phishing intelligence in real time automatically	25%	21%	28%
We can't orchestrate phishing intelligence from multiple sources in real time into our email security solution	13%	12%	13%

Source: Osterman Research, Inc.

It's important to note that there can be limitations on the use of threat intelligence in the context of phishing emails. This was summarized nicely by the Vice President of Security Research at SpyCloud, who noted that reactionary organizations enable threat intelligence to become stale, and that threat intelligence, "fails when you don't mix multiple intelligence points to form a more complete story of your adversaries."

Fundamentally, organizations have a long way to go in the context of how they use phishing threat intelligence and how they integrate this data into their overall email security capabilities.

PHISHING MANAGEMENT IS CONSTRAINED BY LABOR

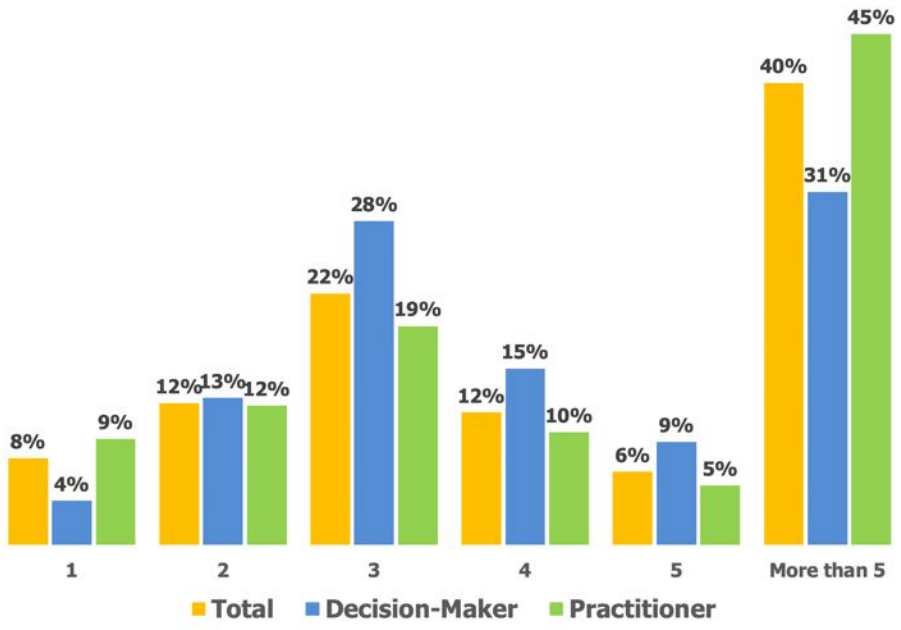
As shown in Figure 14, the majority of the organizations surveyed report that their security practitioners can handle no more than five phishing emails on a typical day for those cases where all mailboxes in the organization are subject to a phishing attack. In fact, practitioners in 56 percent of organizations can handle no more than four phishing emails per day assuming an organization-wide penetration of phishing emails. This is in contrast to the finding from other research that 60 percent of SOC analysts can handle seven to eight investigations per day[vii].

So, just how common is the scenario of multiple phishing attacks impacting all of the mailboxes in an organization on a daily basis? An Aberdeen analysis[viii] using IRONSCALES data from 2019 found that for every uniquely identified phishing email attack, anywhere from two to in excess of 40 mailboxes were affected. Moreover, the total number of organizations impacted by a particular phishing attack ranged from as few as five to more than 150.

In other words, even targeted attacks are becoming more common, and every phishing email attack can affect multiple mailboxes at many different organizations. This requires literally hundreds of successful phishing attack detections at each organization. Based on this analysis, things will get worse: more than four in ten phishing email attacks are polymorphic – a technique used by phishers to modify phishing attempts in order to evade conventional security solutions. A polymorphic attack will change at least once, but can be changed hundreds of times.

Practitioners in 56 percent of organizations can handle no more than four phishing emails per day assuming an organization-wide penetration of phishing emails.

Figure 14
Number of Phishing Emails That an Analyst Can Handle per Day
Assumes that all mailboxes in the organization were affected



Source: Osterman Research, Inc.

