THE STATE OF SECURITY AWARENESS TRAINING

Executive summary

Technology-based security solutions like firewalls, endpoint detection and response solutions, secure email gateways, desktop antivirus, cloud-based malware and spam filtering are essential elements of a security infrastructure. However, too many decision makers neglect another important element that's necessary to keep networks, data, applications, and financial resources safe: the human beings who interact with them.

Security awareness training is designed to bolster users' ability to recognize threats like phishing attempts, unusual requests that claim to be from their company's CEO, malicious advertising on web pages, and a host of other threats that are designed to trick users into doing something that can wreak havoc within an organization. Users who are well trained on security issues will be more skeptical and more careful about opening emails, clicking on social media links, or visiting web pages without first checking for clues about their validity.

This white paper reviews the results of an in-depth survey of organizations conducted by Osterman Research during May and June 2019. This paper discusses the challenges and gaps in existing awareness training trends, and the justification for deploying an effective security awareness training program in order to generate a significant return-on-investment (ROI) and demonstrate results.

Key takeaways

- 75 percent of security decision-makers are highly concerned with phishing attacks.
- 58 percent of decision-makers view awareness training as superior to technology solutions when dealing with phishing.
- Awareness training budgets are increasing faster than security budgets.
- Employees receive more training time, but there is no significant change in employees behavior and no measurable KPIs.
- Most awareness training programs fail to demonstrate a change in employee behavior towards phishing attacks.
- Better awareness training options should include continuous training that is data-driven and offers an adaptive and customized program for each employee.
- A more effective training program does not mean more dollars or training time, but rather a training program that engages employees without taxing the security team.

Security decision makers are mostly concerned with phishing attacks

Phishing attacks top the list of concerns for decision makers. About 75% of executives in small and large enterprises responded that phishing emails tops their list of security concerns.

Figure 1

Decision Makers' and Influencers' Security Concerns
Percentage Indicating They are "Concerned" or "Extremely Concerned"

Security Concern	Total	50 to 999 Employees	1,000+ Employees
Phishing attacks	**74%**	74%	75%
Malware other than ransomware	**68%**	64%	71%
A breach of sensitive or confidential data	**68%**	65%	71%
Ransomware attacks	**67%**	65%	69%
CEO Fraud/BEC attacks	**63%**	60%	66%
Targeted attacks	**61%**	50%	71%
Zero-day exploits	**57%**	53%	61%
Malware infiltration through web traffic	**57%**	50%	64%
Account takeover attacks	**53%**	50%	57%
Malware infections that occur through web surfing	**53%**	55%	52%
Malvertising	**42%**	38%	45%
Spam	**41%**	35%	46%

Decision makers view awareness training as superior to technology solutions when dealing with phishing

The research found that while dealing with most threats, technology-based solutions are generally viewed as superior to security awareness training. However, for phishing and business email compromise (BEC) attacks, decision makers generally regard training as a better way to deal with these threats.

Figure 2

Perceptions About the Effectiveness of Technology-Based Security Defenses vs. Security Awareness Training
Percentage Indicating That Solution Works "Well" or "Extremely Well"

Security Concern	Total		50 to 999 Employees		1,000+ Employees	
	Tech	SAT	Tech	SAT	Tech	SAT
Phishing attacks	50%	58%	43%	57%	56%	60%
CEO Fraud/BEC attacks	48%	65%	41%	63%	55%	66%
Malware other than ransomware	62%	50%	62%	49%	62%	51%
Employees surfing websites that violate policies	62%	51%	62%	48%	62%	55%
Ransomware attacks	61%	51%	58%	47%	64%	55%
Malware infections that occur through web surfing	60%	46%	56%	38%	64%	54%
Malware infiltration through web traffic	59%	44%	60%	41%	58%	47%
Spam	56%	48%	55%	45%	57%	51%
Targeted attacks	51%	45%	48%	40%	54%	50%
A breach of sensitive or confidential data	50%	48%	41%	39%	58%	57%
Cryptocurrency mining malware	50%	40%	43%	34%	55%	46%
Malvertising	50%	44%	48%	37%	53%	55%
Zero-day exploits	48%	39%	45%	35%	50%	43%
Account takeover attacks	48%	39%	45%	35%	50%	43%
"Shadow IT"	48%	42%	42%	37%	53%	47%

