What Constitutes Effective Security Awareness Training?

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for KnowBe4

May 2016

EMA™

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

What Constitutes Effective Security Awareness Training?

Introduction

Employees are a critical part of an organization's defense against many IT security threats. Just as having the correct technology solutions is important, training personnel to recognize security threats is a critical part of any security strategy. As part of that strategy, organizations must consider both the content and the training methods. Training that does not engage employees or provide for continuous learning and reinforcement is not sufficient to truly make employees more security aware.

Security Awareness Programs Have a lot to Learn

A recently changing trend, and an encouraging sign, is that many companies are recognizing the critical need for employee security awareness. In 2014, EMA conducted a security research study that showed only 44% of respondents had security training from a current or previous employer. When the research was conducted again in 2015, 59% of respondents indicated they had received some form of security awareness training.

Not only are more employees being trained, but they are receiving more training. In a 2014 study, only 15% of respondents received five or more hours of security training. In 2015, that number jumped to 23%. This is also true with the periodicity of training. In 2014 only 2% of respondents indicated they had received training post incident, while in 2015 respondents who received training grew to 65%.

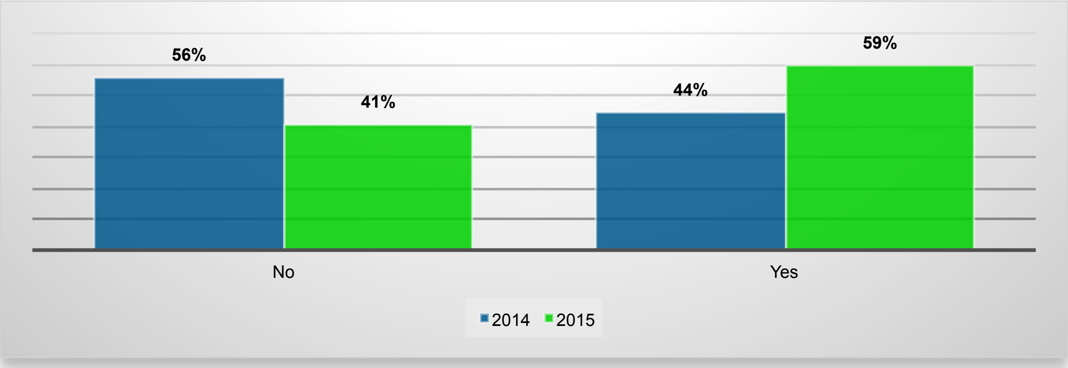

Figure 1a: Security Awareness Training 2014 vs. 2015

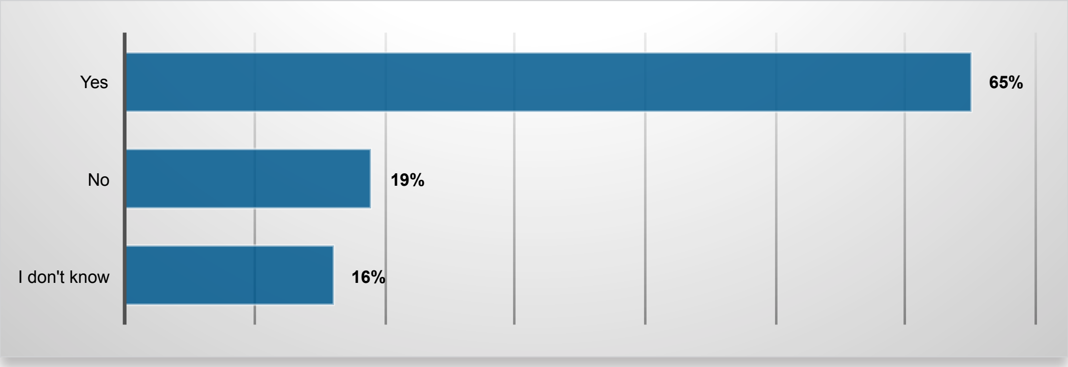

Figure 1b: Organizations Providing Post Incident Awareness Training

Interactive training methods are known to be far more effective at not only engaging attendees, but improving retention of content. These include programs that present employees with realistic content, security scenarios, and even simulated phishing attacks. These methods are also more continuous in nature. Rather than going to a lecture and forgetting it a week later, continuous training can be directed to present employees with shorter bursts of training at multiple points throughout the year.

Of course, the final piece to effective training is measuring success. Unfortunately, many security training programs still measure effectiveness through attendance. However, attendance cannot measure the most important factors, like how much an employee is actually retaining and changes in behavior that ultimately identify how much less likely they are to fall victim to an attack.

Interactive training methods are known to be far more effective at not only engaging attendees, but improving retention of content.

What is Effective Security Awareness Training?

Research proved that effective security training is a must. Certain methods are simply more effective than others, but what strategies are companies currently employing? KnowBe4 categorized training strategies into five approaches:

- **The Do Nothing Approach** - We do not really provide security awareness training.
- **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.
- **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.
- **The Phishing Test Approach** - We preselect certain employees, send them a simulated phishing attack, and see if they fall prey to the phishing attack.
- **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.

Forty-one percent of organizations are still doing nothing about security training. Of the companies that are providing security awareness training, almost 60% are using less effective methods such as the Break Room Approach (23%) and the Monthly Security Video Approach (36%). Thus, fully two-thirds of companies are using training methods that are less than ideal, and do not necessarily result in security awareness.

