WHITE PAPER

Best Practices for Implementing Security Awareness Training

An Osterman Research White Paper

Executive Summary

Fundamentally, security *awareness* training is really more about security *behavior* training: the goal is to provide information to employees that will help them to be more informed about security threats, more skeptical about what they receive in email or through other channels, and less likely to commit damaging behaviors like clicking on malicious links in email, oversharing on social media, or believing requests delivered through electronic channels without first verifying them.

The goal of this white paper was to understand the current state of security awareness training through an in-depth survey of security professionals, and to offer advice about best practices that organizations should consider as they develop a robust training program for their employees.

KEY TAKEAWAYS

- **Security professionals have a number of concerns**
  The survey revealed that there is a wide range of issues about which security professionals are concerned, but the most pressing concerns are focused on data breaches, phishing, spearphishing and ransomware. Interestingly, these are all areas in which good security awareness training can be highly effective at reducing risk.

- **Most organizations have been victimized**
  Sixty-five percent of organizations have been the victim of various types of security threats, most notably phishing attacks that were successful in delivering malware, targeted email attacks and data breaches.

- **Phishing and spearphishing are on the increase**
  More than 90 percent of organizations report that phishing and spearphishing attempts reaching end users over the past 12 months are either increasing or staying at the same levels.

- **Confidence in current security training is low**
  When queried about the perceived effectiveness of their current security awareness training program vs. their current security infrastructure across a wide range of threat types, security professionals consistently expressed more confidence in the latter across a wide range of threat types.

- **Security awareness training is not adequate in most cases**
  The fact that security infrastructure is viewed as a better means of preventing the infiltration of threats than security awareness is not surprising given that training is largely inadequate. We found that four percent of organizations never provide security awareness training for their users, and for those that do it is often infrequent and inadequate.

- **Senior business managers, users are not enthusiastic about training**
  We discovered that while senior IT is supportive and enthusiastic about security awareness training, senior business managers and employees are decidedly less so.

There is a wide range of issues about which security professionals are concerned.

ABOUT THE WHITE PAPER AND SURVEY

This white paper was sponsored by KnowBe4; information about the company is provided at the end of this white paper.

The survey for this white paper was conducted with 134 members of the Osterman Research survey panel during August 2018. The mean size of the organizations surveyed was 17,523 employees. In order to qualify for the survey, respondents had to play a role in computer/cybersecurity issues and security-related decision-making for their organizations.

What Concerns Security Professionals Most?

Security professionals are concerned about a wide range of issues in the context of their organizations' security posture. As shown in Figure 1, topping the list are breaches of sensitive or confidential data, phishing attacks and spearphishing/CEO Fraud attacks, all cited as issues of "major" concern by two-thirds of those surveyed. Also, of major concern by most security professionals are issues like ransomware attacks, cited by more than three in five of those in the security field.

Figure 1
Issues About Which Security Organizations are Concerned
Concerns rated on a scale of 1 (not at all concerned) to 7 (extremely concerned)

Concern	Minimal Concern (1-2)	Moderate Concern (3-5)	Major Concern (6-7)
A breach of sensitive/confidential data	2%	30%	68%
Phishing attacks	1%	31%	68%
Spearphishing/CEO Fraud attacks	1%	32%	68%
Ransomware attacks	0%	38%	62%
Targeted attacks/zero-day exploits	0%	45%	55%
Malware infiltration through HTTPS/SSL web traffic	3%	47%	50%
Endpoints compromised by botnets	4%	53%	43%
Account takeover attacks	4%	55%	42%
"Shadow IT" - employees using unauthorized cloud apps and services	5%	59%	36%
Malvertising	6%	65%	29%
Cryptocurrency mining malware being installed on your internal PCs or servers	13%	60%	27%
Drive-by attacks	7%	67%	26%
Use of CPU by cryptocurrency miners when users visit websites	14%	65%	22%
Employees surfing web sites that violate corporate policies (e.g., porn sites)	19%	62%	19%

Source: Osterman Research, Inc.

The four leading security concerns shown...are also areas in which security awareness training can yield significant benefits.

Clearly, all of these security concerns are issues for which most organizations have deployed various technology-based solutions on-premises and in the cloud, such as firewalls and next-generation firewalls, intrusion detection systems, anti-malware solutions, anti-spam solutions, web application firewalls, secure web gateways and the like. Interestingly, however, the four leading security concerns shown in the table are also areas in which security awareness training can yield significant benefits by sensitizing users to best practices for their use of email and other communication and collaboration channels.