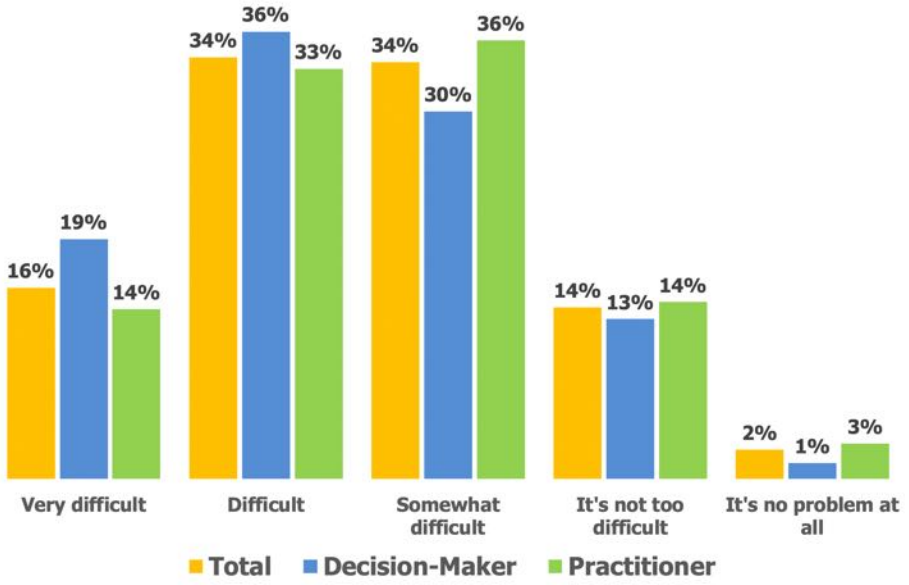
Overall, decision-makers have a somewhat lesser view of phishing management capabilities than practitioners. For example, while 45 percent of practitioners believe that they can manage more than five organization-wide phishing emails on a typical day, only 31 percent of decision-makers believe this is the case.

Decision-makers have a somewhat lesser view of phishing management capabilities than practitioners.

THE SECURITY SKILLS SHORTAGE IS REAL

Exacerbating the problem with the relatively low throughput for managing organization-wide phishing attacks is the fact that it's difficult for many organizations to find the right staffers for their security teams. The security skills shortage is widely discussed in industry publications and at conferences and our research corroborates those discussions, as shown in Figure 15. We found that 50 percent of those surveyed consider that hiring and retaining skilled IT security specialists is either "very difficult" or "difficult". In contrast, almost none of the survey respondents reported have no problem in finding and retaining these people.

Figure 15
Difficulty in Hiring and Retaining Skilled IT Security Specialists



Source: Osterman Research, Inc.

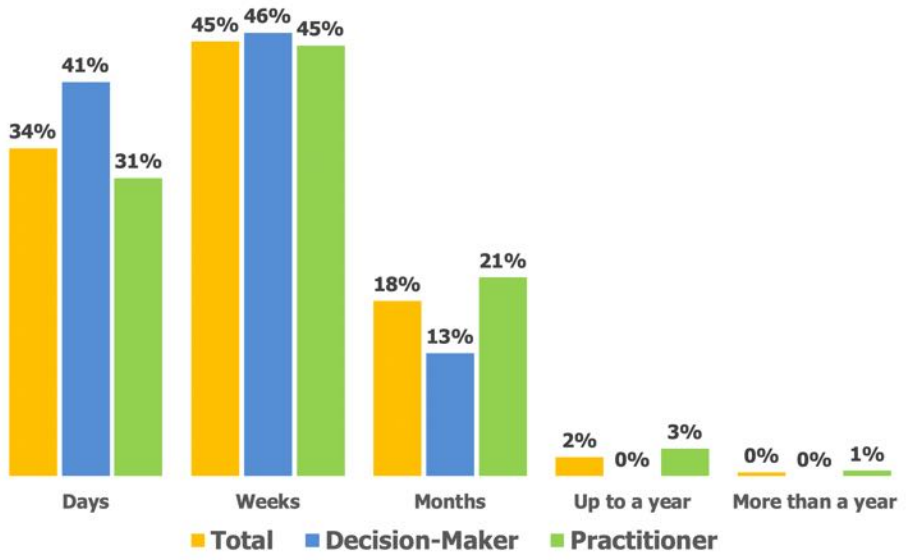
Decision-makers are somewhat more likely to consider the security skills and retention to be either "very difficult" or "difficult", while practitioners don't seem to believe that the problem is quite as serious. However, this may be due to the fact that in most organizations the burden of finding, hiring and retaining skilled security staffers falls more on decision-makers than it does on practitioners

