Survey Report: Best Practices for Dealing With Phishing and Ransomware

An Osterman Research Industry Survey Report

December 2016

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

FIGURES IN THIS REPORT

EXECUTIVE SUMMARY

Phishing and ransomware are serious problems that can steal or disable access to corporate or personal finances, sensitive employee data, patient data, intellectual property, employee files and other valuable content. Both ransomware and phishing attacks and their variants – spearphishing/ whaling and CEO Fraud/Business Email Compromise (BEC) – are increasingly common and are having devastating impacts on businesses of all sizes. The financial impact of cybercrime in general – and phishing and ransomware in particular – is hard to assess for a variety of reasons, but the FBI estimates that ransomware alone cost organizations $209 million in just the first three months of 2016[i].

Phishing and ransomware are critical problems that every organization must address and through a variety of means: user education, security solutions, vulnerability analysis, threat intelligence, good backup processes, and even common sense. The good news is that there is much that organizations can do to protect themselves, their data, their employees and their customers.

ABOUT THIS INDUSTRY SURVEY REPORT

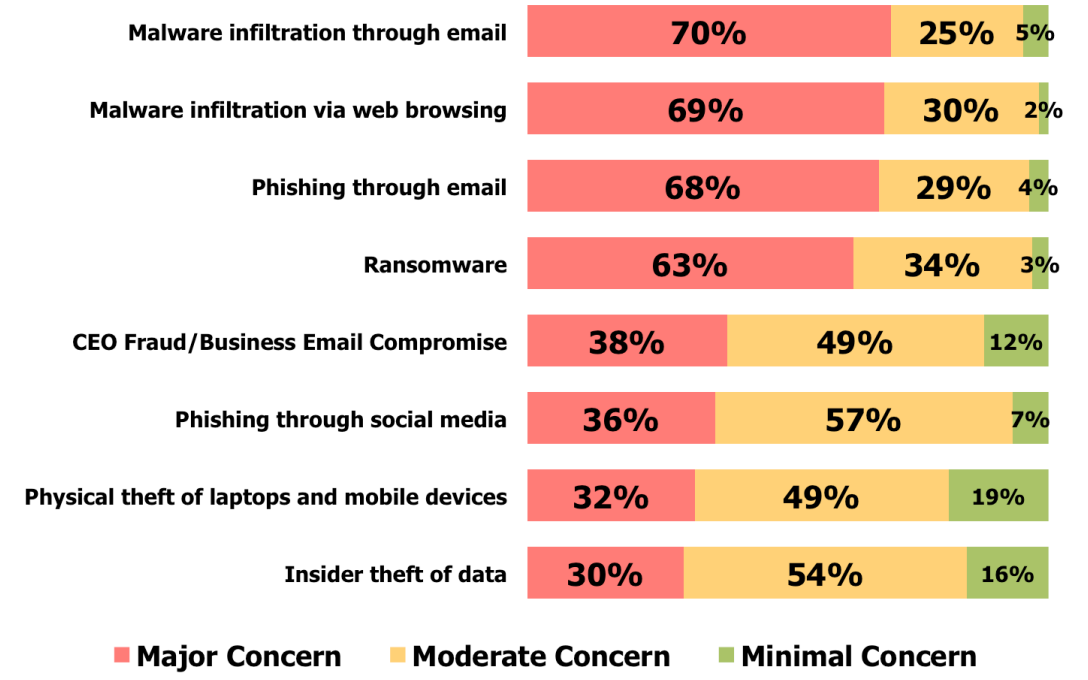
This survey report presents the results of a primary market research survey conducted with members of the Osterman Research survey panel during August 2016. The surveys were conducted with 162 members of the panel, primarily in North America. Here are the key details of the surveys:

- Mean number of employees at the organizations surveyed: 16,313
- Mean number of email users at the organizations surveyed: 14,161

A wide range of industries was represented among the organizations surveyed for this report.

SURVEY FINDINGS

Figure 1
Concerns About Key Security Issues



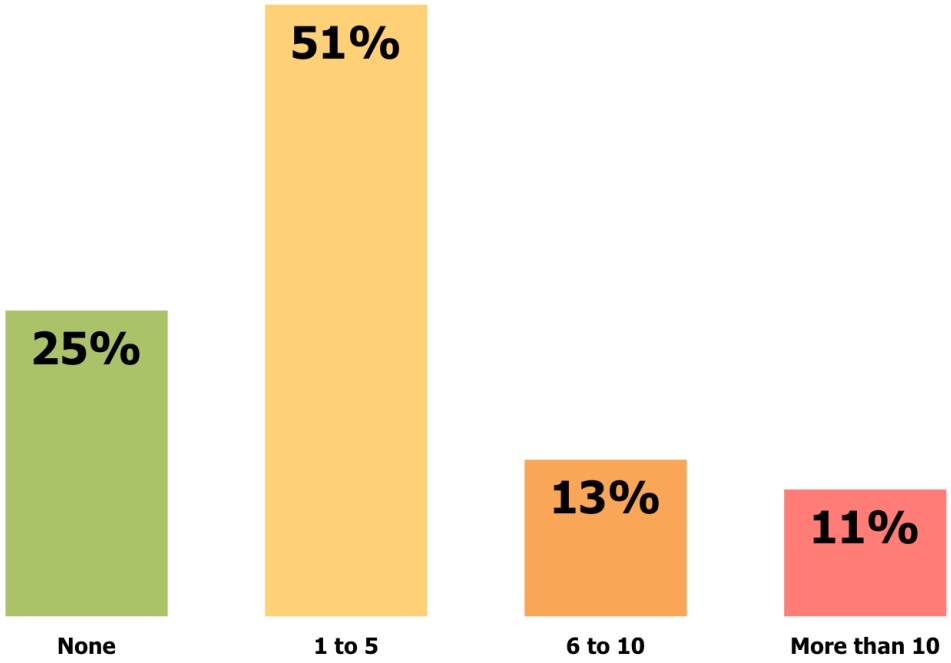
Source: Osterman Research, Inc.