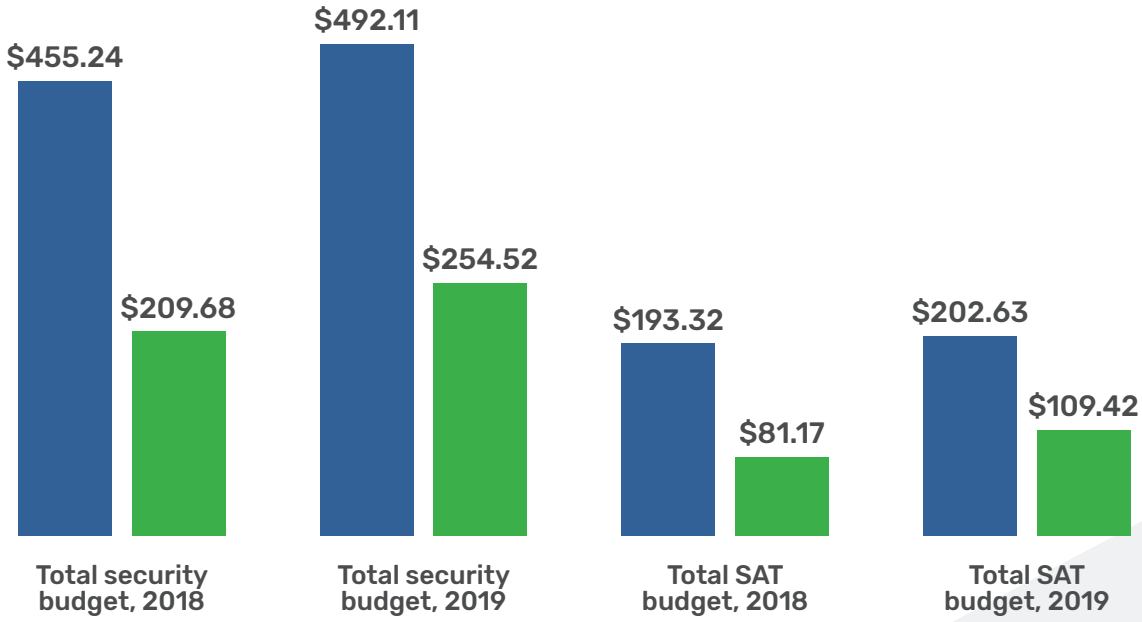
Source: Osterman Research, Inc. *"Tech" refers to technology-based security solutions; SAT refers to security awareness training*

Awareness training budgets are increasing faster than security budgets

Security budgets at the vast majority of organizations have been increasing over time. Interestingly, a relatively small proportion of the total budget is spent on anti-phishing technologies, despite the high concern. Luckily, security awareness budgets are growing at a significantly faster pace than overall security budgets.