TRAINING IS SOMEWHAT TIME-CONSUMING

As shown in Figure 16, the time required to train new security team members on organizational email security solutions and processes varies considerably. Overall, about one-third of organizations report that the time required to train these new staffers can be measured in "days", while nearly one-half believe that "weeks" are required to do so. Interestingly, practitioners believe that it takes somewhat longer to train new staffers than do decision-makers. For example, 10 percent more decision-makers believe that it takes "days" to train new staffers, while eight percent more practitioners believe that it takes "months" to do so properly.

The time required to train new security team members on organizational email security solutions and processes varies considerably.

Figure 16
Time Required to Train New Security Team Members on Email Security Solutions/Processes



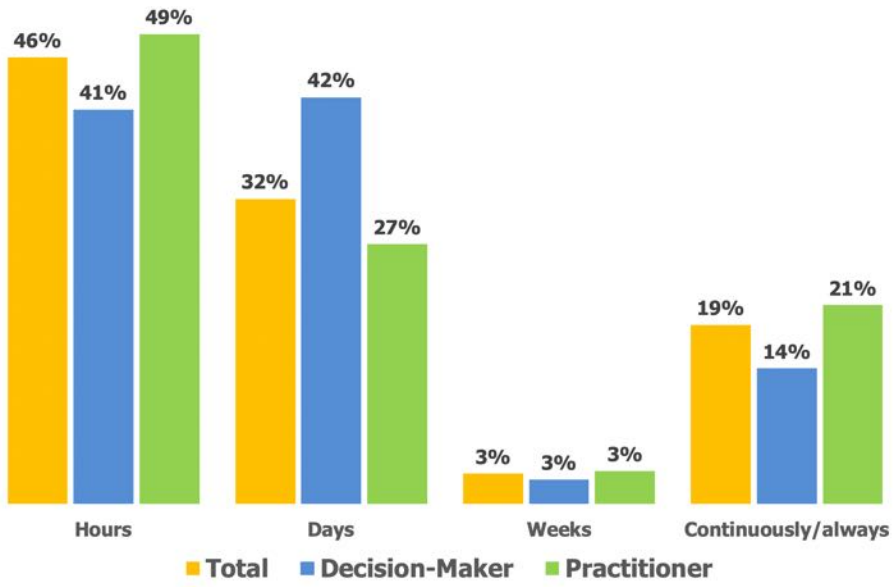
Source: Osterman Research, Inc.

UPDATING EMAIL SECURITY POLICIES VARIES

Our research found that roughly one in five organizations continuously updates and tweaks its corporate email security policies in a typical month, while a significantly larger proportion of organizations spends only "hours" during a typical month doing so. Interestingly, practitioners seem somewhat more divided when estimating the amount of time spent tweaking and updated email security policies – we found that a larger proportion of practitioners believe that just "hours" are required each month for these tweaks, but a larger proportion of practitioners also continuously updates them. Organizations in the US reported that significantly more US-based organizations (60 percent) reported that it takes "hours" to tweak and update email security policies than their UK-based counterparts (33 percent).

Roughly one in five organizations continuously updates and tweaks its corporate email security policies in a typical month.

Figure 17
Time Spent per Month by the Security Team Tweaking and Updating Corporate Email Security Policies



Source: Osterman Research, Inc.

USER TRAINING IS NOT ADEQUATE

Several Osterman Research surveys have found that many users do not receive sufficiently frequent training with regard to security issues and this survey is no different. As shown in Figure 18, 57 percent of organizations train their users on proper email security protocols no more than twice per year, while only 19 percent – one-third of this number – do so at least monthly or continuously. We did not find major differences between decision-makers and practitioners with regard to their estimates of the frequency of security awareness training for their users. We found that organizations in the UK were about five times more likely (19 percent) to report that users were trained just when they join the company than their US counterparts (five percent).