Figure 2
Security Problems That Have Occurred During the Previous 12 Months

Security Problem	%
An email phishing attack was successful in infiltrating our network	34%
One or more of our endpoints had files encrypted because of a successful ransomware attack	30%
Malware has infiltrated our network, but we are uncertain through which channel	29%
Sensitive/confidential info was accidentally or maliciously leaked through email	17%
An email spearphishing attack was successful in infecting one or more senior executives	14%
Our network was successfully infiltrated through a drive-by attack from employee Web surfing	12%
An email as part of a CEO Fraud/Business Email Compromise attack successfully tricked someone in our organization	11%
Sensitive/confidential info was accidentally or maliciously leaked through a cloud-based tool like Dropbox	5%
Sensitive/confidential info was accidentally or maliciously leaked through a social media application	3%
Sensitive/confidential info was accidentally or maliciously leaked, but how it happened is not certain	1%
None of these things happened	27%

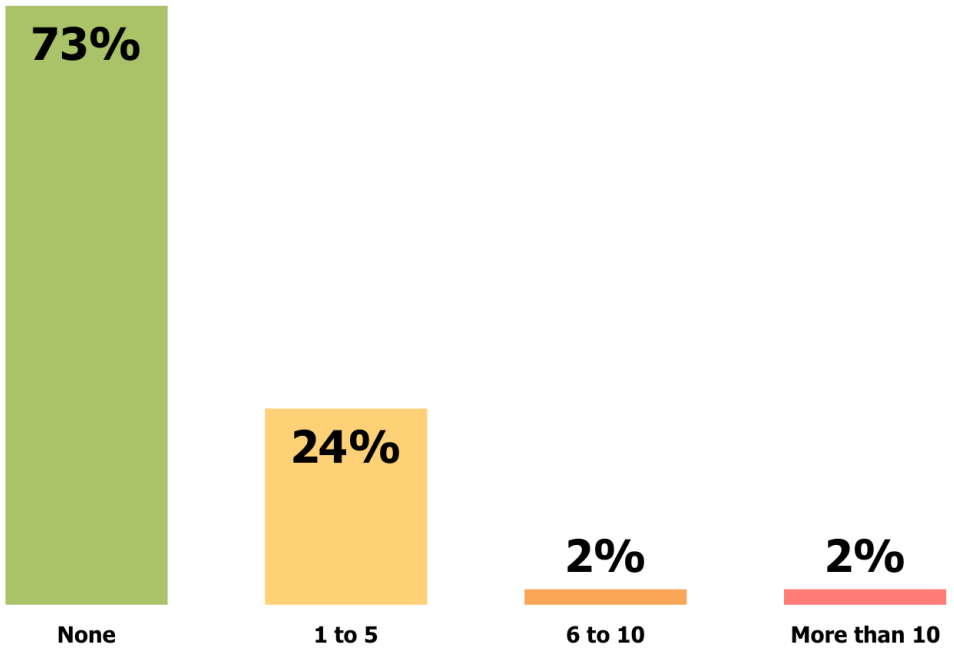
Source: Osterman Research, Inc.

Figure 3
Number of Times That Organizations Have Been Infiltrated by Ransomware, Malware, a Hacker, etc. Because an Employee Clicked on a Phishing Link or Attachment During the Past Year



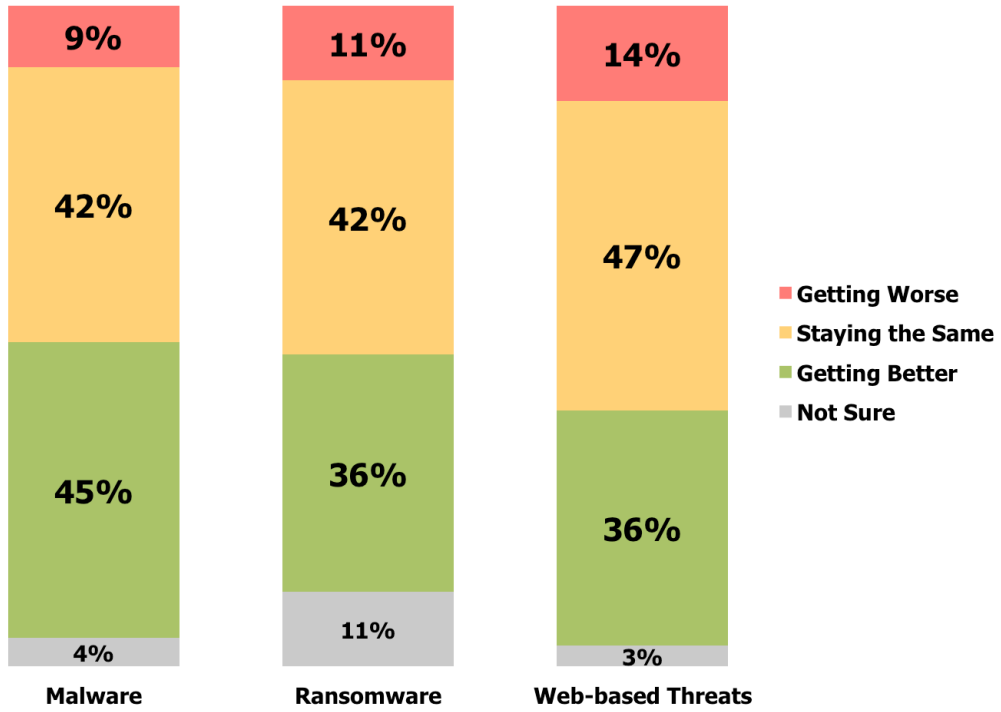
Source: Osterman Research, Inc.

