EMA Report Summary: Security Awareness Training

Are We Getting Any Better at Organizational and Internet Security?

By David Monahan
An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) End-User Research Report

September 2015

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

2014 was dubbed "the year of the breach" as over a billion consumer records across nearly every industry vertical worldwide were exposed, costing billions of dollars in recovery costs and lost revenue for the affected organizations. Though this was a tough wake-up call, many organizations have seen that technology, though a necessary part of a security strategy, is not able to fully prevent breaches. They see that people are now most often the weakest link in security defense. At the same time, the old strategies of locking down everything so people cannot possibly cause a problem increases worker and business friction to a point that is unacceptable to both, putting security programs, and the security personnel, at risk. To achieve both security and usability, security teams must create a change in the mentality and even business culture that by making personnel more aware of and vigilant against the various attacks they face on a near daily basis.

For the 2015 *Security Awareness Training: Are We Getting Any Better at Organizational and Internet Security?* report, EMA surveyed nearly 600 people in North America across the small-to-medium businesses (SMB), midmarket, and enterprise spaces. Respondents represented line of business, IT, and security/fraud/risk across major verticals, including education, finance/banking/insurance, government/nonprofit, health care/medical/pharma, retail, and utilities/infrastructure.

The research revealed that a tremendous shift in awareness training programs has taken place, especially across the previously underserved SMB space. While in 2014 56% of individuals reported they had not received any training from their organizations, in 2015, 59% indicated they had now received some level of training. Many positive trends continued in the research showing the following.

- Training content is becoming more accessible to organizations of all sizes from both a delivery and cost perspective.
- Programs are becoming more effective and have better measurement and management capabilities.
- Due to training, employees are better at recognizing various forms of social engineering.
- Trained personnel recognize that they make better security choices at home as well as at work, further increasing the value of training.

Through awareness, as a collective corporate and Internet populace we are becoming more diligent in detecting and avoiding compromise by social engineering methods, especially phishing attacks. However, attackers are constantly honing their skills and adapting their attack methods. Only through continued diligence and expansion can we be successful in the long run. Program content and delivery must change to include new attack methods and programs must continue to expand to train the other 41% that have not received training as of yet.

Demographics and Budgets

Industry Vertical, Size, Role, and Age

Numerous verticals were represented in the research. The diversity of the respondents in the industry verticals rendered a number of interesting trends and changes that will be brought out during the course of the report. The "Others" category includes legal, hospitality, advertising, marketing, media, and those who identified their industry as "other."

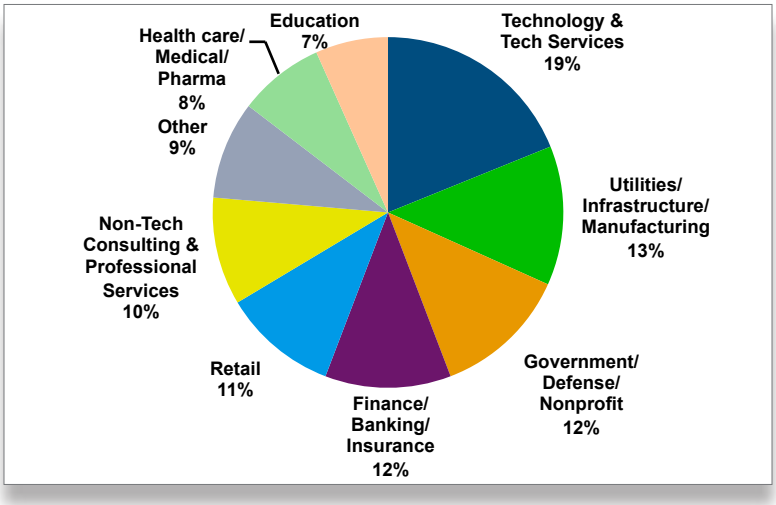

Figure 1. Respondents by Industry Vertical

Organization size was also collected and used in the analysis. In this year's report, the breakout for the three primary categories was larger for the enterprise and SMB spaces and slightly narrower for the midmarket space. In the 2014 report, midmarket was referred to as SME. (In this year's report, EMA replaced the SME nomenclature with the midmarket nomenclature.) With the volume of respondents, the division between the organizational sizes was nearly optimal for addressing organizations by staff size. This was very helpful when analyzing the data by organization size.

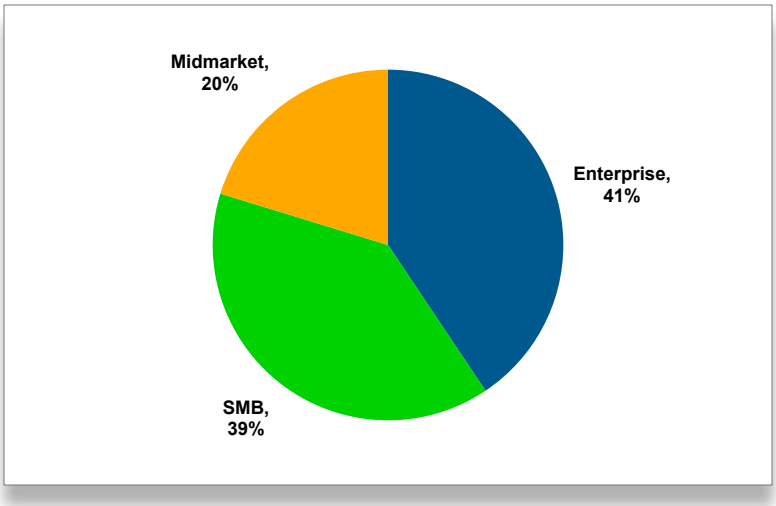

Figure 2. Respondents by Organization Size

This question shows a good global diversity for the respondents, providing a wider insight than expected. Geographical distribution for the research respondents was North America. Interestingly though, when asked where their company operated, many respondents reported a wider spread. The study population was not large enough to provide statistically relevant samples on all responses, but it did provide a relevant sample size for some questions and good indicators for others that lend to some insights.

