Osterman Research
WHITE PAPER

White Paper by Osterman Research
Published **August 2019**
Sponsored by **Infosec**

The ROI of Security Awareness Training

Executive Summary

Technology-based solutions like firewalls, endpoint detection and response solutions, secure email gateways, desktop anti-virus, 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 and financial resources safe: the human beings who interface with their networks, data and financial resources.

Security awareness training is designed to bolster users' ability to recognize threats like phishing attempts, unusual requests that purport 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 discusses the results of an in-depth survey of organizations conducted by Osterman Research during May and June 2019. This paper discusses the financial justification for deploying a robust security awareness training program and demonstrates the significant return-on-investment (ROI) that can result. It is also important to note that security awareness training program is not just about avoiding security problems, but avoiding the significant losses that can result in the absence of training.

Security awareness training is designed to bolster users' ability to recognize threats.

KEY TAKEAWAYS

- **Security budgets are increasing**
  Security budgets at the vast majority of organizations are increasing over time. Interestingly, at many organizations a relatively small proportion of the total security budget is spent on anti-phishing technologies, despite the fact that phishing is regarded as the leading overall concern, and many other concerns are the direct result of phishing.

- **But security awareness training budgets are increasing even faster**
  On a per-employee and per-email-user basis, security awareness budgets are growing at a significantly faster pace than overall security budgets. The growth in these budgets 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.

- **Training dramatically improves users' ability to recognize threats**
  Before security awareness training, IT and security have relatively little confidence in their users' ability to recognize various types of threats. However, after users have received training, the level of confidence in their knowledge and ability to avoid threats jumps dramatically – up to three times in some cases.

- **The ROI for security awareness training is significant**
  The ROI for security awareness training can vary widely based on a number of factors. However, the cost and ROI model that Osterman Research has developed – as shown later in this paper – demonstrate that, on average, smaller organizations (50 to 999 employees) can achieve an ROI of 69 percent from a security awareness training program, while larger organizations (1,000+ employees) can achieve an ROI of 562 percent.

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; information about the sponsor is provided at the end of this paper.

Where are Security Dollars Going?

SECURITY BUDGETS CONTINUE TO INCREASE

Security budgets vary widely based on a number of factors, including the industry in which an organization participates, the number of employees it has, the geographical distribution of its employees and offices, and the risk tolerance of its senior management.

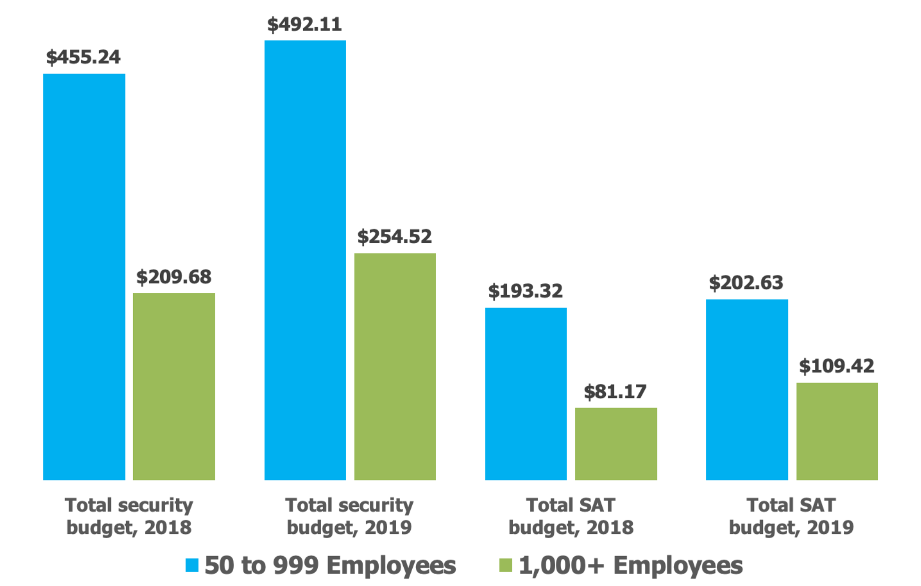
We found that for 2018, the mean security budget at the organizations we surveyed was $332 per employee, increasing to $373 per employee in 2019, an increase of 12 percent. However, the per-employee budget at smaller organizations was much higher in 2018 at $455, growing to $492 in 2019. Larger organizations, owing to the economies of scale that they enjoy, had a mean security budget of $210 per employee in 2018, growing to $255 in 2019.

