White Paper
Osterman Research
Sponsored by Mimecast

mimecast

White Paper

The Truth About Cybersecurity Training

Stop ticking boxes. Start delivering real change.

Executive Summary

The goal of any corporate security infrastructure is to protect corporate data, access to on-premises and cloud-based systems, various types of sensitive information like login credentials and customer data, and even the physical assets used to manage networks and endpoints.

The conventional method of accomplishing the objective of securing these assets has been the deployment of various types of security hardware, software and cloud services, including firewalls, endpoint detection and response solutions, anti-virus software, secure email gateways, web application firewalls, and a host of other solutions. Underscoring just how important this approach has been is the fact that at least 2,336 vendors of these types of solutions currently operate worldwide, with new entrants joining the market continually.

78% believe that both technology and training in combination are equally effective in minimizing our cybersecurity risk.

However, cybersecurity technology can go only so far in protecting an organization. Because bad actors increasingly target users of corporate systems and services, these users must be adequately equipped to deal with a growing variety of threats directed at them, sometimes specifically at their role within the organization. Consequently, good security awareness training is essential in protecting the organization from security threats and the damage they can cause. But the goal of security awareness training should be the development of fundamental change in users – change in the way they think about security – that will translate into the development of a robust security culture.

About this white paper: Two surveys were conducted for this white paper: one survey was conducted with individuals who manage, contribute to or influence their organization's security awareness training program, while a second survey was conducted with 1,000 employees in the United States.

Key Takeaways

Here are the key takeaways presented in this paper:

1. Decision makers are concerned about a wide variety of security issues, most of which are focused on email delivery as a threat vector.

2. Security awareness training is perceived to be as important as technology in dealing with security threats and organizations will be devoting more focus and attention to their employee training programs over the next year.

3. As users receive more security awareness training, their ability to effectively deal with security threats increases. The "before-and-after" picture is impressive: users who are properly trained are much more likely to be able to spot phishing attempts and email compromise than their untrained colleagues.

4. Users who find security awareness training interesting and engaging derive significantly more benefit from the training than users who find it to be boring or uninteresting.

5. Similarly, employees who find cybersecurity training more interesting consider themselves as playing a more important role in the security of their organizations.

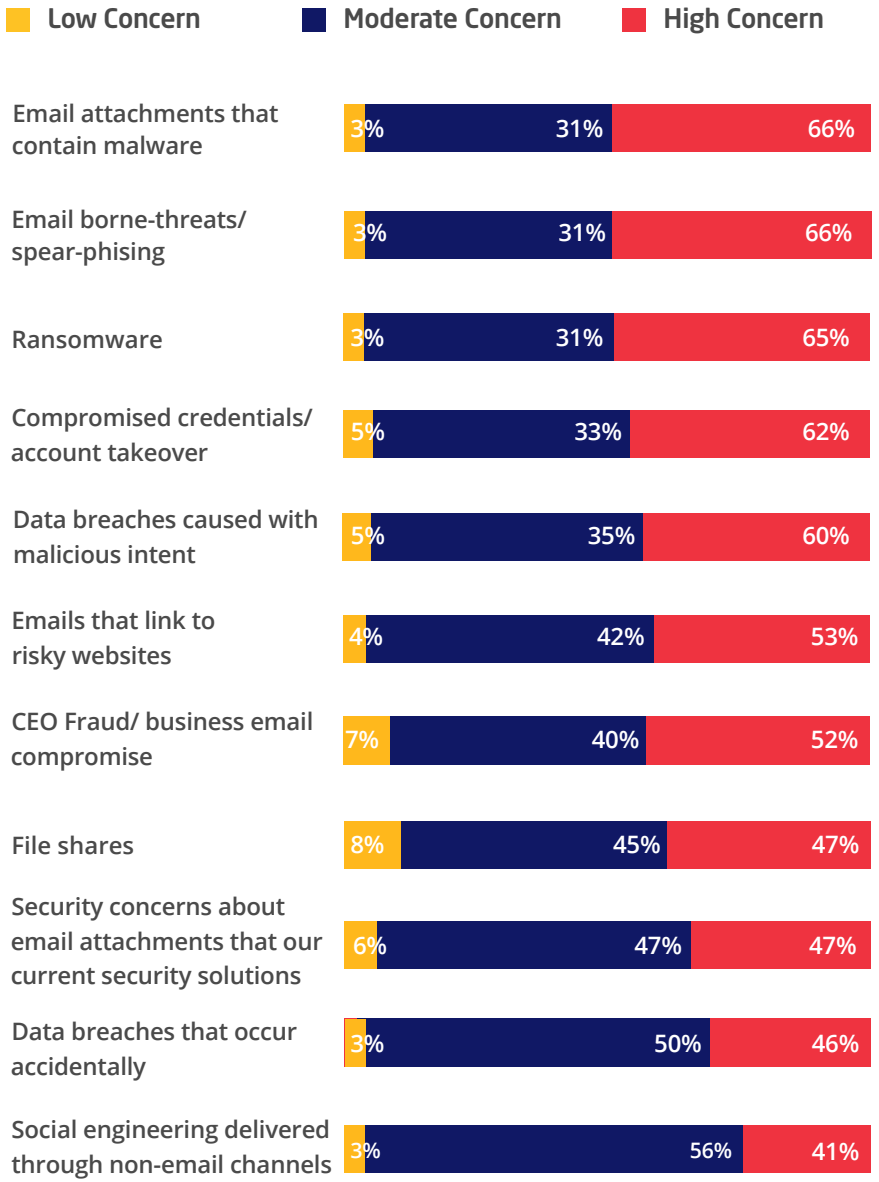
6. Senior IT and business management are much more enthusiastic about security awareness training than non-management employees. Similarly, security and IT leaders, their staff members, and business leaders are largely on-board with the idea that developing a strong cybersecurity culture is important; other employees are much less convinced about the importance of doing so, indicating that the goal of developing a robust security culture has not yet been achieved in most organizations.