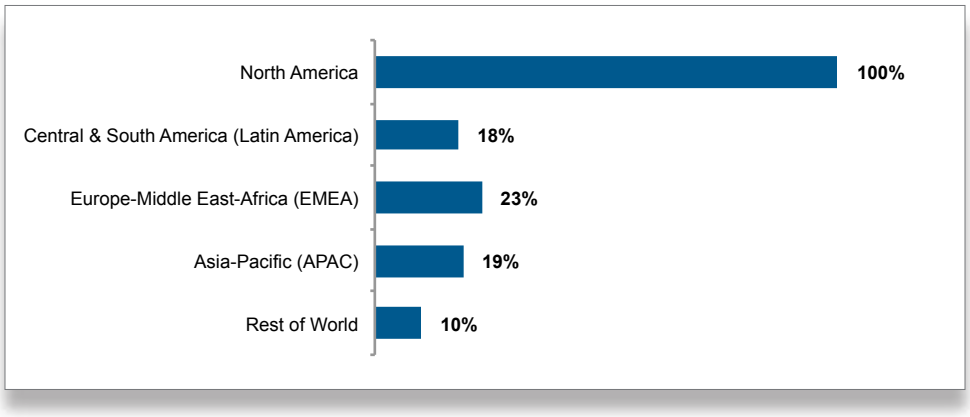

Figure 3. Respondents' Organizations by Operating Geography

Roles

Participant roles were used often in the report for analyzing responses. One of the research project's goals was to understand how respondent's roles within the organization affected both the training they received and their perception of the training. This break out provided excellent perspective across numerous questions.

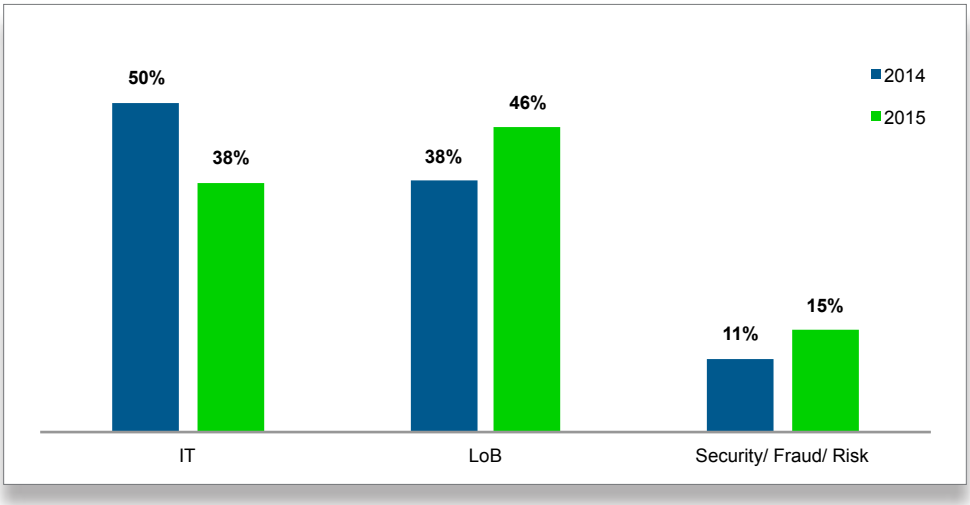

Figure 4. 2014 vs. 2015 Respondents' Organizations by Respondent's Business Role

EMA found that the respondents in the 2015 report were more diverse among the three target roles desired. This year the number of IT respondents was down to 38% from 50% in 2014 with a corresponding rise in the line of business- (LoB) and security-focused respondents.

Age

Another aspect of training that is very germane is preferences and perspective by age. Development and education experts have documented that age is a key factor in learning as it affects the plasticity of the brain and experience gained over time dramatically affects perspective.