SECURITY AWARENESS TRAINING BUDGETS ALSO GROWING

Our research found that the overall security awareness training budget in 2018 was $137 per employee, growing to $156 per employee in 2019. For smaller organizations, the mean expenditure per employee was $193 in 2018, growing to $203 in 2019; for larger organizations, the 2018 security awareness training budget was $81 per employee, growing to $109 in 2019. The survey data on overall security budgets and security awareness training budgets is summarized in Figure 1.

There is a wide range of security awareness training programs in use other than the "do-nothing" approach.

Figure 1
Security and Security Awareness Training Budgets per Employee
2018 and 2019

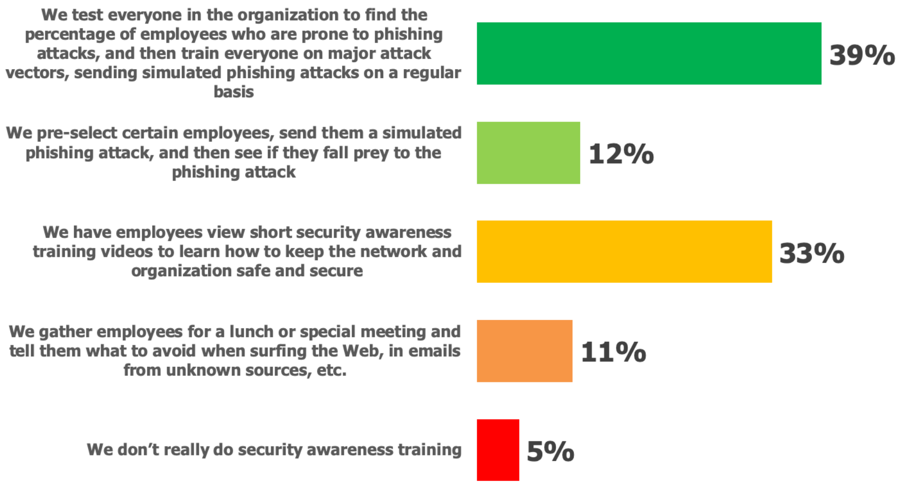


Source: Osterman Research, Inc.

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 2, the most common approach to security awareness training is to test everyone on 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" awareness video approach, following by selective training for some employees, and the "break-room" approach.

Figure 2
Current Approaches to Security Awareness Training



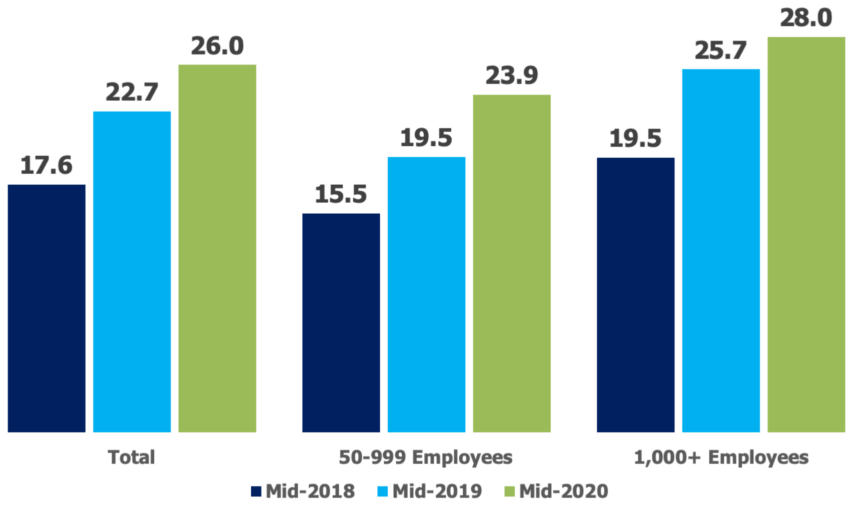
Source: Osterman Research, Inc.