What are Decision Makers Most Concerned About?

Not surprisingly, decision makers and influencers in IT and security departments express serious concerns about a wide range of cyberthreats and other types of cybersecurity issues. As shown in Figure 1, the leading concerns are focused on threats that are most often delivered through email, such as malware, spear-phishing and ransomware. Because email is the primary communication, collaboration and content-sharing tool in most organizations – and will remain so for many years – email-related threats will continue to be a critical security concern for the indefinite future.

What's particularly interesting about the data in the figure above is that despite the hundreds of billions that have been spent on technology-focused solutions to address comparatively simply problems over a period of many years, such as detecting malware in an email, it remains an issue of significant concern to two-thirds of security decision makers and influencers.

Figure 1: Leading cybersecurity concerns



The problem may actually get worse with the growing adoption of Office/Microsoft 365, which is now the dominant business email platform worldwide. For example, an SE Labs test in 2020 found that the total accuracy rating for Microsoft Office 365 Advanced Threat Protection was just 28 percent, despite the fact that security solutions in the same test achieved an accuracy rating of 94 percent. **Osterman Research has found that a growing proportion of decision makers are opting for the "full meal deal" from Microsoft, rolling out the top-level Office/Microsoft 365 plan (Plan E5, as of this writing) to their users instead of deploying third-party security that offers better performance.**

28% total accuracy for Microsoft 365 Advanced Threat Protection

94% total accuracy for other security solutions in the same test

Lockdowns are raising a concern

The COVID-19 pandemic and the associated lockdowns, stay-at-home orders, shelter-in-place orders, and the like that rapidly converted an in-office workforce to one working from home has increased concerns about security. For example, as shown in Figure 2, 46 percent of decision makers and influencers are "concerned" or "extremely concerned" about hackers exploiting the new work-from-home workforce, which numerous analyses from multiple vendors have determined has already happened.

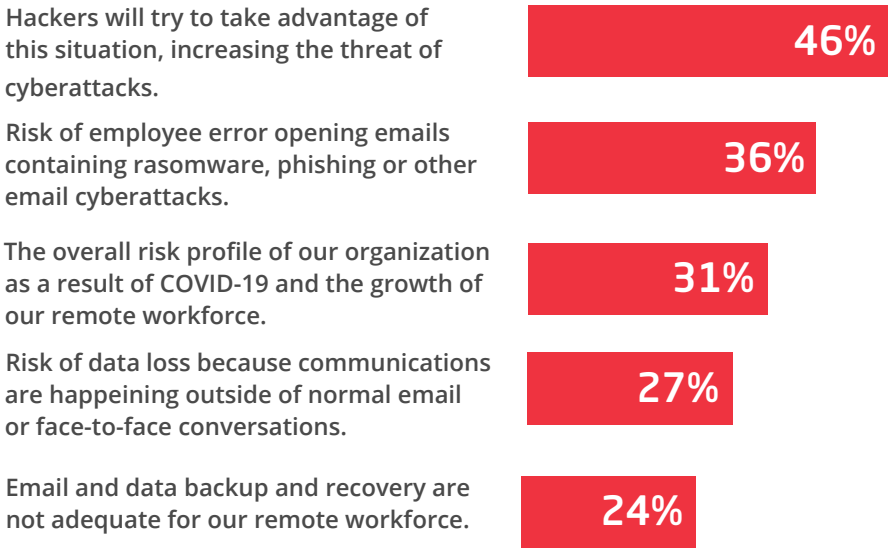
Osterman Research anticipates that these problems will get worse before they get better, even as (and because) more workers are returning to an office environment, bringing their potentially compromised laptops, USB sticks and mobile devices back to corporate networks.