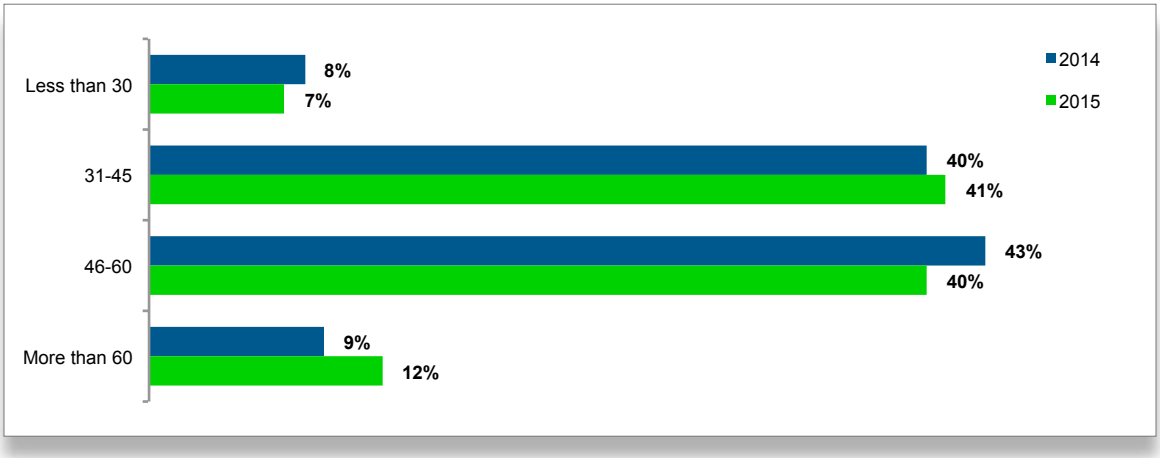

Figure 5. 2014 vs. 2015 Respondents' Ages

Revenue

Revenues for the 2015 study rounded off a little from last year. Overall, they were up and shaped like a more round bell curve. Last year's spike of $1 billion dollars or more was reduced with virtually all of the lesser revenue numbers correspondingly increasing. This was due, at least in part, to fewer very large enterprises of over 20,000 personnel taking part in the survey.

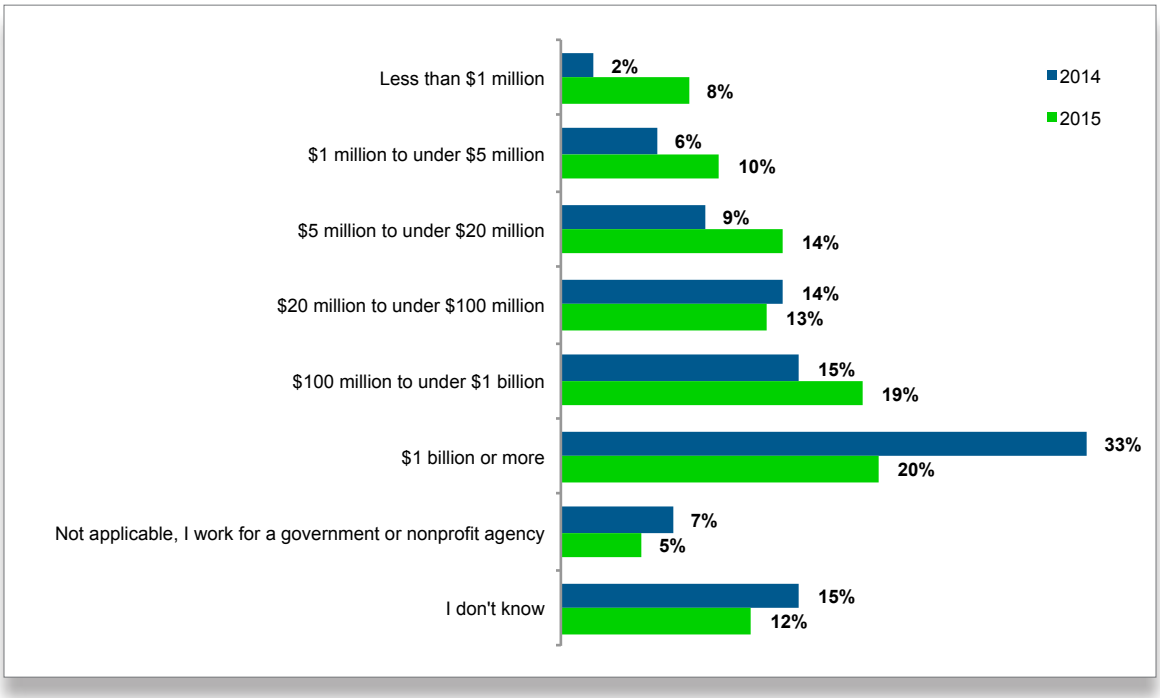

Figure 6. 2014 vs. 2015 Annual Revenue

Research Findings

Budgets and Funding

Participants were asked how their security awareness programs were funded. In the aggregate numbers, respondents indicated that the security group funded projects 35% of the time while their own direct line management funded the awareness training 33% of the time. This is a significant change from historical information. Traditionally, the direct organizations had more budget responsibility for providing training but now other organizations are defraying the cost. This may also account for the dramatic increase in training.

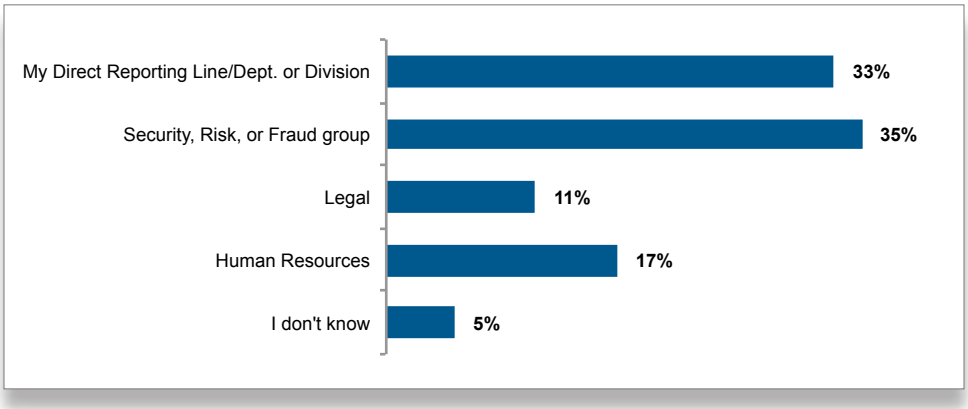

Figure 7. 2015 Organizational Funding of Security Awareness Training

Trained or Not Trained? That Is the Question!