TRAINING INVESTMENTS ARE INCREASING

The increases in budgets for security awareness training discussed earlier are being translated into end users spending significantly more time in training on security issues. As shown in Figure 3, the average employee spent just under 18 minutes per month in mid-2018, but this has jumped to nearly 23 minutes in 2019 and is expected to increase to 26 minutes by mid-2020. These data show there has been an increase in the average time spent in security awareness training of 29 percent from 2018 to 2019, and there will be a 15 percent increase from 2019 to 2020. Moreover, we found that employee time spent in security awareness training is greater in larger organizations.

The increases in budgets for security awareness training are being translated into end users spending significantly more time in training.

Figure 3
Monthly Minutes of Security Awareness Training for the Typical Employee
2018 through 2020



Source: Osterman Research, Inc.

WHY ARE INVESTMENTS GROWING?

Why are investments in security awareness training increasing and significantly so? We believe there are two primary reasons:

- Corporate security decision makers increasingly understand the benefits of security awareness training as a complement to technology-based security infrastructure and services. The evidence is clear, as presented in this report and elsewhere, that security awareness training can reduce the success of phishing attempts and other types of attacks and can provide a significant ROI.

- Traditional security vendors increasingly realize that security awareness training offers an important complement to their traditional offerings and are either acquiring security awareness vendors or offering various types of security awareness training. For example, in 2018, Mimecast acquired Ataata, Barracuda acquired PhishLine, and Proofpoint acquired Wombat Security Technologies; and in 2017 Webroot acquired Securecast. Plus, there are traditional, infrastructure- and solution-focused security vendors that offer some form of security awareness training, including Trend Micro (which has recently partnered with four security awareness vendors[i]), Sophos, and Symantec. In short, it's no longer just security awareness training companies that are pushing the importance of training users, but traditional security solution vendors as well.

Corporate security decision makers increasingly understand the benefits of security awareness training.

The ROI of Security Awareness Training

THE COSTS WITH AND WITHOUT TRAINING

To determine the costs of not having security awareness and the costs experienced after a security awareness training program has been implemented, we built a cost model based on the survey data and various assumptions:

- Annual, fully burdened salary of IT staff members: $80,000

- Annual, fully burdened salary of non-IT employees: $75,000

- Hours worked per year per employee: 2,080

- Employee productivity loss during downtime caused by malware/ransomware while the incident is being remediated remediation: 70 percent

- Mean number of hours that employees would experience downtime during a malware/ransomware incident: 9.9 hours in smaller organizations; 18.0 hours in larger organizations (based on the research conducted for this white paper).

- There is one major malware/ransomware incident per year caused by an employee mistake. We further assume that after security awareness training, the chance of an employee-caused mistake of this type is reduced by 90 percent.

- Despite the time investment required of employees for security awareness training, much of this occurs during the normal work process and so the actual reduction in employee productivity from training is only 15 percent.

- Pricing for security awareness training is the average pricing for smaller and larger organizations published by a leading vendor in the training space.

Please note that these assumptions can vary widely based on geography and other factors. For example, the average base pay for a systems administrator in Jacksonville, Florida is $61,877, whereas the same position in San Jose, California averages $92,962[1], so salaries by themselves can have a major impact on ROI. Combining these assumptions and the research conducted for this white paper, we developed the following calculations shown in Figures 4 and 5.

Salaries by themselves can have a major impact on ROI.

Figure 4
Costs Before Security Awareness Training

Cost Elements	50 to 99 Emps	1,000+ Emps
Annual IT/security person-hours spent per 1,000 email users disinfecting workstations, networks	760.0	137.3
Annual cost per email user	$29.23	$5.28
IT/security hours to remediate one major malware or ransomware attack per 1,000 email users	195.2	730.9
Hours of downtime per 1,000 email users during remediation period [2]	9,881	18,043
Annual IT/security costs	$7,510	$28,111
Annual non-IT employee costs	$249,394	$455,406
Annual IT/security costs, per email user	$7.51	$28.11
Annual costs, per email user	$249.39	$455.41
TOTAL COSTS PER EMAIL USER BEFORE SAT	**$286.14**	**$488.80**

Source: Osterman Research, Inc.