Figure 4
Number of Times That Organizations Have Been the Victim of a CEO Fraud/Business Email Compromise Attack During the Past Year



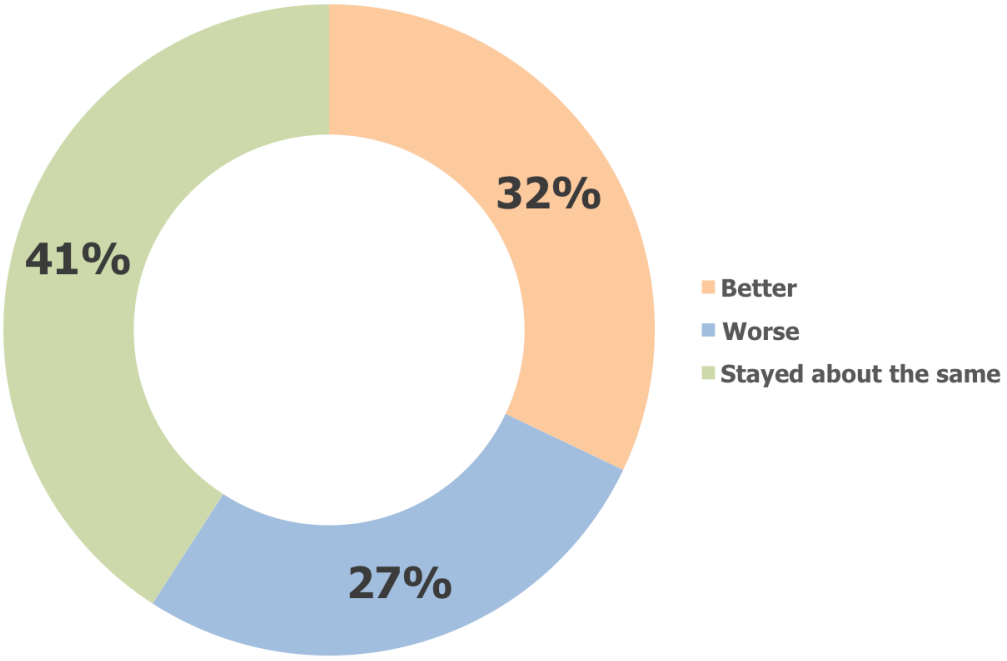
Source: Osterman Research, Inc.

Figure 5
"Is the percentage of malware, ransomware and Web-based threats blocked by your security infrastructure getting better, worse or staying the same over time?"



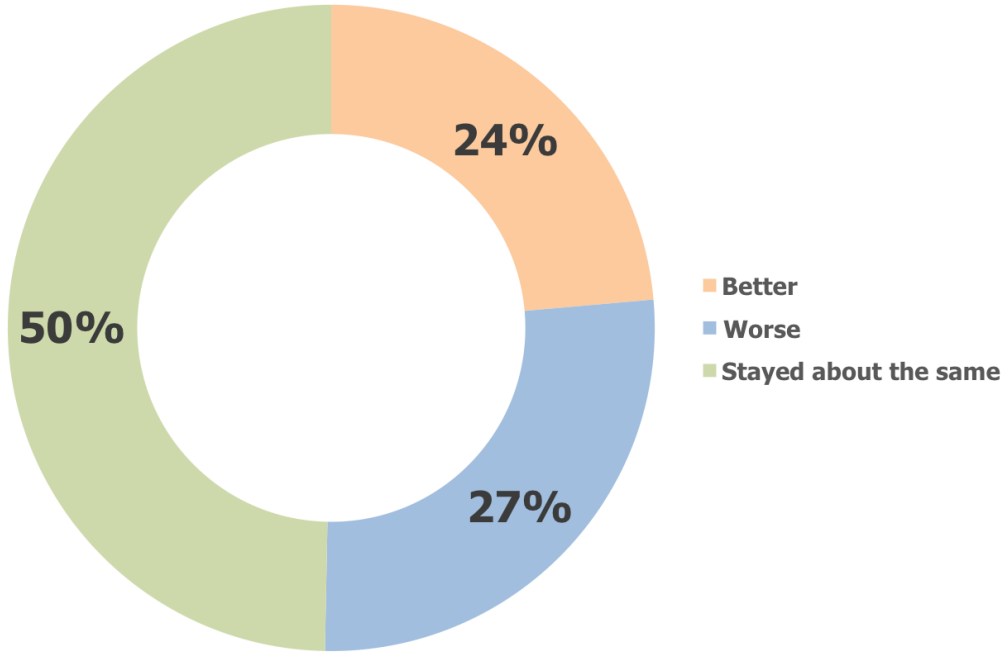
Source: Osterman Research, Inc.