57 percent of organizations train their users on proper email security protocols no more than twice per year.

Figure 18
Frequency With Which End Users are Trained on Proper Email Security Protocols

Frequency	Total	Decision-Makers	Pract-itioners
Just when they join the company	12%	14%	11%
After a security incident occurs	8%	12%	7%
Once a year	18%	19%	17%
Twice a year	19%	15%	21%
Three to four times per year	19%	15%	21%
About every other month	5%	5%	5%
Monthly	6%	8%	5%
Continuously	13%	12%	14%
Never	0%	0%	0%

Source: Osterman Research, Inc.

So, what is the "right" frequency for security awareness training for end users? While there is no hard-and-fast answer that can apply to all organizations in all industries, Infosec recommends as a general rule training every 90 days, or four times per year[ix].

One of the important issues that security decision makers must deal with is determining the role of technology-based solutions versus training in the context of preventing various types of threats. Finding the right balance is key, especially for threats that do not contain any malware or links to malicious sites, such as BEC attempts. An Osterman Research survey in 2019[x] found that the majority of security decision makers believe that there is a role to play for both security awareness training *and* technology-based solutions, although this varies based on the type of threat. For example, while 40-plus percent of those surveyed view phishing and BEC prevention as mostly or completely about good training, only 17 percent consider that account takeover prevention is primarily about good training. Conversely, while only 11 percent consider spear phishing prevention to be primarily a technology-focused issue, 36 percent consider ransomware a problem to be addressed primarily or completely using technology solutions.

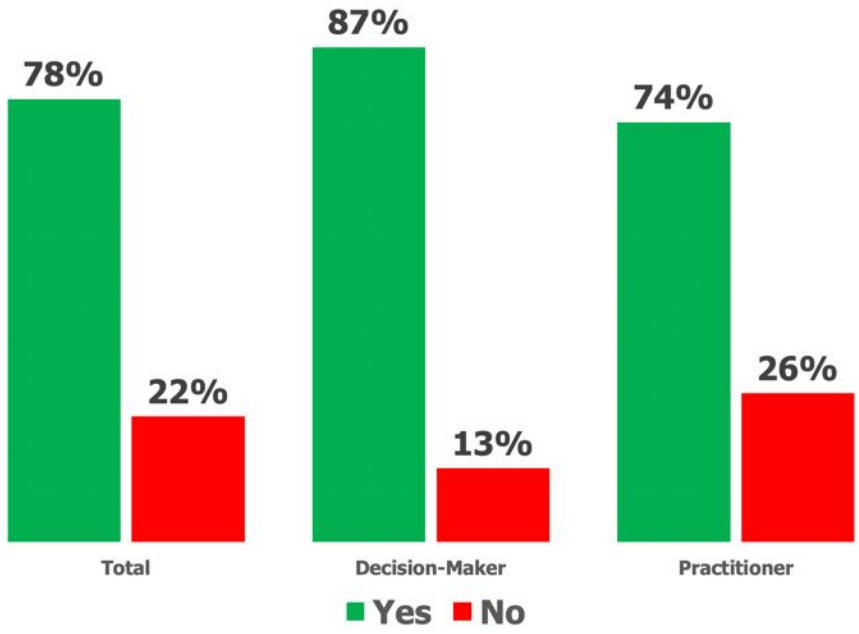
While all of these threats demonstrate a need for technology *and* training, there are clearly different views – and perhaps some misconceptions – about the emphasis that should be placed on both for a particular threat.

PHISHING SIMULATION IS COMMON

We found that the vast majority of organizations are using phishing simulation to train their users. As shown in Figure 19, 78 percent of organizations are using this type of training for their users – decision-makers are significantly more likely to report that phishing simulation is used in their organizations.

The vast majority of organizations are using phishing simulation to train their users.

Figure 19
"Does your organization use phishing simulation to train your users?"