SECURITY PROFESSIONALS ARE RIGHT TO BE CONCERNED

Those who manage security for their organizations are right to be concerned about security threats. As shown in Figures 2 and 3, the vast majority of organizations have been infected with various types of exploits and attacks, including phishing attacks that successfully infiltrated corporate defenses and infected the network with malware, targeted email attacks that were launched from compromised accounts, data breaches through email and a host of other issues. The table reveals that nearly two-thirds of those surveyed suffered through some type of compromise or successful attack for the period ended March 2018.

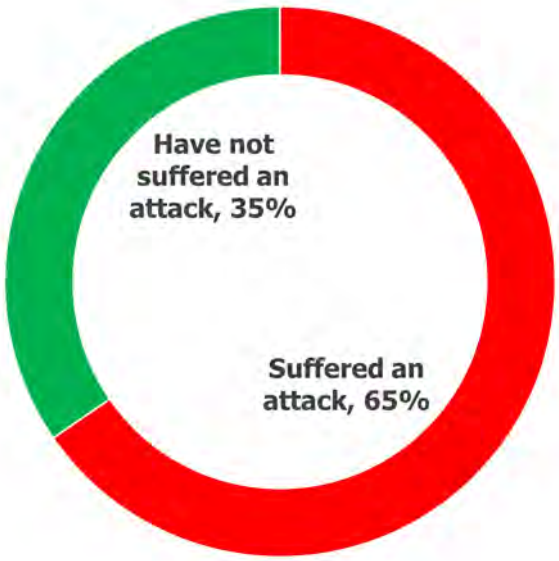
Figure 2
Percentage of Organizations That Have Been the Victim of Specific Security Incident During the Period March 2017 to March 2018

Incident	% of Orgs
A phishing attack was successful in infecting systems on our network with malware	27.9%
A targeted email attack launched from a compromised account successfully infected an endpoint with malware	25.0%
Sensitive / confidential info was accidentally leaked through email	25.0%
A targeted email attack launched from a compromised account successfully stole a user's account credentials	23.1%
One or more of our endpoints had files encrypted because of a successful ransomware attack	22.1%
Malware has infiltrated our internal systems, but we are uncertain through which channel	21.2%
One or more of our systems were successfully infiltrated through a drive-by malware attack from employee web surfing	19.2%
An email as part of a CEO Fraud/BEC attack successfully tricked one or more senior executives in our organization	17.3%
A fileless/malwareless attack reached an endpoint	17.3%
An account takeover-based email attack was successful	15.4%
Sensitive / confidential info was accidentally or maliciously leaked through a cloud-based tool like Dropbox	8.7%
A targeted email attack was successful in infecting one or more of our senior executives' systems with malware	7.7%
Sensitive / confidential info was accidentally or maliciously leaked through a social media / cloud application	5.8%
Sensitive / confidential info was accidentally or maliciously leaked, but how it happened is uncertain	5.8%
Sensitive / confidential info was maliciously leaked through email	4.8%
None of the above	34.6%

Source: Osterman Research, Inc.

Nearly two-thirds of those surveyed suffered through some type of compromise or successful attack for the period ended March 2018.

Figure 3
Percentage of Organizations That Have Been the Victim of at Least One Security Incident During the Period March 2017 to March 2018



Source: Osterman Research, Inc.

Many security professionals are likely unaware that their organization has been breached.

It's important to note that while about 35 percent of those surveyed reported that none of the attacks shown in the table actually occurred in their organizations, this number is likely a conservative estimate and the situation is probably worse than what was reported. There are two reasons for this:

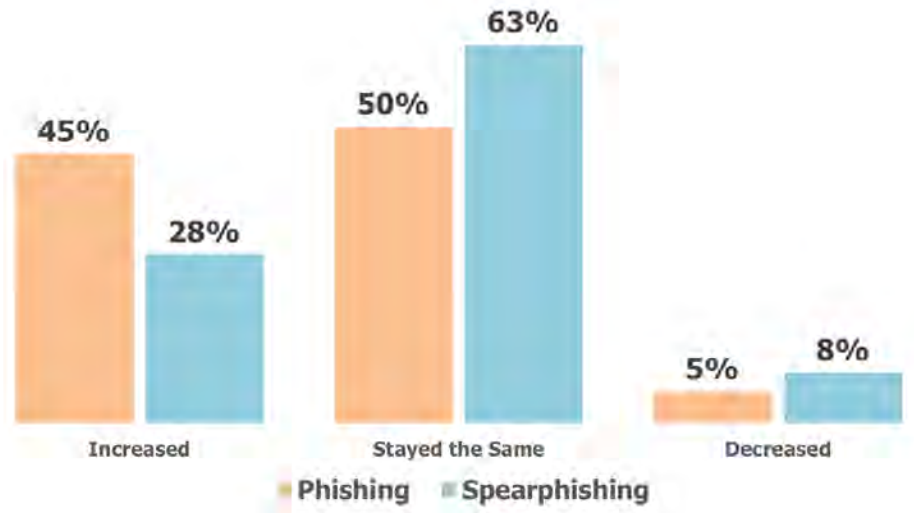
- Some security professionals will naturally be reticent about revealing each and every attack that has occurred within their organization. While our survey panel provides very reliable results and has proven to be quite candid, there are always a few individuals who might be reluctant to air every bit of their organizations' "dirty laundry" for public consumption.

- Many security professionals are likely unaware that their organization has been breached. Given that most cybercriminals going after high-value targets work hard to operate as stealthily as possible, the average global "dwell time" for cyberthreats has lengthened to 229 days according to a Ponemon Institute study published in 2017. What this means is that the typical organization that has been breached will be unaware of the incursion for nearly eight months before discovering and beginning the process of remediating the threat.

THREATS ARE INCREASING FOR MANY

Our research also discovered that for a significant proportion of the organizations surveyed, both phishing and spearphishing emails that actually reach end users have increased over the past 12 months. As shown in Figure 4, 45 percent of organizations reported that phishing emails that bypass existing security defenses and reach end users have increased over the past year, while only five percent reported a decrease. Similarly, 28 percent reported an increase in spearphishing emails over the past year with only eight percent reporting a decrease. Among those reporting an increase in phishing and spearphishing emails reaching end users over the past year, the average increases were 33 percent and 49 percent, respectively.

Figure 4
Changes in Phishing and Spearphishing Emails Reaching End Users Over the Past 12 Months



Source: Osterman Research, Inc.

The implications of these findings are significant because it means that despite the significant amounts that organizations spend on anti-phishing and anti-spearphishing technologies for their email systems, the volume of these threats is continuing to grow. Moreover, these findings suggest that technology-based solutions focused on detecting and filtering out phishing and spearphishing threats are having almost no impact on the volume of these attacks that actually reach end users.

To be fair, it's important to note that there are two significant issues that are creating an almost untenable situation for vendors of technology-based solutions in the context of detecting and filtering out phishing and spearphishing threats:

- Security awareness training is lacking in many organizations, making the security infrastructure dependent almost exclusively on technology – not users – to ensure that phishing and spearphishing attempts are detected and acted upon before a user clicks on them. While training by itself won't stop such as attempt from reaching an end user, it will go a long way toward rendering the attack moot.

- Many users overshare information on social media and in other venues. This provides useful fodder for cybercriminals, particularly those who are focused on spearphishing attempts. For example, someone who extensively shares details about their business travel, restaurants they have recently visited, their vacations and other personal information provides information that will be useful for cybercriminals in crafting emails that appear to be timely and believable.