Figure 3

Security and Security Awareness Training Budgets per Employee
2018 and 2019



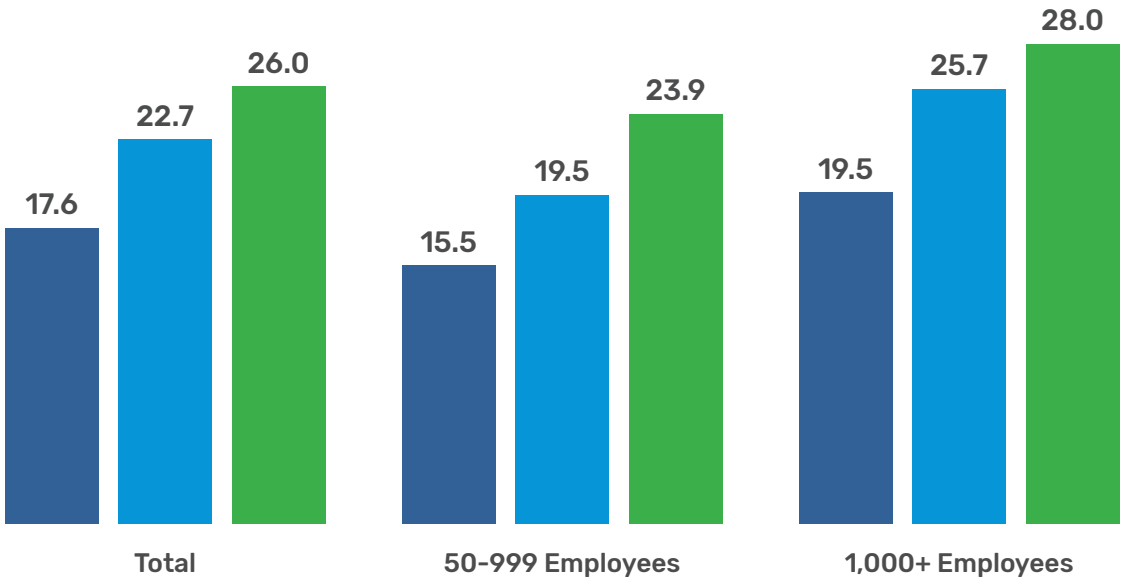
Source: *Osterman Research, Inc.*

Employees receive more training time but not at sufficient frequency

The budget growth coincides with a significant increase in the monthly minutes of security awareness training that users receive, from an average of 17.6 minutes in mid-2018 to 26.0 minutes expected by mid-2020.

Figure 4

Monthly Minutes of Security Awareness Training for the Typical Employe
2018 through 2020



Source: *Osterman Research, Inc.*

Various approaches to training

Our research found that there is a wide range of security awareness training programs in use other than the "do-nothing" approach employed by five percent of organizations. As shown in Figure 3, the most common approach to security awareness training is to test everyone using simulated phishing attacks, the approach taken by 39 percent of organizations. Employed by one-third of organizations is the security awareness video approach, followed by selective training for some employees, and the "break-room or lunch-and-learn" approach.