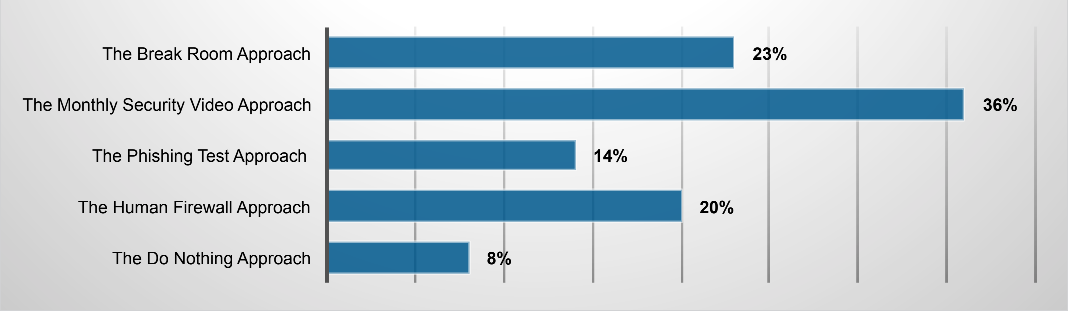

Figure 2: Organizational Approaches to Security Awareness Training

What Constitutes Effective Security Awareness Training?

These numbers demonstrate that despite the training program improvements, there is still significant room for growth in the more interactive, and thus more effective, methods. The Phishing Test Approach, which creates a simulated phishing attack, was employed by just 14% of companies. The Human Firewall Approach, which should really be the goal of a mature awareness program, was used in only 20% of companies that participated.

These results are surprisingly consistent across companies of all sizes and with a variety of employee roles. The results are also fairly consistent across industries. However, education shows a particular lack of more robust training, with no respondents indicating they use the Human Firewall Approach, and just 12% using simulated phishing options. Retail and wholesale organizations also seem to rely heavily on the Break Room Approach (33%) and Monthly Videos (44%) at the expense of more interactive training methods.

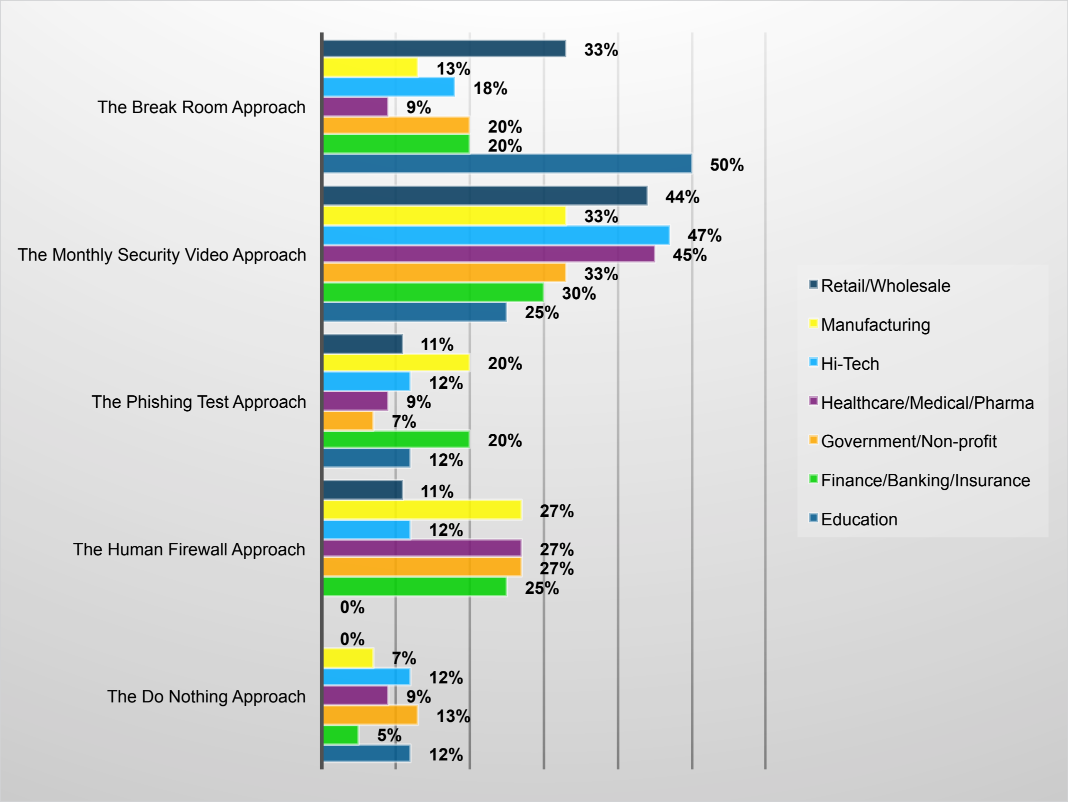

Figure 3: Approaches to Security Awareness Training by Industry

EMA Perspective

Does training lead to confidence that employees are, in fact, well trained against phishing attacks?

It comes back to the type of awareness training. As this paper indicated, the types of training that truly result in security awareness:

- involve interactive elements
- are continuous in nature, with regular follow-ups
- simulate real-life attacks
- have their effectiveness monitored

To achieve security awareness, and thus effective defense, companies must employ comprehensive, interactive training.

Research shows that most of the training employees receive does not offer simulated attacks, testing, or interactivity. The Break Room Approach and Monthly Security Video Approach are still more popular than the more effective training methods such as the Phishing Test Approach and Human Firewall Approach.

To achieve security awareness, and thus effective defense, companies must employ comprehensive, interactive training. This training must be updated regularly, and its effectiveness must be measured through strategies, or another word like employee susceptibility to attack, post incident follow up, and improvement tracking.

If a company is not taking these steps, its employees will not be security aware and the company certainly is not getting the most for its training dollar.

About KnowBe4

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach. This method integrates baseline testing using mock attacks, engaging interactive training, continuous assessment through simulated phishing, vishing and smishing attacks, and enterprise-strength reporting to build a more resilient organization with security top of mind. Thousands of organizations use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government, and insurance. To learn more visit www.KnowBe4.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3395.052316