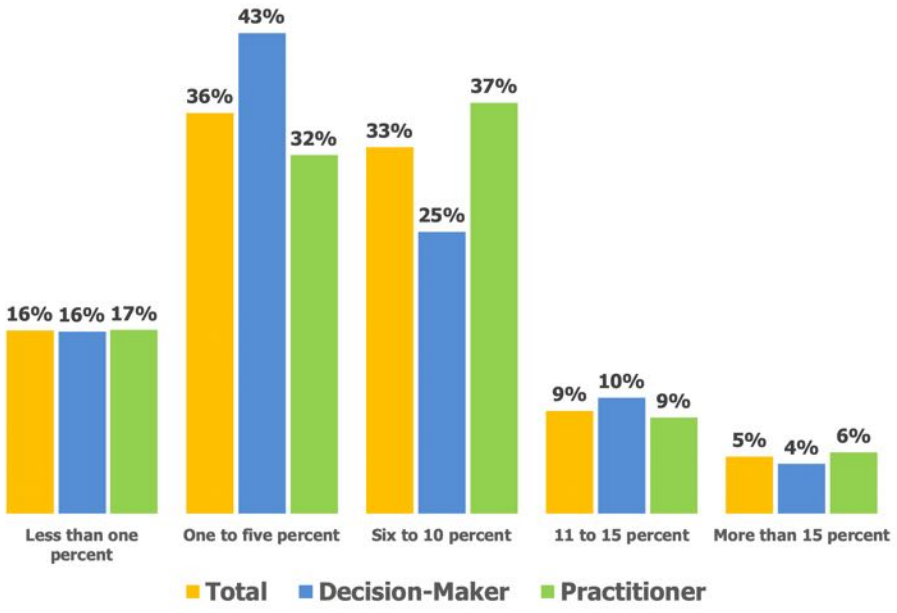


Source: Osterman Research, Inc.

USER CLICK RATES VARY

Among organizations that are using phishing simulation to train their users, the percentage of these simulated phishing emails that are clicked on by users varies widely. As shown in Figure 20, more than one-half of users click on no more than five percent of these emails, while only 14 percent click on more than 10 percent of them. Decision-makers are somewhat more likely to estimate a lower percentage of users who click on simulated phishing emails than do their practitioner counterparts.

Figure 20
Percentage of Simulated Phishing Emails that are Clicked On By Users



Source: Osterman Research, Inc.

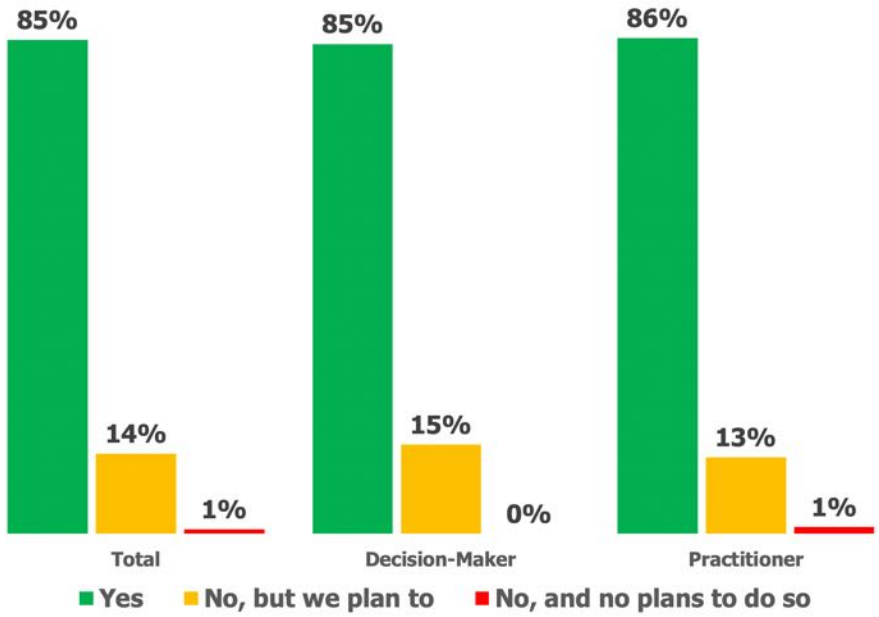
Even with a focus on applied training exercises, some users continue to be tricked.

Despite the use of simulated phishing to train users, our research found that 47 percent of users still click on malicious links, demonstrating that even with a focus on applied training exercises, some users continue to be tricked. There are several explanations for this, including inadequate phishing training, insufficiently frequent training, and/or some users for which training simply does not "take".