46%

of decision makers are 'concerned' or 'extremely concerned' about hackers exploiting the new work-from-home workforce

Figure 2: Concerns about various issues

Percentage responding "concerned" or "extremely concerned"



mimecast

Increased use of email is complicating the problem

As noted above, email is the primary threat vector in most organizations. Complicating the security problem is that IT and security decision makers and influencers anticipated that use of email for key processes would increase during the pandemic. As shown in Figure 3, 95 percent believed that use of email for conventional communications would either increase or remain the same during the crisis, while only five percent believed that email communications would decrease. Forty-four percent believed that use of email for sending files and documents would increase and nearly as many believed that the same level of demand for these services would be required.

This makes it clear that email will remain a mainstay of corporate communications during the pandemic, and that in order for employees to remain productive, corporate email systems will need to be operate at a very high level – and certainly no less securely than they do under normal circumstances.

64%

believe that during this crisis email communication will increase

Figure 3: Anticipated changes in use of email during the COVID-19 crisis compared to before the crisis

	More	Same	Less
Email communications	64%	31%	5%
Sending files/documents	44%	42%	13%
Sending contracts/approvals	30%	45%	25%
Sales activity/contact customers, prospects	35%	35%	35%

mimecast

Security and compliance are suffering

Both security and compliance have suffered during the current work-from-home environment. For example, while 64 percent of organizations agree with the notion that they were doing an excellent at job maintaining compliance with their various obligations before the COVID-19 crisis, that level of agreement fell to just 56 percent shortly after the lockdowns began. Similarly, while 56 percent agreed that they were doing an excellent job at blocking security threats prior to the lockdowns, that dropped to just 49 percent. **Even under normal circumstances figures for doing an "excellent" job at compliance and security should not be this low, but the lockdowns have clearly had an impact on organizations' ability to deal effectively with both.**

Before the crisis

64%

We were doing an excellent job at **maintaining compliance** with our various compliance obligations.

56%

We were doing an excellent job at **blocking security threats** from impacting our organization.

During the crisis

56%

We were doing an excellent job at **maintaining compliance** with our various compliance obligations.

49%

We are doing an excellent job at **blocking security threats** from impacting our organization.

Changing the IT Security Culture

This section discusses the results of the survey of those who contribute to or influence their organization's security awareness training program – what we refer to in this paper as "IT/security decision makers and influencers." The following section discusses the results of the survey with end users.

The progression of security awareness training

Security awareness training should have as its goal moving users from a state of ignorance, where they are largely or completely unaware of threats like phishing attempts or how to exercise basic, "safe" behaviors; to "systemic" change, where security becomes so ingrained in the way they use email and other tools that good security practices become second nature to them, as shown in Figure 4. **In short, the end result of good security training should be the development of a user mindset akin to "muscle memory," where good security practices become almost second nature.**

A good security awareness training program should focus not on just changing users' behavior, as useful as that is, but rather creating the sort of systemic change in users that they will almost instinctively understand how to use any sort of communication tool, deal with any kind of content, know when and when not to open attachments or click on links in an email, know how they can validate requests, and so forth.