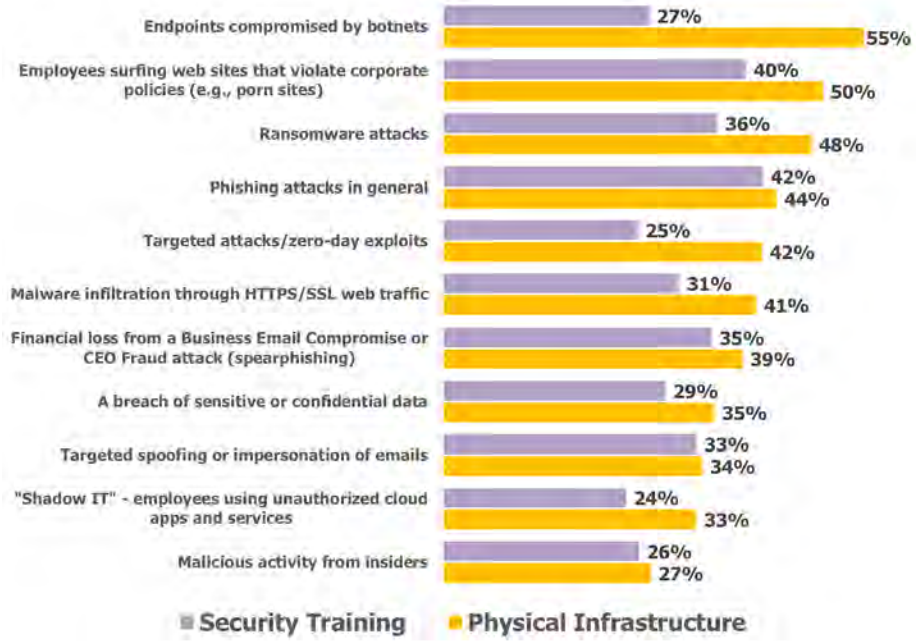
Many security professionals are likely unaware that their organization has been breached.

Security Training vs. Infrastructure

One of the key issues we investigated in the research conducted for this white paper was security professionals' perceptions about the effectiveness of their current physical security infrastructure compared to their current level of security awareness training. Not surprisingly, given that security awareness training is not at the level it should be, as discussed later in this white paper, it fell short relative to the physical security infrastructure in every area, as shown in Figure 5. For example, while 55 percent of the security professionals surveyed believe that their physical infrastructure is protecting the organization from endpoints that are compromised by

botnets "well" or "very well", only 27 percent believe that their security awareness training is providing this level of protection. Similarly, while 48 percent of those surveyed believe that their physical infrastructure is protecting against ransomware attacks "well" or "very well", only 36 percent perceive this level of effectiveness for the training that end users receive.

Figure 5
Perceptions About the Effectiveness of Security Training vs. Infrastructure
Percentage Responding Protecting "Well" or "Extremely Well"



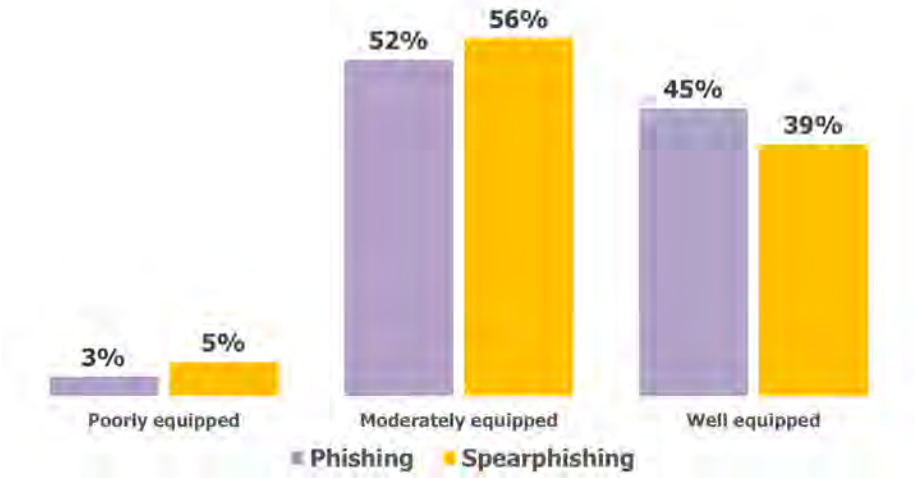
Source: Osterman Research, Inc.

Many users overshare information on social media and in other venues.

MOST USERS ARE NOT ADEQUATELY EQUIPPED TO DEAL WITH PHISHING AND SPEARPHISHING

Another issue about which we queried security professionals in the survey was their perception about how adequate their end users are in detecting phishing and spearphishing emails. As shown in Figure 6, only 45 percent of security professionals believe their users are well-equipped to recognize phishing attempts and only 39 percent are believed to be well-equipped to recognize spearphishing. While the majority of users are perceived to be moderately well-equipped to deal with these threats, a small proportion of users are poorly equipped.

Figure 6
Perceptions About Users' Ability to Recognize Phishing and Spearphishing Emails



Source: Osterman Research, Inc.

Here again, the relatively low proportion of users that are well equipped to recognize phishing and spearphishing attempting points primarily to the inadequate level of security awareness training that we discovered in our research.