In the 2014 study, 56% of the respondents said they had not been trained. When broken out by organization size and role, the research identified, not unexpectedly, that significantly more of the **SMB** respondents (72%) had not received training than midmarket or enterprise respondents. The research also identified that 56% of the **Line of Business** respondents were not trained, which was significantly higher than the 35% of **IT** personnel and the 8% of **Security** personnel that had not received awareness training.

One of the colloquial definitions of insanity is "repeating the same thing and expecting a different result." Fortunately, organizations seem to be coming out of that mentality when it comes to security awareness training and data loss. Last year's report seemed to be the catalyst for a significant spike in the tech-sector media attention on security awareness. In addition to the attention on the lack of awareness training being provided, 2014 had the highest number of noted data records exposed due to breaches ever seen. This seems to have been the wake-up call for many organizations. There are now significant and measureable costs from having a data breach and the costs increase when the plaintiffs can prove lack of due diligence, which can be considered part of security awareness training.

The most startling and positive turnaround from this year's report is the change in the percentage of respondents that indicated they had become trained. Of the nearly 600 respondents, 59% said they had received some form of security awareness training from their employer, making this year's report a 180 degree turn around from last year. The SMB space saw an 84%. Increase in trained respondents, making it by far the largest gainer of the three segments.

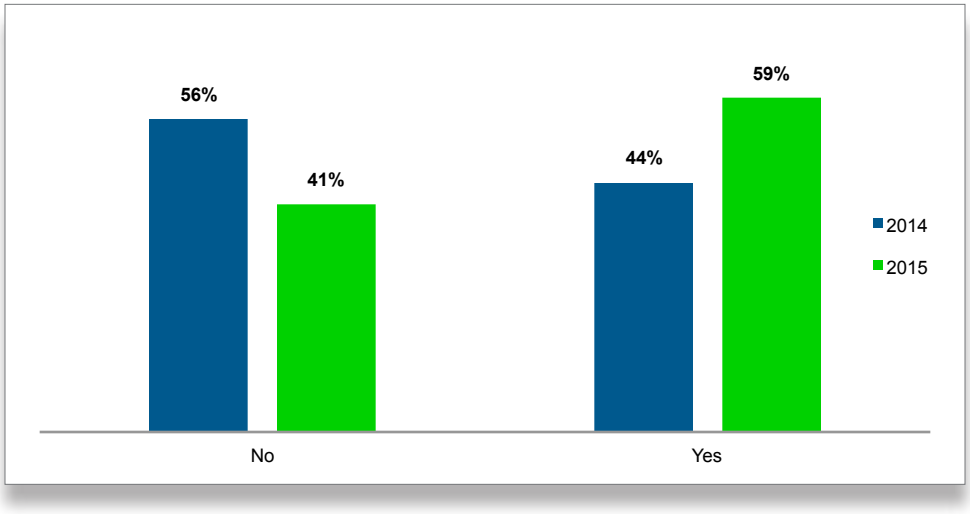

Figure 8. 2014 vs. 2015 Percent of Respondents Trained

Key Security Topics

Recipients reinforced the need for awareness training in their perception of its overall impact to their choices. One way this was expressed was respondents' understanding that the security awareness training they received at work positively influenced their security decisions at home. This perception increased a point and, though this is not statistically significant in this situation, the fact that it is a high percentage is encouraging.

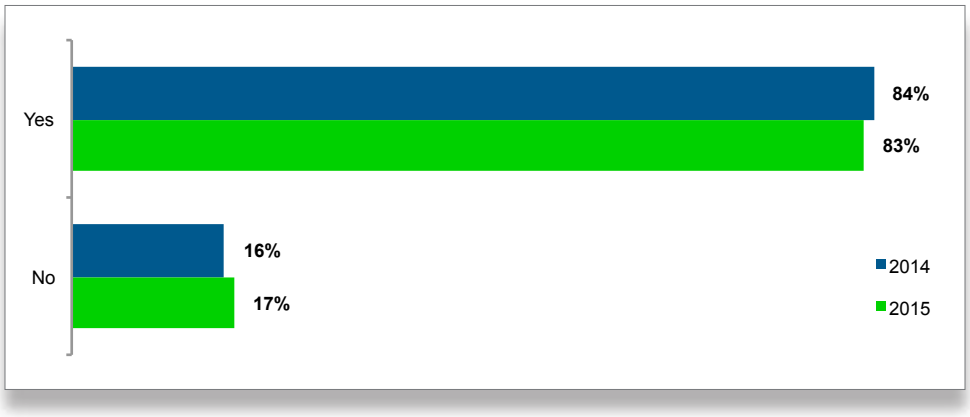

Figure 9. 2014 vs. 2015 Awareness Training at Work's Influence on Security Decisions at Home

Respondents were provided a list of seventeen security topics and asked to identify the topics on which they had received training, and also, which topics they felt were most important for maintaining security within their organizations and which they thought would have the largest impact should they be violated. Respondents overwhelmingly identified email and phishing security as their most trained topic. This makes perfect sense in most environments since email is the primary window into an organization from the outside world.