Figure 4: Security awareness training progression

Training is perceived to be as important as technology, if not more so

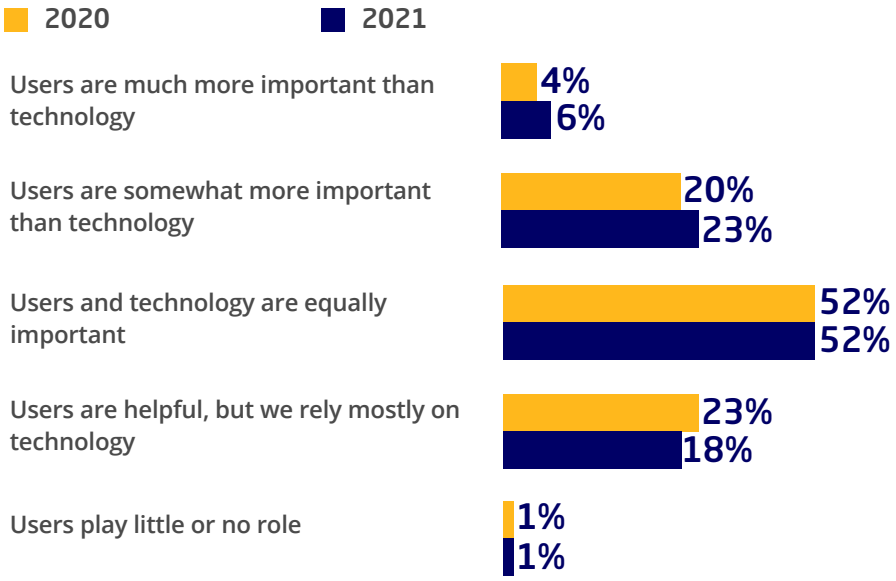
As shown in Figure 5, **nearly four in five IT/Security decision makers and influencers consider the combination of technology and training to be equally important in dealing with security threats.** However, when analyzing the results from those who believe that training or technology is more effective in dealing with these threats, the former gets the nod. Over the next 12 months, both training and technology are expected to increase in their perceived importance, although a slightly larger proportion of those in IT and security will place more emphasis on training.

As a good security awareness training program should focus not on just changing users' behavior but also creating systematic change.

Figure 5: Importance of training vs. technology

Percentage responding "agree" or "strongly agree"

Figure 6: Views of IT and Security leadership on roles of users vs. technology

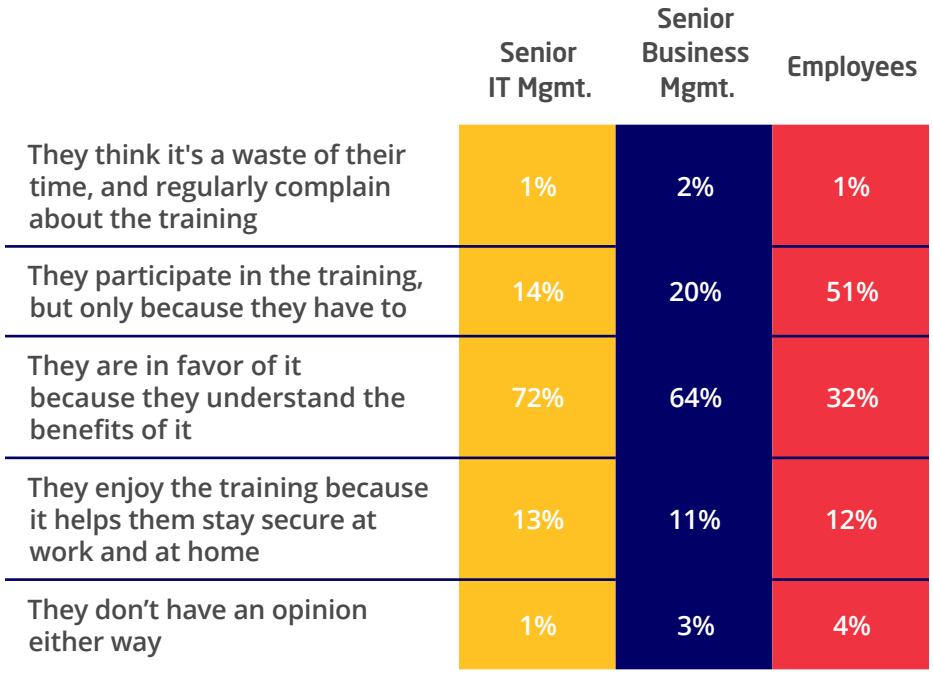


IT is more enthusiastic about training than rank-and-file employees

One of the goals of security awareness training is to get employees and contractors on-board with at least the notion that training is useful in helping them to protect corporate data and systems. Ideally, however, the goal should be to move employees from changing their behavior, the fourth step noted in Figure 4, to true systemic change – a change that results in employees not only changing their behavior but changing their entire mindset so that they want to practice safe computing for personal, as well as professional, reasons.