CONFIDENCE IN END USERS IS LACKING

As shown in Figure 7, security professionals lack confidence in their end users' ability to deal with phishing and spearphishing, and also in the level of training that they receive on these two threats. For example, on a scale of 0 (not confident at all) to 100 (very confident), security professionals gave employees in their company a rather mediocre confidence rating of 64 when asked if these employees were well-trained to deal with phishing. Security professionals gave the same confidence score when asked about senior executives' likelihood of clicking on a spearphishing link, but have even less confidence when asked about employees clicking on phishing links.

Interestingly, security professionals have little confidence in the inherent ability of end users to deal with phishing if they are untrained. However, as the top bar in the figure shows, even with training – which, as discussed later in this white paper, is fairly inadequate – confidence doesn't really improve all that much.

Only 45 percent of security professionals believe their users are well-equipped to recognize phishing attempts.

Figure 7
Confidence in Users' Ability with Regard to Phishing and Spearphishing
Rated on a Scale of 1 (Not Confident at All) to 100 (Very Confident)

Source: Osterman Research, Inc.

Approaches to Security Awareness Training

There are number of approaches to security awareness training that are practiced by organizations and managed by security teams. In this section we discuss some of the key issues we discovered in the context of how well organizations are managing their security awareness training programs.

SEVERAL APPROACHES ARE USED

There are five basic approaches taken to provide security awareness training for corporate employees:

- **The Break Room Approach**
  Employees are gathered for a lunch or special meeting and told what to avoid when surfing the web, when receiving emails from unknown sources, etc.

- **The Monthly Security Video Approach**
  Employees view short security awareness training videos to learn how to keep the network and organization safe and secure.

- **The Phishing Test Approach**
  Certain employees are pre-selected, sent a simulated phishing attack, and then security staff determine if they fall prey to the phishing attack.

- **The Human Firewall Approach**
  Everyone in the organization is tested, the percentage of employees who are prone to phishing attacks is determined, and then everyone is trained on major attack vectors, sending simulated phishing attacks on a regular basis.

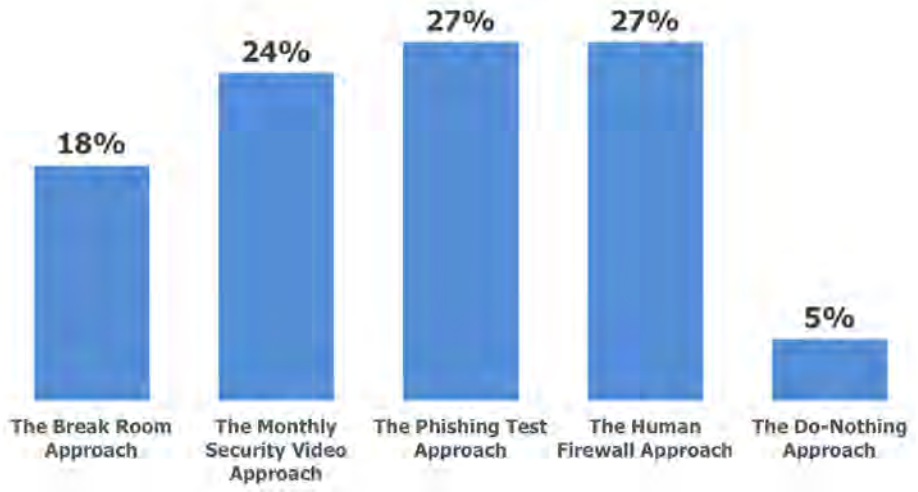
- **The Do-Nothing Approach**
  Organizations don't do security awareness training.

As shown in Figure 8, the most common approaches are the Phishing Test and Human Firewall, followed closely by the Monthly Security Video approach. We found that one in 20 organizations do no security awareness training. It's important to note, however, that these represent the *primary* approach to security awareness training in the organizations we surveyed, but each is not the only approach that can or should be used. For example, an organization may provide short videos for employees to

There are five basic approaches taken to provide security awareness training for corporate employees.

watch and then test them through phishing attempts, while offering a quarterly lunch meeting on the topic of newly discovered cyberthreats.

Figure 8
Approaches Taken to Security Awareness Training



Source: Osterman Research, Inc.