[1] Source: Glassdoor

[2] This calculation is based on the number of hours per 1,000 email users. It also applies to organizations with fewer than 1,000 email users.

Figure 5
Costs After Security Awareness Training

Cost Elements	50 to 99 Emps	1,000+ Emps
Annual IT/security person-hours spent disinfecting workstations, networks	565.5	120.5
Cost per email user	$21.75	$4.63
IT/security hours to remediate one major malware or ransomware attack per 1,000 email users	195.2	730.9
Hours of downtime per 1,000 email users	9,881	18,043
Annual IT/security costs, per email user	$7.51	$28.11
Annual email user costs, per email user	$249.39	$455.41
Likelihood of an attack caused by a user mistake	10%	10%
Annual IT/security costs, per email user	$0.75	$2.81
Annual costs, per email user	$24.94	$45.54
Annual IT/security hours devoted to SAT per 1,000 email users	1,159.9	309.4
Cost per email user	$44.61	$11.90
Cost of SAT, per email user	$23.00	$17.50
Cost of employee time spent in SAT	$21.11	$27.83
TOTAL COSTS PER EMPLOYEE AFTER SAT	**$136.17**	**$110.21**

Source: Osterman Research, Inc.

SCENARIO 1: ONGOING, REGULAR SECURITY EVENTS

Using these calculations, we determined that the aggregate costs of dealing with disinfecting workstations and remediating malware/ransomware incidents without security awareness training are as shown in Figures 11 and 12, respectively.

We also found that when security awareness training is implemented, the costs of disinfecting workstations and remediating malware/ransomware attacks goes down dramatically, resulting in a significant ROI for both small and large organizations. However, given that our research found that larger organizations spend less on security awareness training per employee and experience some costs that can be lower than for their smaller counterparts, the ROI is significantly greater for large firms, as shown in Figures 6 and 7.

When security awareness training is implemented, the costs of disinfecting workstations and remediating malware/ransomware attacks goes down dramatically.

Figure 6
Smaller Organizations, Annual Cost per Employee

	Before SAT	After SAT	ROI
Disinfecting workstations	$29.23	$21.75	**69%**
Remediating malware/ransomware	$256.90	$25.69	
Labor cost of SAT	$0	$44.61	
Cost of SAT	$0	$23.00	
Employee time spent on SAT	$0	$21.11	
TOTAL	**$286.14**	**$136.17**	

Source: Osterman Research, Inc.

Figure 7
Larger Organizations, Annual Cost per Employee

	Before SAT	After SAT	ROI
Disinfecting workstations	$5.28	$4.63	562%
Remediating malware/ransomware	$483.52	$48.35	
Labor cost of SAT	$0	$11.90	
Cost of SAT	$0	$17.50	
Employee time spent on SAT	$0	$27.83	
TOTAL	**$488.80**	**$110.21**	

Source: Osterman Research, Inc.

OTHER COSTS

It's important to note the figures above represent the direct costs that security awareness training can reduce. However, there are other costs that are more difficult to quantify, such as:

- **Loss of customers and revenue**
  A data breach can result in loss of customers. For example, a Carnegie Mellon study of more than 500,000 bank customers found that if a customer discovered unauthorized charges on his or her account, they were one percent more likely to switch banks during the following six months than the average customer of the bank. The study also found that long-term customers were more likely to leave[ii]. Target experienced a 46 percent year-over-year sales decline in the fourth quarter of 2013 following disclosure of its data breach[iii]. A Gemalto study found that for companies that suffer a data breach, seven in 10 customers would stop doing business[iv]; another study had similar findings[v].

- **Loss of valuation**
  A data breach, ransomware infection or some other major security issue can have both immediate and long-term impacts on an organization's valuation. For example, one analysis found that the largest drop in a company's stock price comes 14 days after public disclosure of the breach. While the stock will rebound significantly in the 12 months following disclosure of the breach, the increase in stock price is not as great as it would have been had the breach not occurred[vi].