Figure 7 shows that most organizations are nowhere near approaching that reality today. While the vast majority of senior IT and business management are on board with security awareness training, favoring it because they understand its benefits, most are still not at the point where they have become fundamentally changed as a result of it. However, for non-senior employees, systemic change is still further down the road, **with only about one-half of employees participating in their training not because they understand its benefits, but because they are forced to do so**.

Figure 7: Views among different consumer groups on the effectiveness of training



Over the next 12 months, the role of users will increase in importance as defense to threats relative to technology.

mimecast

What's the best format to deliver training?

One of the reasons that employees, to a much greater extent than senior IT or business management, should consider security awareness training to be more compulsory than beneficial may be the quality of the training that they're receiving. As shown in Figure 8, nearly one-half of IT/security decision makers and influencers believe that information-based training with actionable advice is the most effective and engaging type of training for their employees. The second most popular type of training is considered to be entertaining, although not necessarily humorous, content.

However, our research found that among organizations that survey their employees about the security awareness training that they receive, the results are not stellar. For example, only 50 percent of those surveyed like or strongly like the quality of the writing in their training materials or presentations, only 41 percent feel this way about the level of interactivity in the training, and only 37 percent agree or strongly agree that they enjoy their training overall. It's clear from these results that the quality and enjoyment of training has some way to go.

only

50%

of those surveyed like or strongly like the quality of the writing in their training materials or presentations

Figure 8: Training approach determined by employees to be most effective and engaging the crisis

The importance of developing a strong security culture varies widely

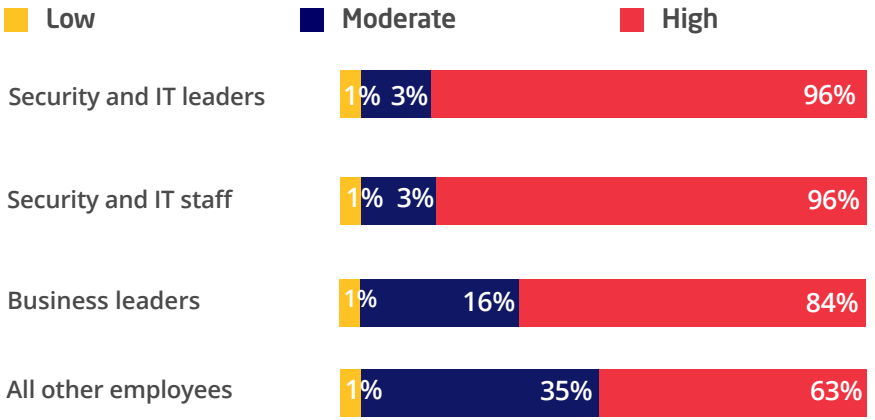
Is developing a strong security culture important? It depends on who you talk to. As shown in Figure 9, 24 out of 25 security IT leaders, as well as the staff members who report to them, consider the development of such a culture to be either "important" or "extremely important." Business leaders, on the other hand, while not quite as enthusiastic about the benefits of developing a strong security culture, are largely on-board with the idea that it's an important thing to develop for their organizations. However, fewer than two-thirds of other employees are similarly inclined: only 63 percent consider the development of a strong cybersecurity culture to be "important" or "extremely important," while more than one-third consider it to be of only moderate importance.

What this tells us is that IT, security and business leaders – while generally desirous of establishing a strong cybersecurity culture within their organization – are somehow not conveying that idea effectively to a large proportion of their employees. This could be the result of a number of factors, such as high employee turnover, ineffective training, insufficient time given to training, a failure to convey just how important security really is to the organization, an overreliance on technology to stop threats, and other factors.

However, as discussed later in this section, a key reason that many employees are not fully engaged in developing a strong cybersecurity culture may be that their management has not made it clear just how important users are in the security process – or management may not actually believe that to be the case.

Figure 9: Importance of developing a strong cybersecurity culture

Percentage responding "agree" or "strongly agree"