EMA compared the 2014 results with the 2015 results and found that privacy had the highest jump, rising 10 points from 58 to 68%, while physical/office security had the largest decline, dropping 10

points from 51 to 41%. This also stands to reason because, although physical security is important, possession being nine-tenths of the law, with some budget constraints and the large attention on cyber breaches rather than physical breaches, organizations were bound to shift focus.

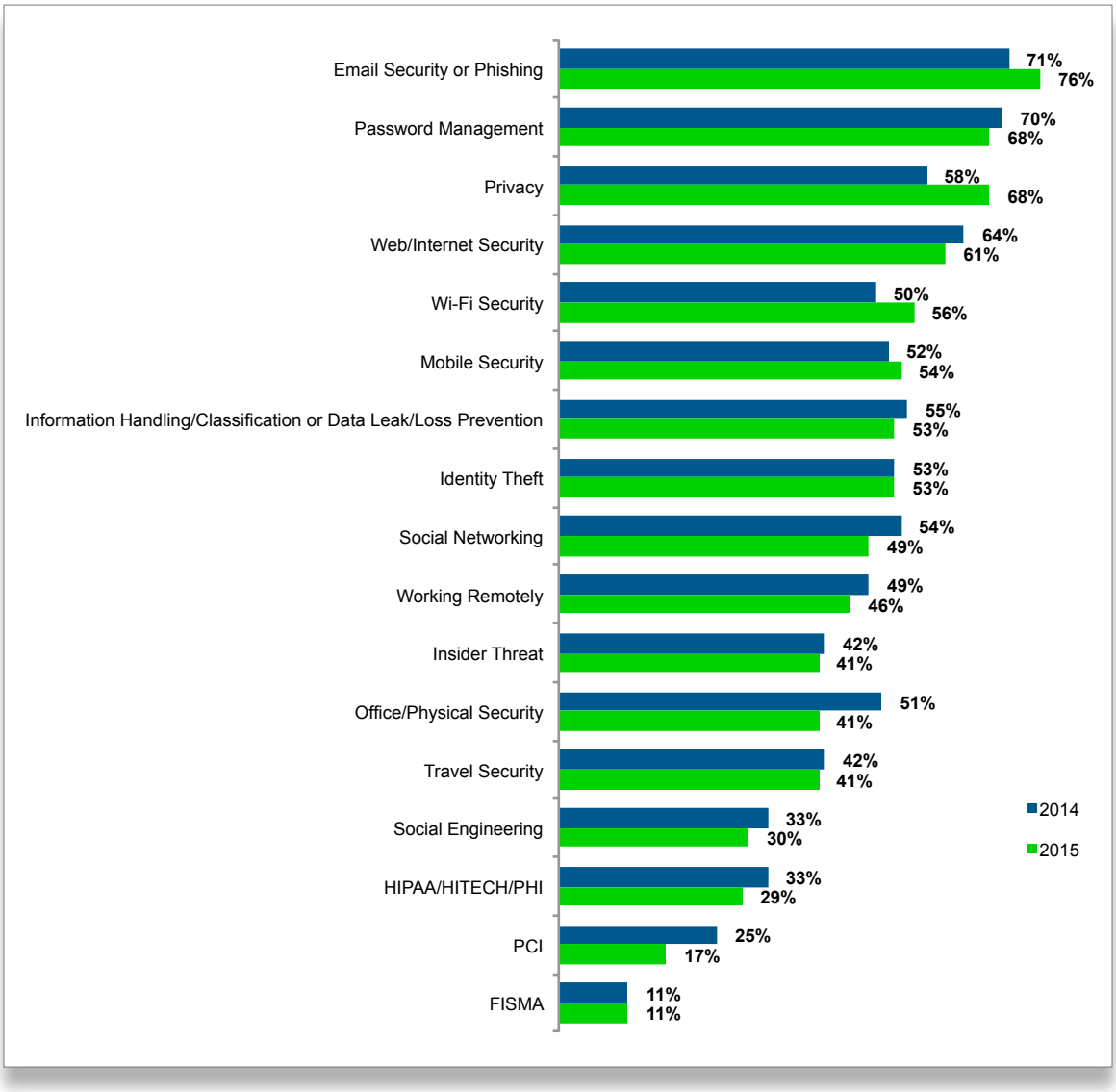

Figure 10. 2015 Areas of Security Awareness Training Received

In comparing the most trained topics with those that were perceived as most important to protecting the organization and those perceived as the largest threat if breached, the good news is that there was far more consistency this year than in 2014.

In 2014, the top five security topics for awareness training in 2014 were **Email/Phishing Security**, **Password Management**, **Web/Internet Security**, **Office/Physical Security**, and **Privacy**.