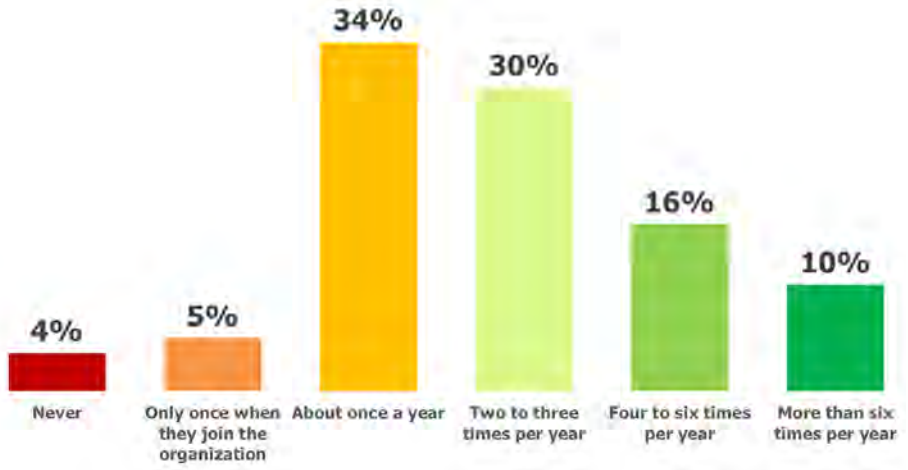
It is important to note that what seems like a discrepancy in the figure above and the one below – 24 percent use the "Monthly Security Video Approach", but only 10 percent train users more than six times per year, as shown in Figure 9 – is really not a discrepancy. The data in Figure 8 show the basic, overall approach that an organization might have adopted, but that does not mean that all employees, or even the entire organization, follows it religiously.

SECURITY AWARENESS IS USUALLY NOT FREQUENT

One of the key issues that helps to determine the effectiveness of security awareness training is the frequency with which it is offered. As shown in Figure 9, training is infrequent for a large proportion of organizations, if it exists at all. For example, one in 25 employees never receives security awareness training, another five percent receive it only when they join the organization, and a plurality – fully one-third of employees – receive it only about once each year. Even most of those who do receive security awareness training more than once per year go through this training fairly infrequently.

One of the key issues that helps to determine the effectiveness of security awareness training is the frequency with which it is offered.

Figure 9
Frequency with Which Security Awareness Training is Conducted



Source: Osterman Research, Inc.

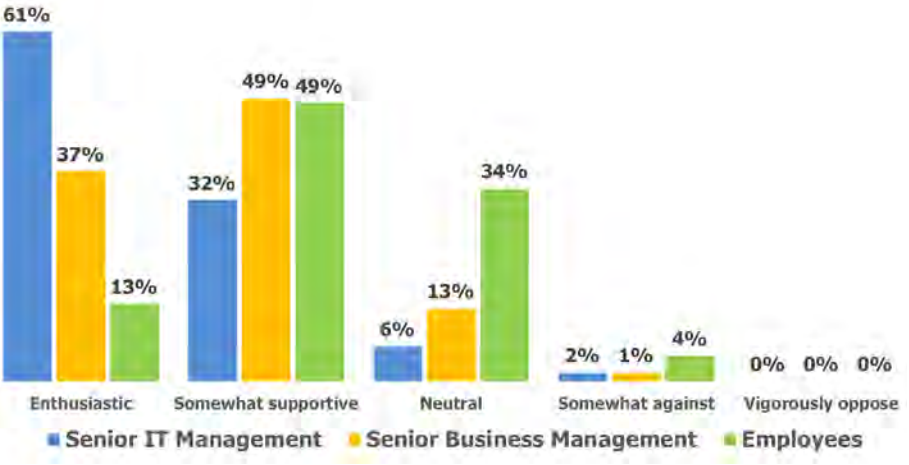
IT MANAGERS ARE ENTHUSIASTIC ABOUT SECURITY AWARENESS TRAINING – OTHERS, NOT SO MUCH

Senior IT management are enthusiastic about security awareness training – more than three in five organizations report that those who oversee IT are sold on the idea of training their employees about security; another 32 percent are at least somewhat supportive of the idea. The result is that more than nine in 10 senior IT managers support or strongly support the idea that security awareness training should be part of their organizations' employees' training regimen.

However, as shown in Figure 10, enthusiasm drops off substantially among senior business managers; and it drops off even more for employees who are the primary focus of security awareness training.

Senior IT management are enthu-siastic about security awareness training.