REPORTING MECHANISMS ARE VERY COMMON

The vast majority of organizations have provided some sort of method for users to report phishing attempts to their IT and/or security teams, as shown in Figure 21. While 85 percent of organizations provide these reporting mechanisms today, almost all of the remaining organizations that do not enable reporting today plan to do so at some point in the future. We found no statistically relevant difference between decision-makers and practitioners on this question. While 94 percent of US-based organizations reported that they have a mechanism in place to enable users to report phishing attempts, only 76 percent of organizations in the UK reported that they offer this capability.

Figure 21
"Is there a way for users in your organization to report phishing attempts to IT and/or security?"



Source: Osterman Research, Inc.

MANUAL REVIEW IS THE MOST COMMON PRACTICE FOR REPORT PHISHING EMAILS

As shown in Figure 22, most organizations that provide a means for users to report phishing emails to their IT and/or security teams have their security teams manually review all of these user-reported emails. A much smaller percentage of organizations – only 29 percent – use automation to cluster and triage these email phishing incidents. An even smaller proportion of organizations have their security team manually review only some of the reports. We found relatively little difference between decision-makers and practitioners on this question. Assuming that automation is the goal for most organizations, these data points clearly indicate that most organizations have a long way to go to improve their phishing response capabilities.

Most organizations have a long way to go to improve their phishing response capabilities.

Figure 22
What Happens When Users Report a Phishing Email

Incident	Total	Decision-Makers	Pract-itioners
The security team manually reviews all reports	54%	52%	55%
Automation is used to cluster and triage incidents	29%	33%	27%
The security team manually reviews some reports	17%	15%	18%
Nothing really happens	0%	0%	0%

Source: Osterman Research, Inc.

What the data above tells us is that the mechanism for reviewing user-reported phishing emails – **in which more than 70 percent of organizations use only manual processes – is too labor intensive**. If we assume that in an organization of 5,000 email users in which the average user reports only one phishing email per week, the result would be 1,000 emails that would need to be reviewed each week. In many organizations, this level of effort is not unsustainable.

Summary

Mid-sized and large organizations are spending significant amounts of time and effort on dealing with email phishing. However, their current technologies, practices and processes are often not adequate to fully address the problem, resulting in phishing remaining as the primary concern relative to other security issues. Given that the average number of phishing attacks that can be investigated using current processes is low, the data from this survey tells us that the mechanism for reviewing user-reported phishing emails – in which more than 70 percent of organizations use only manual processes – is too labor intensive. If we assume that in an organization of 5,000 email users in which the average user reports only one phishing email per week, the result would be 1,000 emails that would need to be reviewed every week. In many organizations, this level of effort is simply not sustainable.

About IRONSCALES

IRONSCALES is the future of phishing protection, incubated inside the world's top venture program for cybersecurity and founded by alumni of the Israel Defense Forces' elite Intelligence Technology unit. We offer security professionals and end users an AI-driven, self-learning email security platform that provides a comprehensive solution to stop tomorrow's phishing attacks today. Using the world's most decentralized threat protection network, our platform accelerates the prevention, detection and remediation of phishing attacks already inside your email with threat removal times in seconds, not minutes or hours. We give organizations of all sizes complete anti-phishing protection against any type of phishing attack, right now. Visit **www.ironscales.com** to learn more about *The Power of Now*.

REFERENCES

[i] https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

[ii] https://www.darkreading.com/fbi-business-email-compromise-cost-businesses-$17b-in-2019/d/d-id/1337035

[iii] *New Methods for Solving Phishing, Spearphishing and BEC and Other Security Threats*, Osterman Research, Inc.

[iv] https://www.infosecurity-magazine.com/opinions/phishing-time-matters-1-1/

[v] Source: Indeed as of January 17, 2020

[vi] Source: Microsoft

[vii] https://www.infosecurity-magazine.com/news/socs-are-overwhelmed-and-face-deep/

[viii] *Email Security is Ineffective, and Getting Worse: What You Can Do About It*, Aberdeen

[ix] https://resources.infosecinstitute.com/security-awareness-course-design-best-practices/#gref

[x] *New Methods for Solving Phishing, Spearphishing and BEC and Other Security Threats*, Osterman Research, Inc.