Figure 6
"Over the past year, would you say that the phishing problem you experience has gotten better, worse or stayed about the same?"



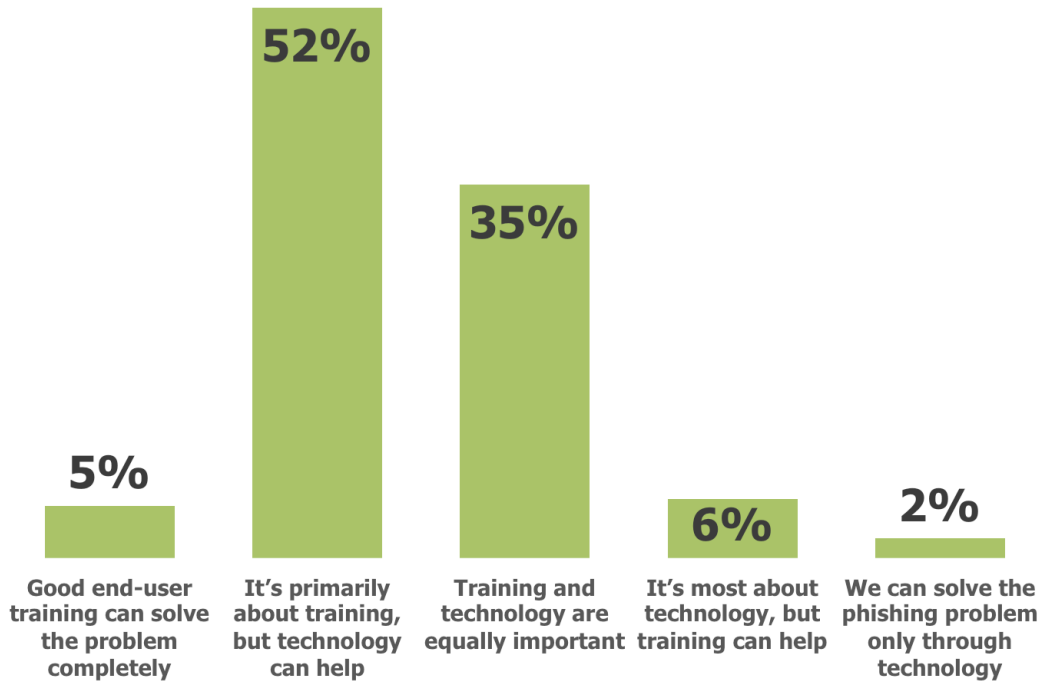
Source: Osterman Research, Inc.

Figure 7
"Over the past year, would you say that the ransomware problem you experience has gotten better, worse or stayed about the same?"



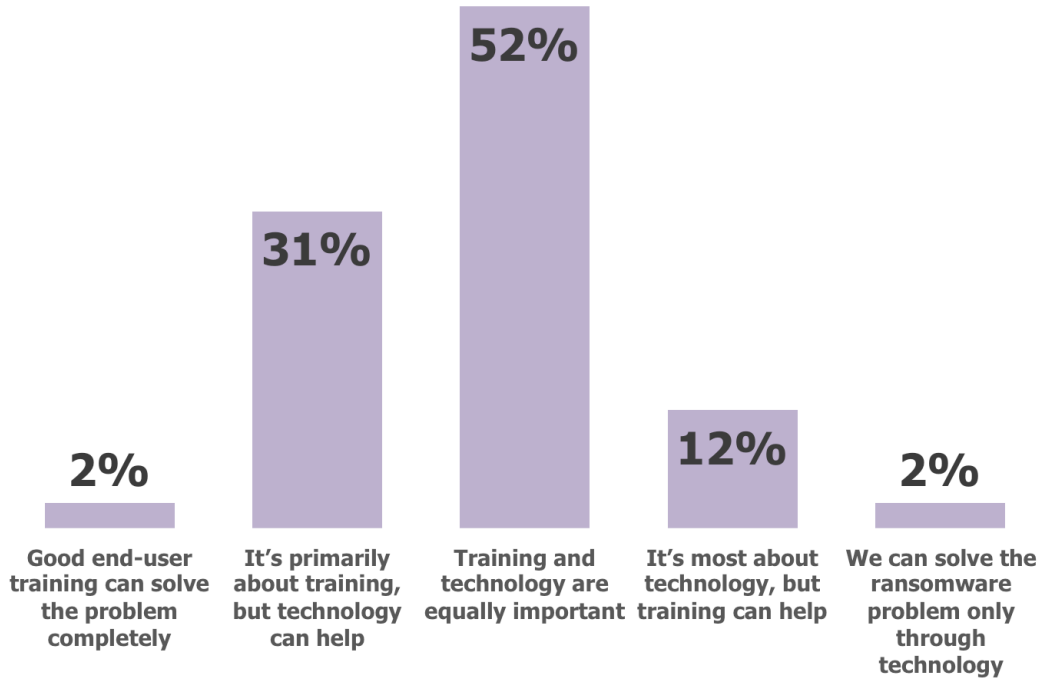
Source: Osterman Research, Inc.