- **Loss of reputation**
  An organization that suffers a ransomware attack or a data breach, for example, will certainly face a loss of reputation when the problem becomes public knowledge. While loss of reputation carries with it a number of problems, it's a difficult one to quantify the context of ROI calculations.

- **Other costs**
  There are several other costs associated with data breaches and various kinds of security problems. These include fines from regulators, legal costs, the cost of credit reporting services provided to customers who have had their data stolen, and the cost of terminating employees who were responsible for the breach. Moreover, if a data breach results in the loss of intellectual property, there can be protracted legal actions, loss of patents, and the intellectual property itself.

For companies that suffer a data breach, seven in 10 customers would stop doing business.

SCENARIO 2: OCCASIONAL, "UNLIKELY" EVENTS

The scenario above describes the somewhat regular, ongoing events that impact organizations. But what about events that occur with much less regularity, but that can cause devastating consequences, and could be prevented – or the chance of them occurring reduced – with appropriate security awareness training? For example:

- Let's assume that a 500-user organization has the potential of experiencing a data breach from a data-stealing malware attack that costs it $2 million dollars in remediation costs, lost revenue, lost goodwill, and the like.

- Let's also assume that a 5,000-user organization faces the potential of the same type of attack, but its cost would be $9 million because of the much larger number of records that would be lost, greater costs of remediation, and so forth.

- We will also conservatively assume that these risks are unlikely, and will occur only once every 10 years.

- Finally, we will conservatively assume that good security awareness training can reduce the likelihood of these attacks by 80 percent. Please note that this is an assumption that can vary widely.

Based on these assumptions, the costs and ROI associated with these unlikely events are shown in Figures 8 and 9.

Figure 8
500-User Organization, Cost and ROI of Unusual Events

Cost of data breach	$2,000,000	**1,500% ROI**
Likelihood per year	10%	
Cost per year without SAT	$200,000	
Annual security awareness training costs	$10,000	
Cost per year with SAT	$40,000	

Source: Osterman Research, Inc.

Figure 9
500-User Organization, Cost and ROI of Unusual Events

Cost of data breach	$9,000,000	**2,204% ROI**
Likelihood per year	10%	
Cost per year without SAT	$900,000	
Annual security awareness training costs	$31,250	
Cost per year with SAT	$180,000	

Source: Osterman Research, Inc.

Security awareness training should be a key element of any organization's security strategy.

Summary

Security awareness training should be a key element of any organization's security strategy. Just like the right technology like firewalls, endpoint detection and response solutions, secure email gateways, cloud-based filtering, and other solutions, good employee training can also protect an organization's data and financial assets from theft or destruction. Good security awareness training can provide a significant ROI and pay for itself in a short time.

Sponsor of This White Paper

INFOSEC

www.infosecinstitute.com/iq

info@infosecinstitute.com

@InfosecEdu

+1 708 689 0131

At Infosec, we believe knowledge is the most powerful tool in the fight against cybercrime. We empower all employees with security awareness training to stay cybersecure at work and home, and we help IT and security professionals advance their careers with a full regimen of certification and skills training. Driven by smart people wanting to do good, Infosec educates entire organizations on how to defend themselves from cybercrime. That's what we do every day — equipping everyone with the latest security skills so the good guys win.

Infosec IQ security training and awareness empowers your employees with the knowledge and skills to stay cybersecure at work and home. With over 2,000 awareness and training resources, you'll have everything you need to prepare employees to detect, report and defeat cybercrime. Every aspect of the platform can be customized and personalized to match your organization's culture and employees' learning styles.

To learn more, visit: https://www.infosecinstitute.com/iq.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

[i] http://www.enterpriseitworld.com/news/trend-micro-partners-with-market-leading-security-awareness-vendors/

[ii] https://deltarisk.com/blog/the-impact-of-bank-data-breaches-on-customer-loyalty-and-retention/

[iii] https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html

[iv] https://itsecuritycentral.teramind.co/2017/12/20/data-breach-cost-when-you-lose-your-customers/

[v] https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html

[vi] https://duo.com/decipher/data-breaches-have-long-term-impact-on-stock-price