The top five training topics perceived by respondents to be most important for security in 2014 were Information Classification/Handling and Leak Prevention, Web/Internet Security, Email Security/Phishing, HIPAA/HITECH/PHI, and Password Management. The two years had strong overlap, but also had some noticeable differences.

Evaluating the training areas identified, EMA found an inconsistency in what businesses identify as most important and provide training for, and what employees see as the greatest threat to the organization. Both perspectives were valid, but the divergence was pointed out as a possible issue to address. It appears that organizations took the opportunity to understand those differences and have begun addressing them. Though not totally aligned yet, which may be an impossibility based on changes in perception and attack vectors and the resulting perception, they are tighter than the 2014 study.

All Areas (Alphabetical)	Top 5 Training Topics	Top 5 Most Important	Top 5 Perceived Threat Areas
Information handling/ classification or data leak/ loss prevention	Email security or phishing	Information handling/ classification or data leak/ loss prevention	Information handling/ classification or data leak/ loss prevention
Email security or phishing	Password management	Email security or phishing	Email security or phishing
HIPAA/HITECH/PHI	Privacy	Web/internet security	Web/internet security
Identity theft	Web/internet security	HIPAA/HITECH/PHI	Identity theft
Insider threat	Wi-Fi security	Privacy	Password management
Mobile security			
Office/physical security (securing doors, windows and items)			
Password management			
PCI			
Privacy			
Social engineering			
Social networking			
Travel security			
Web/Internet security			
Wi-Fi security			
Working remotely			

Figure 11. 2015 Top 5 Training Topics vs. Top 5 Perceived Most Important vs. Top 5 Largest Perceived Threat Areas

In reviewing the figure above, it is important to note the full impact of what it is depicting. A match in column 1 and column 2 means organizations understand where the largest training gaps for employees are. A match in column 2 and column 3 means the training participants perceive as the most needed align well with the business areas that have the greatest impacts. A match in column 1 and 3 means that the organization are applying training to the largest risk areas. However, the issue there is the program owners have not necessarily aligned the training to the areas where personnel believe they have the greatest knowledge gap. This means the actual exposure may be greater in certain areas because of the gap in knowledge and real exposure rather than the overall possible exposure. The most significant example of this gap is information handling and classification. It was seventh in rank for training received but first in rank by respondents in terms of what they perceived as most needed, and if done improperly, most impactful.

Training Attributes

Hours of Training Required per Year

Once again, organizations responded positively to the need for training. Not only are more individuals trained, but more training hours are being required. There was significant movement in the number of hours per person, both in aggregate and across numerous industry verticals. Thirty-three percent of the respondents indicated the amount of time they spend in awareness training per year is still between one and three hours per year, keeping it in the top single time block. However, depending upon how that training is delivered and the delivery interval, that could still be low. Though that block dropped in prevalence by two points from 2014, the real change was in the greater than five hour block. Twenty-three percent of respondents said they now get greater than five hours of awareness training per year, pushing it into a strong second place. That is eight points or 53% higher than 2014.