Figure 8
Extent to Which Security Professionals Believe that Solving the Phishing Problem is a Training vs. Technology Issue



Source: Osterman Research, Inc.

Figure 9
Extent to Which Security Professionals Believe that Solving the Ransomware Problem is a Training vs. Technology Issue



Source: Osterman Research, Inc.

Figure 10
Perceived Effectiveness of Organizational Effectiveness Against Various Threats
Percentage Responding Good or Excellent

Issue	Poor	Moderate	Well or Excellent
Training end users on detecting and dealing with ransomware	13%	61%	27%
Training end users on detecting and dealing with phishing threats	9%	55%	37%
Training end users on best practices when surfing the Web	9%	63%	28%
Training end users on detecting and dealing with CEO Fraud/Business Email Compromise	9%	58%	33%
Preventing users' personally owned mobile devices from introducing malware into the corporate network	9%	48%	43%
Preventing data loss via email or the Web	8%	57%	36%
Eliminating ransomware before it reaches end users	1%	49%	50%
Eliminating spam before it reaches end users	0%	43%	58%
Eliminating malware before it reaches end users	0%	44%	56%

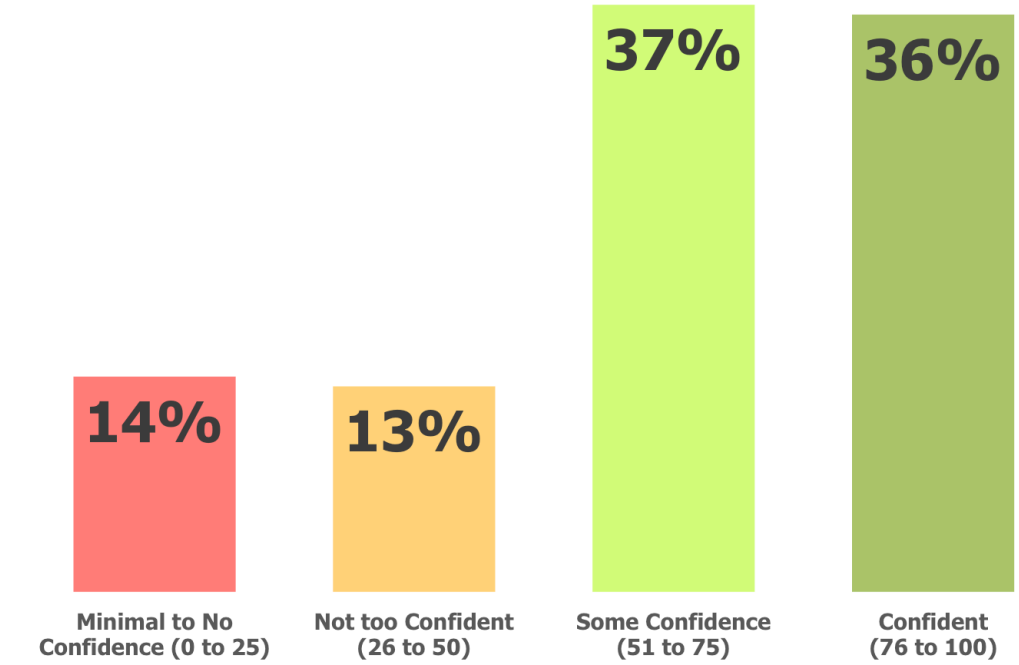
Source: Osterman Research, Inc.

Figure 11
Approaches That Organizations Use for Security Awareness Training

Issue	Commonly Used	Occasionally Used	Never Used
The Break Room Approach: We gather employees for a lunch or special meeting and tell them what to avoid when surfing the Web, in emails from unknown sources, etc.	23%	44%	33%
The Monthly Security Video Approach: We have employees view short security awareness training videos to learn how to keep the network and organization safe and secure.	22%	33%	46%
The Phishing Test Approach: We pre-select certain employees, send them a simulated phishing attack, and then see if they fall prey to the phishing attack.	19%	30%	51%
The Do Nothing Approach: We don't really do security awareness training.	16%	21%	63%
The Human Firewall Approach: We test everyone in the organization, find the percentage of employees who are prone to phishing attacks, and then train everyone on major attack vectors, sending simulated phishing attacks on a regular basis.	14%	19%	67%