96%

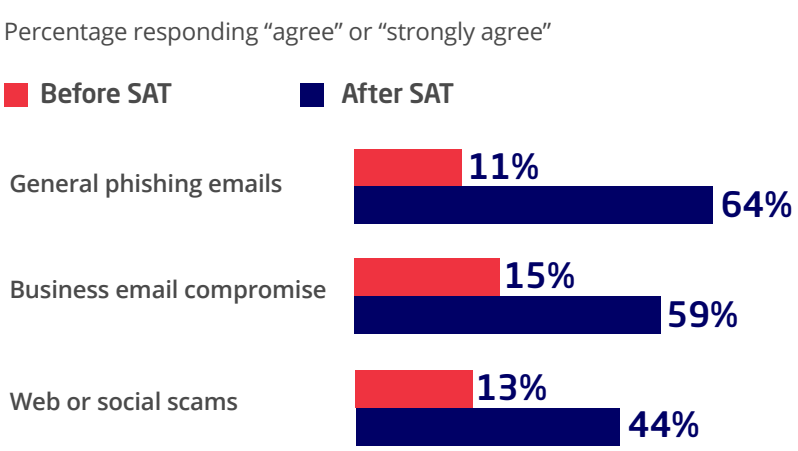
of IT, security decision makers and influencers clearly understand that security awareness training provides significant benefits.

Training increases users' security savvy

IT and security decision makers and influencers clearly understand that security awareness training provides significant benefits. As shown in Figure 10, IT and security decision makers and influencers had little confidence in the average user's ability to detect threats like phishing emails, business email compromise attempts, or web/social media scams prior to going through training. However, after training these users are perceived to be dramatically more capable than they were before – in the case of phishing emails, for example, the number of users perceived to be "capable" or "very capable" at detecting these threats jumped nearly six-fold, from 11 percent to 64 percent.

The good news here is that IT and security decision makers and influencers really do understand just how effective good security awareness training can be in developing users' abilities to detect malicious content. **The bad news is that the figures in the blue bars should be significantly greater, since this data tells us that, despite training, a large proportion of users still is not capable of detecting common security threats.**

Figure 10: Capability of users before and after training for various threats



mimecast

Changing User Behavior to Change the Security Culture

To complement the results of the survey of those who contribute to or influence their organization's security awareness training program, we conducted a survey of 1,000 U.S.-based employees about their security awareness training and other issues. This section presents the results of that survey.

The perceived utility of training increases with interest level and continuous employee engagement

Our research discovered that the perceived utility of training is closely aligned to both the interest level that users have in this training and the amount of interaction they spend in it. For example, as shown in Figure 11, those who find security awareness training to be "very interesting" also are most likely to find it has created the type of systemic change discussed in the previous section. Similarly, a plurality of those who spend the most time in training also become fundamentally changed in terms of how they think about security.

Figure 11: Perceived utility of training vs. user interest in training

	Boring	Somewhat Interesting	Very Interesting
It's not useful and has made no change in how I deal with security	36%	4%	3%
It's somewhat useful and has gotten me to think more about security	47%	40%	8%
It's quite useful and has caused me to substantially change how I think about security	13%	44%	21%
Sales activity/contact customers, prospects	5%	12%	68%

Users get better when their interest increases in their training

Not all that surprisingly, we also found a **relationship between the interest level and the users' perceptions of their own ability to detect things like phishing emails and email compromise attacks**. For example, as shown in Figure 12, only 47 percent of users who find security awareness training to be "boring" believe they are highly capable of detecting a phishing attempt, whereas 73 percent of those who find their training to be "very interesting" are capable of doing so. Similarly, while 50 percent of those who spend no more than five minutes per month in security awareness training believe they can reliably detect a phishing email, 63 percent of users who spend more than 15 minutes per month in training believe they can reliably detect such an email.

Figure 12: Users' ability to detect various types of threats vs. interest level in training

	Boring	Somewhat Interesting	Very Interesting
A mass-mailed phishing email	47%	50%	73%
A spear-phishing email that specifically targets your organization or a group in your organization	38%	43%	79%
An email compromise attack that is supposedly from your organization's CEO or another leader in your organization	40%	44%	73%
A fake tweet on Twitter	30%	34%	66%
A malicious advertisement on Facebook	36%	37%	68%

Interesting training completed in regular intervals benefits users personally

Ideally, the ultimate goal of security awareness training is the creation of systemic change in users as evidenced by users applying the principles they've learned to their non-work life. If the training is effective, it will convince users that modifying their behavior and thinking about security in a fundamentally different way will be to their advantage in all areas of life, both professional and personal.

Our research found that the more interesting security awareness training is perceived to be, the more likely that users will fundamentally change their security behavior in areas like changing passwords regularly, eliminating password re-use, or not using public Wi-Fi hotspots without appropriate protection, as shown in Figure 13.

The more interesting security awareness training is percieved to be, the more likely that users will fundamentally change their security behavior.