Figure 10
Various Groups' Views on Security Awareness Training



Source: Osterman Research, Inc.

WHY THE LACK OF ENTHUSIASM?

It's not surprising that senior IT management are overwhelmingly enthusiastic about security awareness training: by making users more aware of phishing, spearphishing and the growing number of other threats that can impact an organization (and, hopefully, changing user behavior in the process), they reduce the number of threats that they must detect and remediate.

It's also not surprising that senior business managers are less enthusiastic about security awareness training, since many likely view this as a time sink that takes away from employees' productivity. Of course, by eliminating security threats users will be more productive by becoming less vulnerable to phishing attempts that can install ransomware and other types of malware, or that might steal corporate data or finances.

Interestingly, employees are the least enthusiastic of the groups surveyed about security awareness training – here too, that result is not all that surprising. While none of the groups about which we surveyed "vigorously oppose" security awareness training, 38 percent of employees are either neutral or somewhat opposed to the training they receive, while only one in eight are enthusiastic. Reasons for this lack of support for training can include:

- Poorly written and irrelevant training curricula
- Lack of incentives for participating in security awareness training programs
- A failure to show a link between good training and reduced infections
- Training that is dry and boring
- Making training lengthy and infrequent instead of short and frequent
- Multiple topics covered per session instead of one topic per session
- Lack of gamification, or otherwise making the training fun
- A lack of reward for changed security behaviors

Best Practice Guidance

So, what are some best practices to consider in developing a security awareness training program that will actually change behavior and make the organization less likely to fall prey to a cyberattack? Here are some suggestions on processes and practices to consider.

SECURITY MUST BE A BOARD-LEVEL ISSUE

Security – and, by extension, security awareness training – must be a board-level issue in order for it to get the attention it deserves. In a growing number of organizations, security is getting much more attention from boards of directors. CISOs and similar, director-level positions are joining boards of directors to keep members apprised of security issues and corporate risks of non-compliance. A board of directors that takes security seriously and gives it the priority it deserves will go a long way toward bolstering the security training program in an organization.

Security – and, by extension, security awareness training – must be a board-level issue in order for it to get the attention it deserves.

UNDERSTAND YOUR CORPORATE CULTURE

It's important to understand that not all corporate cultures are equally conducive to the notion of security awareness training. Some organizations' management, particularly those outside of IT, is not open to the idea of security awareness training and so won't support or fund it to the extent they should. As a corollary to the notion that boards should be focused on security, so should senior management so that training will be supported and will be given the opportunity to flourish. In short, gaining management buy-in to fund and encourage security awareness training will be essential to fostering not only good security training programs, but also creating a corporate culture in which security is valued.

An essential element of ensuring that corporate culture will support security awareness training and good security practices is determining if corporate managers

are open to the idea of being challenged. For example, if a CEO requires that his orders be carried out without question, then the CFO who receives a spearphishing email, purportedly from the CEO, demanding that a wire transfer be made to a company supplier will probably be afraid to question that demand. A healthy corporate culture that supports a healthy security culture won't enable that kind of fear.

ENSURE THAT TRAINING COVERS ALL THE BASES

Of course, security awareness training should start with the low-hanging fruit focused on the most common threats, such as mass-emailed phishing attempts that purport to be from employees' banks or from the corporate email administrator. However, security awareness training should also focus on less common threat vectors, such as spearphishing aimed at senior executives and oversharing on social media that can divulge sensitive corporate information. With regard to the latter, oversharing information on social media about family members, personal history, favorite restaurants, business travel and the like can make it easier for cybercriminals to guess passwords or craft messaging that will enable them to hack into corporate email and other accounts.