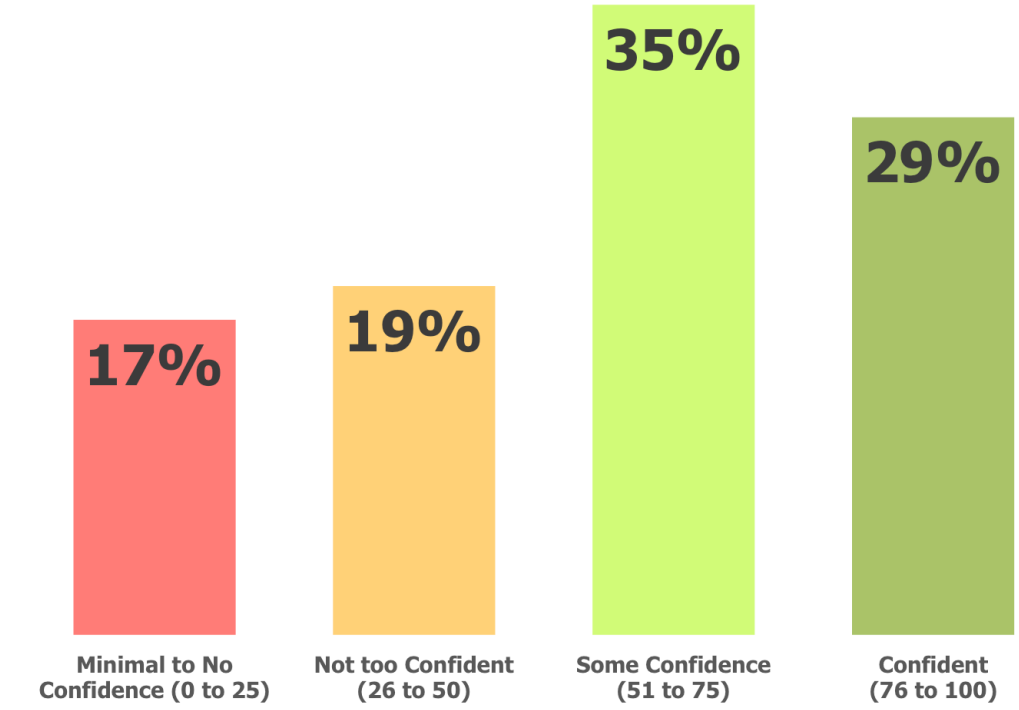
Source: Osterman Research, Inc.

Figure 12
Security Professionals' Confidence That Employees are Well-Trained to Deal With Phishing Attacks



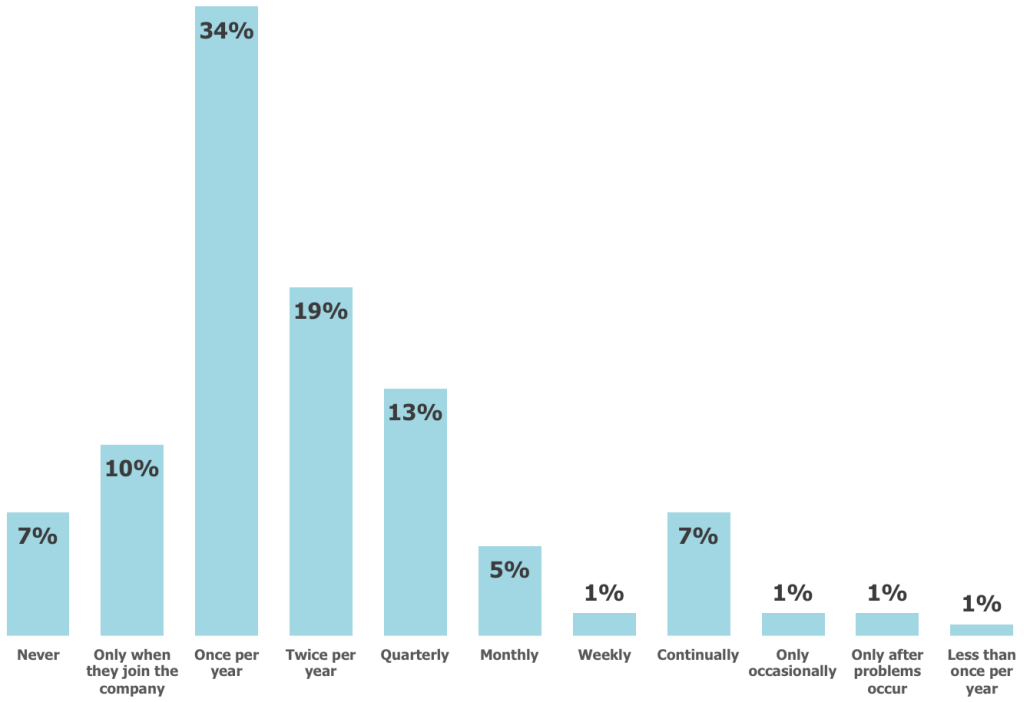
Source: Osterman Research, Inc.

Figure 13
Security Professionals' Confidence That Employees are Well-Trained to Deal With Ransomware Attacks