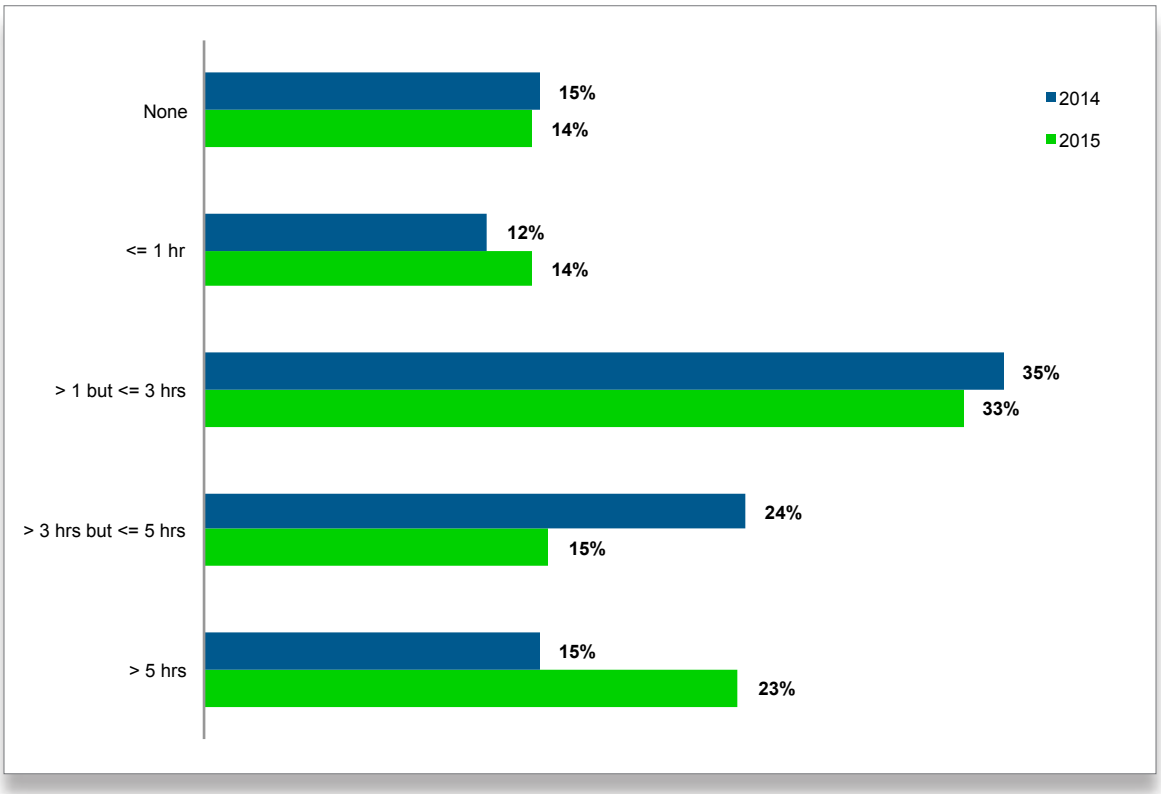

Figure 12. 2014 vs. 2015 Hours of Training Required

Training Measurement

Another significant gain between 2014 and 2015 is measurement of the effectiveness of awareness training. Fifty percent more respondents reported that their organizations were measuring the awareness training effectiveness, moving the needle from 48 to 64%. This was a point brought out in last year's reports as a recommended improvement for a much needed gain both from the respect of measurement and communication of measurement. It is a safe bet to make the assumption that most of the gains came from the communication of training being measured, but given the lack of a direct historical comparative question, there is no way to truly tell. Whether from new programs or just from an improvement in communication, organizations are making progress. As the old saying goes, we cannot improve what we do not measure. This is just as true for security awareness as it is for other areas of the business.

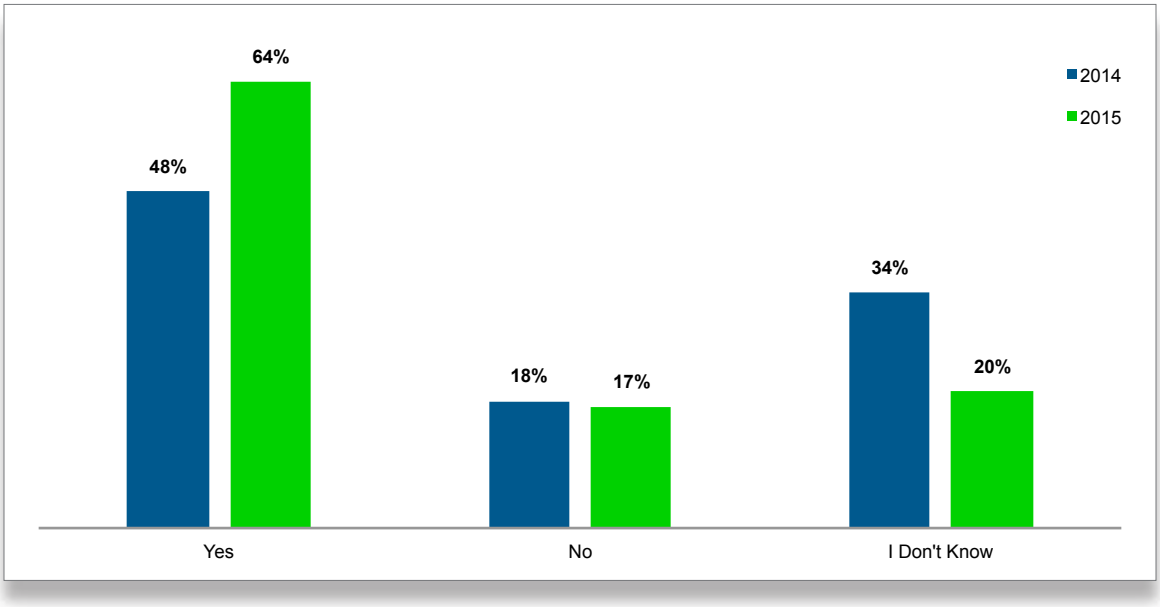

Figure 13. 2014 vs. 2015 Measuring Awareness Training Effectiveness

Though the reduction from 52 to 37% for organizations that either do not have measurement systems in place or are not communicating how they are measuring them is good, that percentage is still far too high. The organizations that are depending on security awareness training but are not measuring its effectiveness have no quantitative way to assess if their training dollars are well spent, or if training is making a difference in reducing the risk exposure within their workforce. Having poor or nonexistent measurements also leaves program managers without the data they need to garner continued investment in the program.

Training Effectiveness

Participants were queried on the effectiveness of the security awareness training they received. The most surprising result was the data returned was virtually identical to the 2014 study. In 2014, 67% of the respondents rated their training as **Above average** to **Highly effective**. In 2015, 69% provided the same ratings. In both cases, none of the respondents rated their training as **Not effective**.