MAKE SURE THAT PHISHING TESTS ARE RANDOM

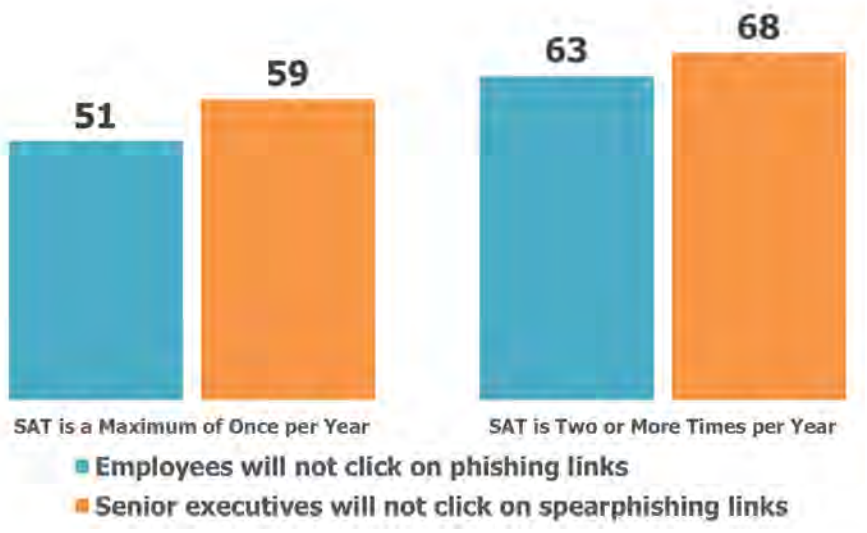
It is essential to make sure that phishing and other security awareness training tests are truly random. An employee-testing program that conducts testing on a regularly defined schedule will be more easily identified by employees as a phishing test and will elicit behaviors that are not representative of the actual threats that employees might receive.

TRAINING SHOULD BE SUFFICIENTLY FREQUENT

As noted earlier, training within a large proportion of organizations – if it is conducted at all – is infrequent. Training users once per year or only when they join the company is simply not adequate to convey information about critical security issues that is designed to alter users' behavior. Moreover, the survey data suggests there is a relationship between the frequency of training and security professionals' confidence in their users' abilities. As shown in Figure 11, security professionals in organizations with infrequent security awareness training have less confidence in their users' abilities than those in organizations with more frequent training.

Training within a large proportion of organizations – if it is conducted at all – is infrequent.

Figure 11
Relationship Between Frequency of Training and Confidence in User Behavior



Source: Osterman Research, Inc.

"RIGHTSIZE" TRAINING FOR SPECIFIC GROUPS

While all employees are potential victims of cybercrime and can serve as a conduit for bad actors to infiltrate an organization, some users are higher value targets than others. For example, a company's CFO is more likely to be the target of a coordinated and focused spearphishing campaign than someone who does not have access to corporate financial accounts. Consequently, it makes sense to consider providing additional security awareness training for some individuals. The research conducted for this white paper found that IT, senior executives and finance were the three most likely groups to receive enhanced training.

CREATE A GOOD BEFORE AND AFTER PICTURE

Before implementing a security awareness training program, it's useful for decision makers to establish a baseline so that the level of awareness is understood before training commences. Creation of this "before" picture is an essential element of understanding how effective training has been over time.

LINK TRAINING WITH TESTING

It's important to link security awareness training with testing on key issues like phishing detection. For example, an employee who fails a phishing test should be given additional, context-sensitive training with an eye to addressing the deficiencies that were uncovered in the test.

CREATE COMMUNICATIONS BACKCHANNELS

It's important for all employees to have an appropriate backchannel for checking on questionable requests received through email. For example, a CFO who receives a request from the CEO to make a wire transfer, particularly under unusual circumstances, should have a method for verifying that request independently of the channel that was used to make the request.

FOCUS ON BEHAVIORIAL CHANGE

As noted earlier, security awareness training is really about behavior modification: helping users to be more skeptical and less gullible about cybercriminals' attempts to fool them, less likely to share information that could be used by cybercriminals to create customized messages, being more careful about opening attachments, verifying senders of emails, and so forth. The goal of security awareness training must ultimately be about improving the behavior of employees who have the potential of undermining the security provided by the organization's security infrastructure.

Security awareness training is really about behavior modification: helping users to be more skeptical and less gullible.

MAKE TRAINING FUN

Security awareness training that isn't fun, or at least enjoyable, for employees will be resisted and, ultimately, ineffective. While gamification of the training process is not and absolute requirement for a security awareness training program, it should be interesting and engaging enough to keep users interested and willing to participate with the goals of the program.

DON'T PUNISH MISTAKES

One of the essential best practices that any organization should follow as part of any security awareness training program is not to punish mistakes that users make, whether mistakes made during testing or clicking on actual malicious content. If employees are not free to make mistakes and share their experience openly with security teams and their peers, they won't participate in the process. Of course, an employee who continues to click on malicious links and never improves their behavior may require more attention, but punishment – if meted out at all – should be a last resort.