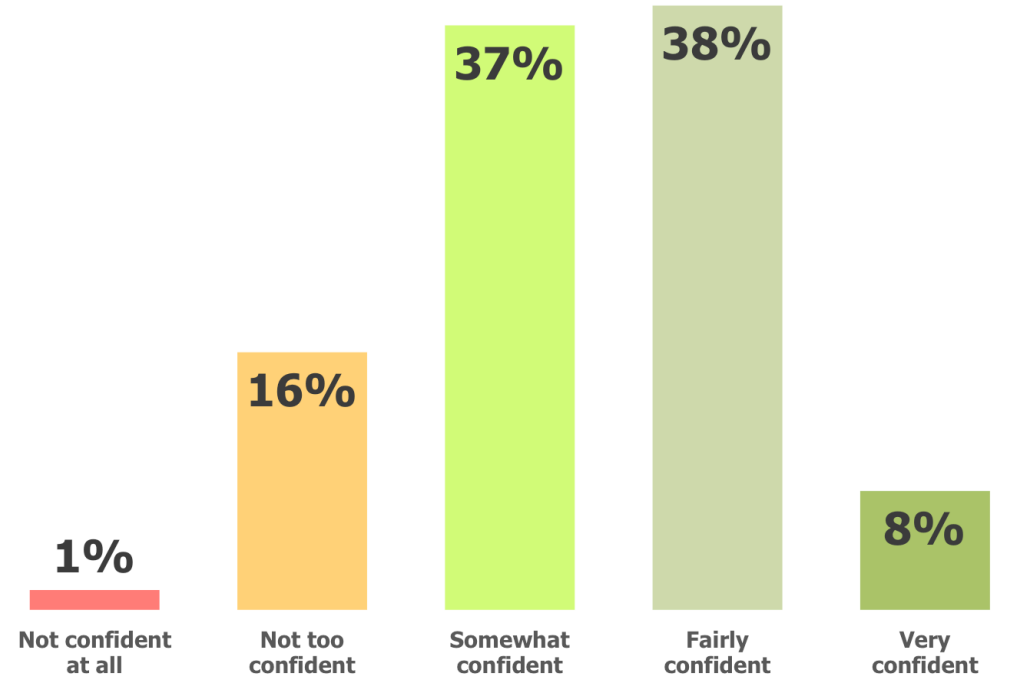
Source: Osterman Research, Inc.

Figure 14
Frequency With Which Employees are Trained on Security Awareness



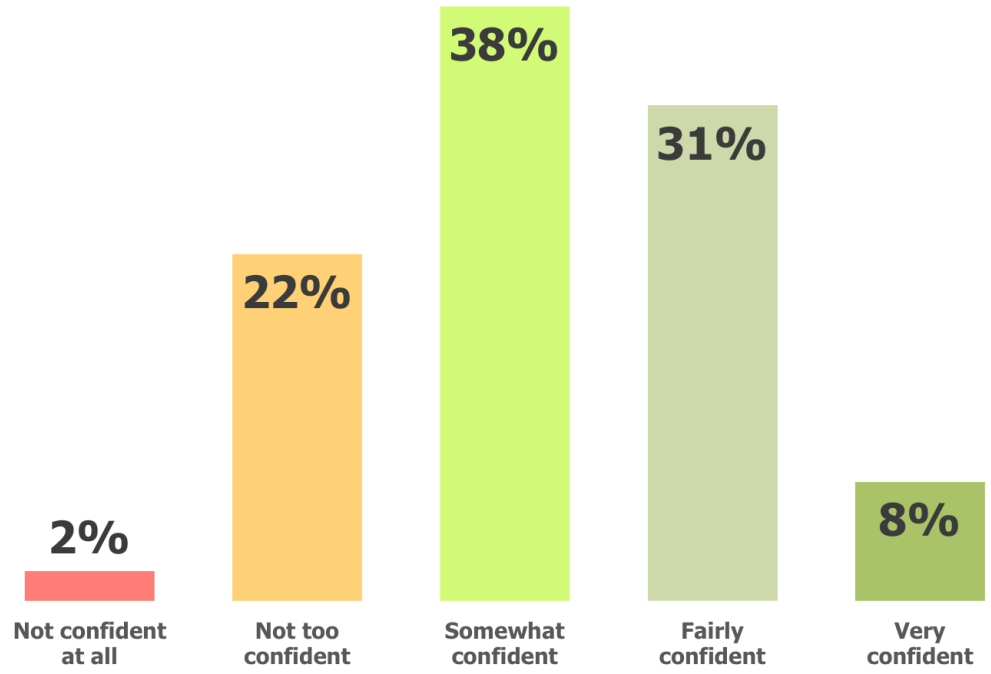
Source: Osterman Research, Inc.

Figure 15
Security Professionals' Confidence That Their Organizations Can Stop Phishing Attacks



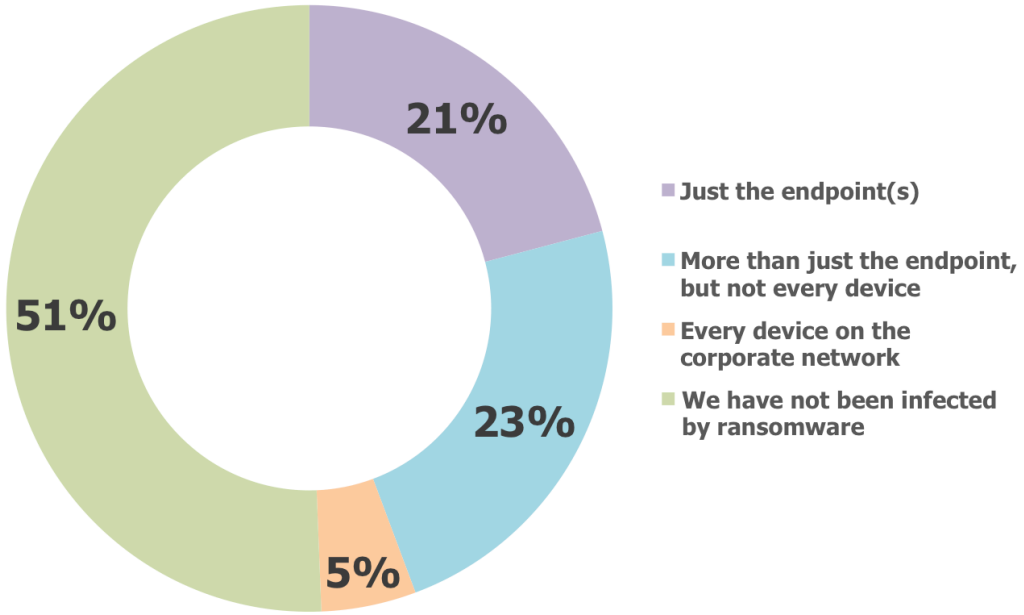
Source: Osterman Research, Inc.