Figure 13: Extent to which training has changed users' personal behavior based on users' interest level in training

	Boring	Somewhat Interesting	Very Interesting
I update my passwords on a regular basis			
• Done this because of training	43%	40%	73%
• Considering because of training	14%	25%	14%
• Would have done this anyway	26%	29%	11%
• Have not done this	17%	6%	3%
I use a unique password for every device and application			
• Done this because of training	24%	26%	53%
• Considering because of training	26%	30%	34%
• Would have done this anyway	25%	29%	11%
• Have not done this	25%	11%	2%
I change the password on my home's Wi-Fi router			
• Done this because of training	18%	25%	52%
• Considering because of training	19%	28%	28%
• Would have done this anyway	26%	27%	14%
• Have not done this	37%	21%	5%
I enable 2FA on my banking or other personal accounts			
• Done this because of training	23%	34%	52%
• Considering because of training	17%	22%	31%
• Would have done this anyway	37%	32%	14%
• Have not done this	23%	13%	5%
I protect my mobile phone with a PIN or fingerprint			
• Done this because of training	21%	28%	54%
• Considering because of training	15%	19%	26%
• Would have done this anyway	44%	42%	14%
• Have not done this	20%	12%	5%
I won't access a public Wi-Fi hotspot without a VPN or other protection			
• Done this because of training	19%	30%	49%
• Considering because of training	23%	20%	31%
• Would have done this anyway	25%	32%	12%
• Have not done this	32%	18%	9%

We found a similar relationship between users' level of interest in their security awareness training and the proportion that can report suspicious content. As shown in Figure 14, among those who find their training to be "boring", only 76 percent can report suspicious emails and the like. However, among those who find their training to be very interesting, 95 percent can report suspicious content to their IT and/or security teams.

These results were not really all that surprising. For just about any user, the more time they spend using something, the more they discover things they like and dislike about it. A user of Microsoft Excel, for example, will find previously undiscovered features that they can put to good use the more they use the software, but they will also discover previously unknown quirks and bugs.

Figure 14: Ability for users to report suspicious emails, attachments, etc. based on their interest level in training

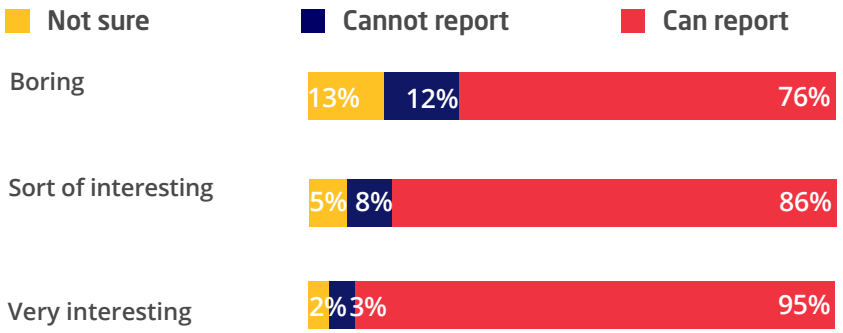


Figure 15: Users' agreement with various aspects of training based on interest level

	Boring	Somewhat Interesting	Very Interesting
It speaks in a way I can clearly understand	37%	53%	85%
It's relevant to my responsibilities	35%	55%	82%
It's visually appealing	22%	40%	77%
It lasts the right amount of time per session	25%	45%	78%
It's well written	29%	47%	80%
It gives security advice I can use	35%	58%	85%
It provides the right amount of interactivity	29%	45%	80%
I like its use of real-world examples	34%	55%	80%
I learn a lot from it	29%	49%	83%
It's too technical	23%	21%	57%
It's ugly or bland to look at	22%	16%	56%
It's too wordy	23%	19%	54%
I feel like the training is talking down to me	26%	17%	61%

Next Steps to Improving the Security Culture

Osterman Research offers the following recommendations for decision makers to consider as they evaluate the role that security awareness training should play in their organizations

01

Train users with a view toward systemic change

The fundamental goal of security awareness training must be to affect substantive and permanent change in the security practices of those who learn from it, not merely "checking the boxes" that they understand security.

When employees go through training and then willingly put into practice what they've learned, both professionally and personally, that will be the sign that the training has hit its mark and moved the organization closer to becoming a culture of security.

This systemic change must become an essential part of how employees and contractors work with communications systems, corporate data sources, cloud services, and the like.

In essence, good security awareness training will result in something akin to "muscle memory" – skepticism about suspicious-looking requests, care in opening attachments or clicking on links, caution when accessing new networks, and the like will become more or less automatic to those properly immersed in good security training.