Figure 5

Current Approaches to Security Awareness Training

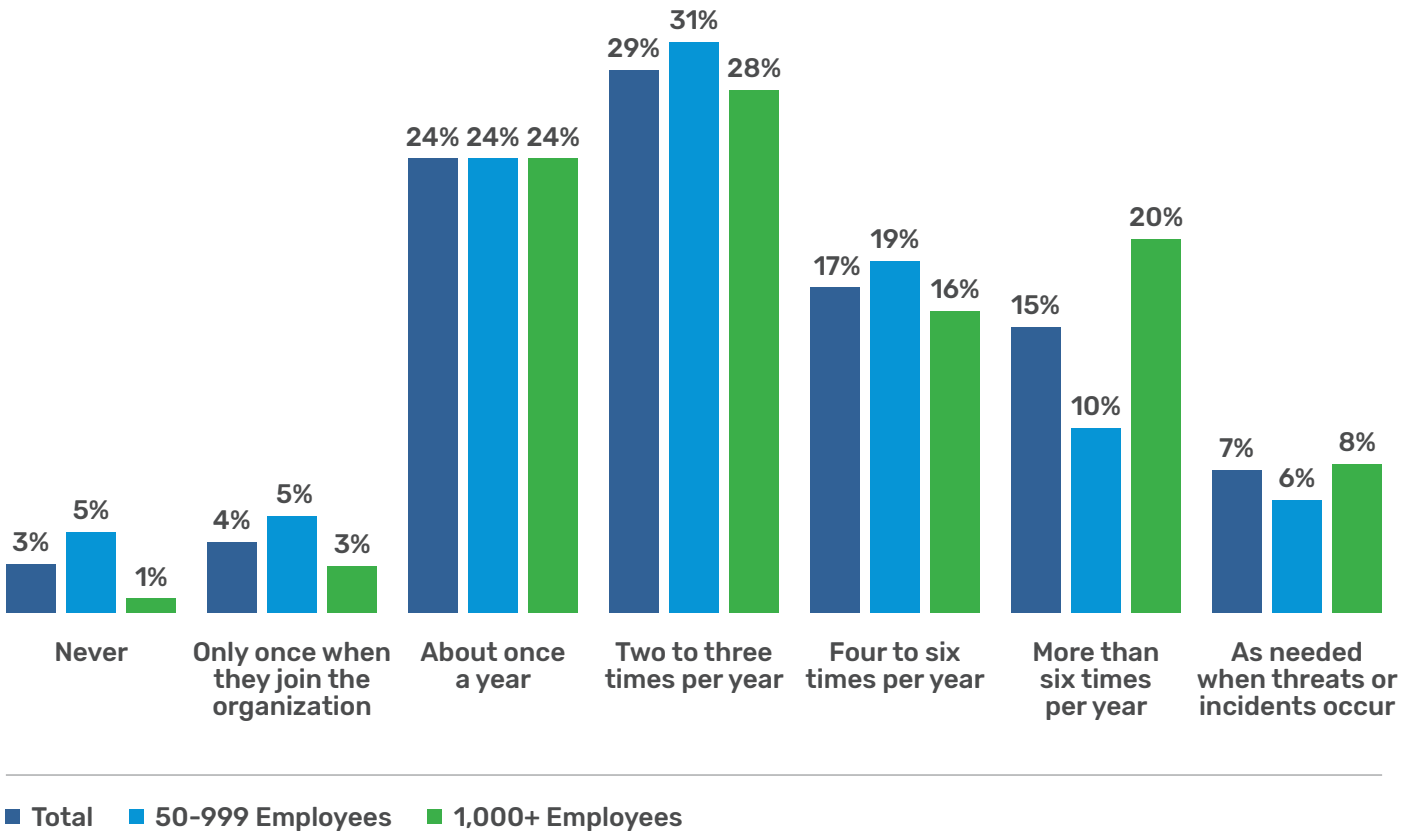
Source: *Osterman Research, Inc.*

Most users are not adequately trained

Despite the fact that users are receiving more security training over time, many users still do not receive adequate training to protect their organizations. As shown in Figure 6, nearly one-third of users receive training no more than about once each year or less often. Another 29 percent receive security awareness training only two to three times per year. Only 39 percent of users receive training quarterly or more often.

Figure 6

Frequency of Conducting Security Awareness Training



Source: *Osterman Research, Inc.*

Conclusion

There's currently a gap in the awareness training market which needs to be filled out with more effective awareness training solutions. To show consistent results and change employee behavior, awareness training needs to be conducted continuously, be driven by data science and follow a proven methodology. Awareness training also needs to offer customization, and utilize machine learning to adapt its training content and frequency to employees learning patterns and pace (as opposed to the one-size-fits-all approach offered by some training vendors).

A different training approach doesn't mean greater effort and increased investment in training time or financial resources. On the contrary, it should offer short, frequent training engagements that are continuous, so the learning itself is more engaging, effective and measurable.

About Cybeready

CybeReady is the only autonomous cybersecurity training platform for enterprises. The CyberReady solution utilizes data science-powered training that implements next-level, adaptive learning methodology and guarantees change in employee behavior towards phishing attacks. CybeReady's human learning automation allows employees to train year-round, continuously advancing and adapting their skills to match real-world phishing attacks. The solution is fully-managed, making CybeReady the security awareness training solution with the lowest total cost of ownership (TCO) available today. Founded in 2015 by Omer Taran (CTO) and Mike Polatsek (CSO), CybeReady is headquartered in Tel Aviv, Israel, with offices in London and the Silicon Valley. For more information, please visit www.cybeready.com.

About the survey and white paper

Osterman Research conducted a survey among 230 individuals in North American organizations (primarily for-profit companies) who are familiar with security and security awareness training issues in their organizations. We split the survey respondents into two groups, those with 50 to 999 employees and those with 1,000 or more employees, to understand and evaluate differences between them. This white paper was sponsored by Infosec, KnowBe4 and Mimecast; information about each sponsor is provided at the end of this paper.