Figure 16
Security Professionals' Confidence That Their Organizations Can Stop Ransomware Attacks



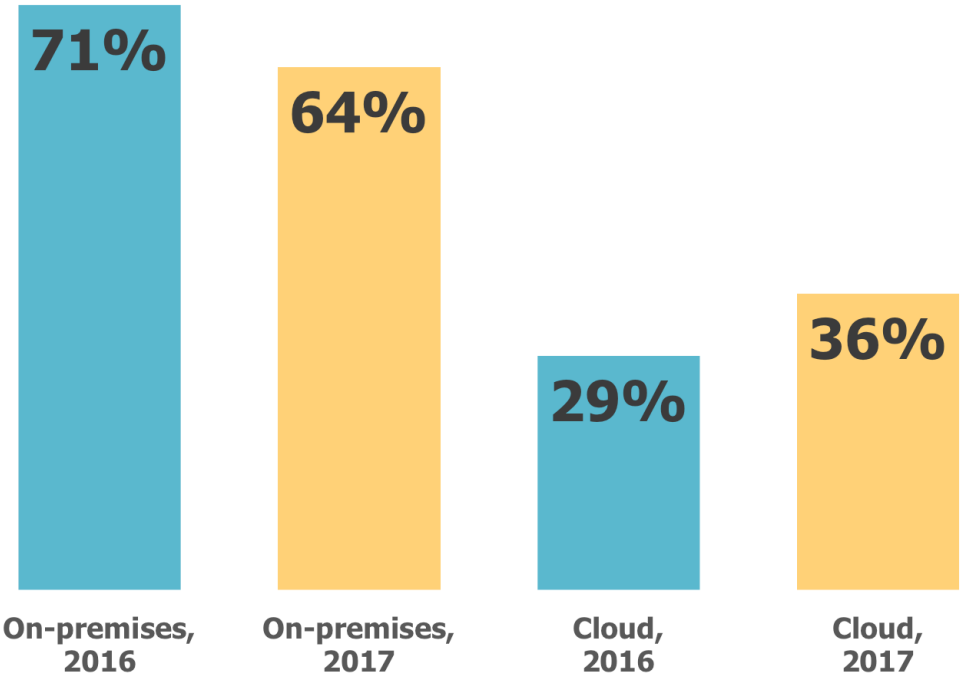
Source: Osterman Research, Inc.

Figure 17
Impact of the Most Recent Ransomware Attack



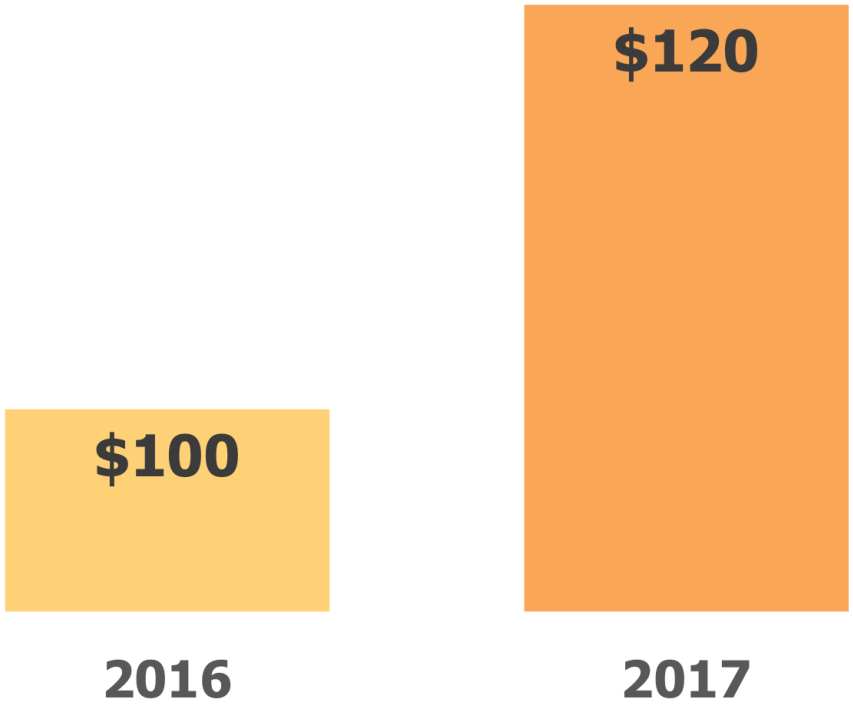
Source: Osterman Research, Inc.

Figure 18
On-Premises and Cloud Security Budgets, 2016 and 2017



Source: Osterman Research, Inc.

Figure 19
Median Security Budget per Employee, 2016 and 2017



Source: Osterman Research, Inc.

[i] http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/