02

Get buy-in from the board of directors and senior management

Arguably, the most important single element of success for any security awareness training program will be obtaining buy-in from senior management across the organization, including the board of directors. Senior managers or board members who see little value in good security awareness training, or who see employees as an encumbrance to good security rather than part of the solution to security problems, are very unlikely to support any meaningful training program.

Moreover, senior management must be willing consumers of the training, not merely those ordering those beneath them to go through it while not going through it themselves. In short, if security awareness training is to be successful, it must first find strong support among those who have the power to make it successful.

Figure out if your current culture supports good training

Not all corporate cultures will lend themselves well to making the sort of systemic changes that are necessary to create a security-focused culture. If senior managers are not teachable, if employees are resistant to the idea of change or implicitly rewarded for not changing, or if management merely gives lip service to good security awareness training without providing adequate funding and effort to make it happen, the culture simply won't change.

Make sure that training is adequate and tailored to the organization

Security awareness training must address all of the issues that are relevant to the organization, including those that are specific to the organization and the industry in which it operates. Generic training will be useful to a point, but it must include specifics that will enable employees to address their unique obligations and requirements.

Make training interesting and enjoyable

Security awareness training that is dull and boring won't be nearly as successful in accomplishing its goals as that which is interesting and enjoyable. As discussed in this paper, the more interesting that users find training to be, the more effective it is in accomplishing its goals of helping to develop the necessary change in users' security mindset.

Measure your success and identify areas for improvement

It's important to measure the success of any security awareness training program with the goal of making improvements in how information is presented, how receptive users are to the information presented to them, and how effective it actually is in changing the corporate culture. The survey of IT and security decision makers and influencers conducted for this program found that only 23 percent of organizations always survey employees on what they think of the training they receive, while another 52 percent sometimes do so. The IT/security survey also found that only 37 percent of employees really enjoy the training they receive, revealing that there is significant room for improvement in making the content more engaging.

Ensure training is more positive than punitive

Finally, as many have said in the past, security awareness training should be primarily about enforcing positive changes, not punishing negative ones. To be sure, an employee who goes through training and continues to practice risky behaviors should be dealt with appropriately, but positive reinforcement will generally be more effective in accomplishing the long-term goals of systemic change that most organizations are seeking from their investments in training.

Summary

Good security awareness training is an essential element in improving any organization's security defenses because it gives employees and contractors the knowledge and skepticism necessary to avoid making mistakes that could lead to security problems like ransomware infections or data breaches.

The fundamental goal of any security awareness training should be the development of systemic change that will fundamentally alter the behavior of employees and lead to the development of a truly security-focused corporate culture.

mimecast

Why Mimecast Awareness Training?

Stop Ticking Boxes. Start Delivering Real Change.

If you're like most companies, your cybersecurity awareness training isn't working. In fact, more than 90% of breaches involve human error. Don't just focus on the bad actors. Focus on the inside. If your employees aren't engaged, you're just wasting time and money – and they're still forwarding spam emails and clicking phishing links.

Why? We're sorry to break it to you, but traditional cybersecurity awareness training can be really boring. But it doesn't have to be.

We're all human. We all make mistakes. But some mistakes can have a big impact on your business. That's why you need to know what causes human error when designing your training program. Mimecast's Awareness Training isn't anyone's grandfather's security training solution. It's different. By assessing risk in real-time using a broad host of criteria.

Mimecast's security awareness training will actually make your people sit up, listen and rethink their cybersecurity habits, well after they've finished it. And they might even have a few laughs along the way. It's time to stop blindly ticking boxes - and join us in delivering real, powerful and lasting change.

Learn More

Evaluate risk in real-time, using a broad host of criteria:

- **Lack of Knowledge:** Don't go on a rant about JavaScript. Tell them what to do, what not to do, and why.
- **Lack of Attention:** Cut through the noise, grab their attention – and make them laugh. That way, they'll be emotionally invested enough to remember not to click on that suspicious dancing leprechaun GIF.
- **Lack of Concern:** Security should be a constant concern for everyone. Make sure you explain to your employees why they should care, even after training.
- **Human Error:** Mimecast's platform, Mime|OS is designed from the ground up to connect with humans, no robots. The Mimecast solution evaluates employees in real-time across the root causes of human error, and assessing your user and organizational risk score.

mimecast™

[i.] *Richard Steinnon, Security Yearbook 2020: A History and Directory of the IT Security Industry* | [ii.] *SE Labs, Email Security Services Protection, Jan-Mar 2020*