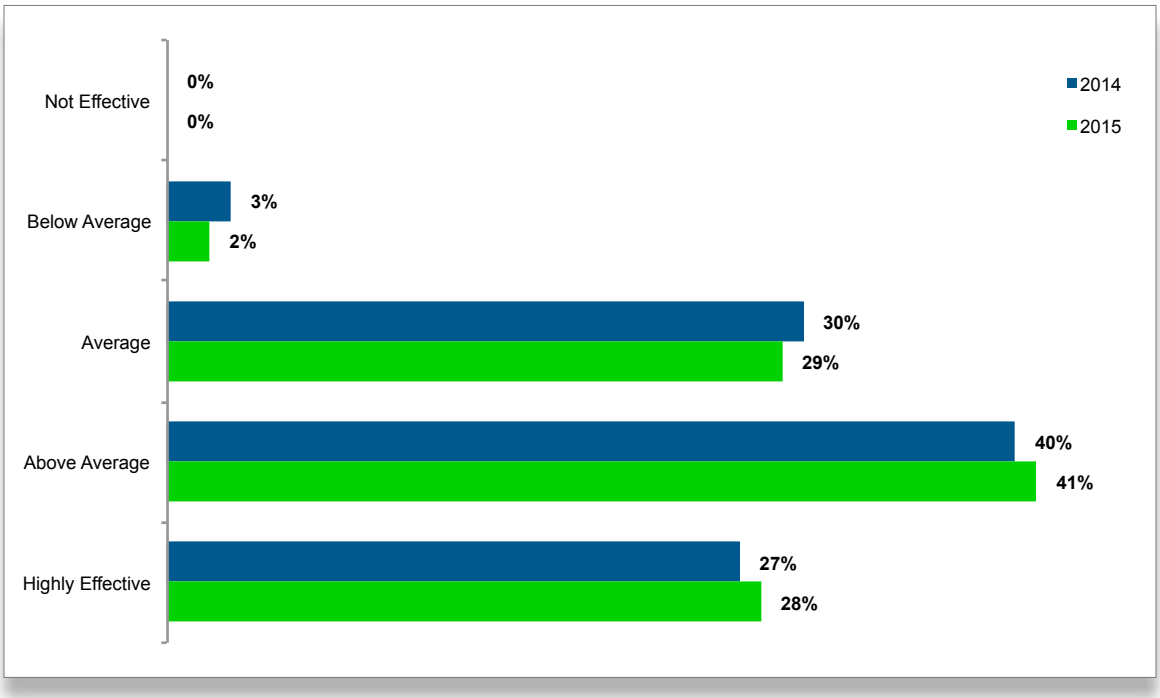

Figure 14. 2014 vs. 2015 Perceived Effectiveness of Awareness Training

Training Delivery Methods

Training delivery has changed between 2014 and 2015. More training programs are moving towards using social engineering (phishing email, impersonation calls, in-person interaction) to train their employees. The gains seem to come from areas that have been traditionally more popular, but also less effective and/or less scalable. These include lecturing, noninteractive online training, and interactive online training. Lecturing is often less effective since most lecturers are not trained educators and students tune out. Most noninteractive web-based training can easily scale to larger organizations, but it is also less effective because the delivery lecture replaces a live person with a recording. The interactive web-based training tends to be a more effective delivery method than both lecturing and the noninteractive delivery methods, but it still often suffers because it is less tailored for specific business environments and thus has difficulty creating a strong context for certain aspects of the environment.

This migration of techniques is a huge step forward for increasing return in the training programs that take the step and also for the security of those companies.

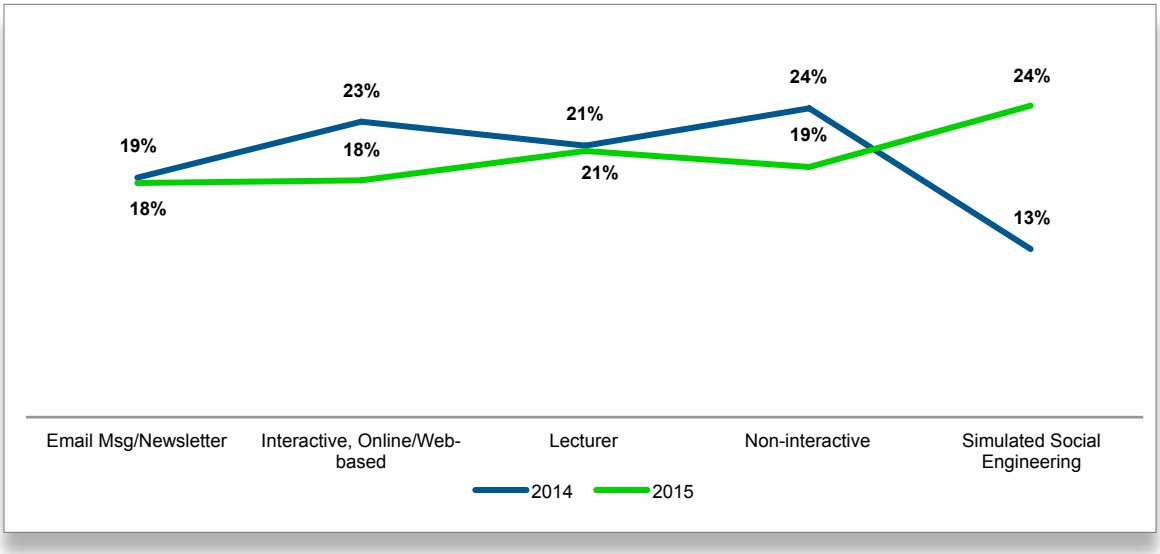

Figure 15. 2014 vs. 2015 Awareness Training Delivery Methods

Resistance to Phishing Attacks

A key aspect of security awareness is being able to detect and resist phishing attempts. EMA asked respondents how they detect phishing emails. The results between 2014 and 2015 were very similar and pretty evenly spread between the different detection methods.

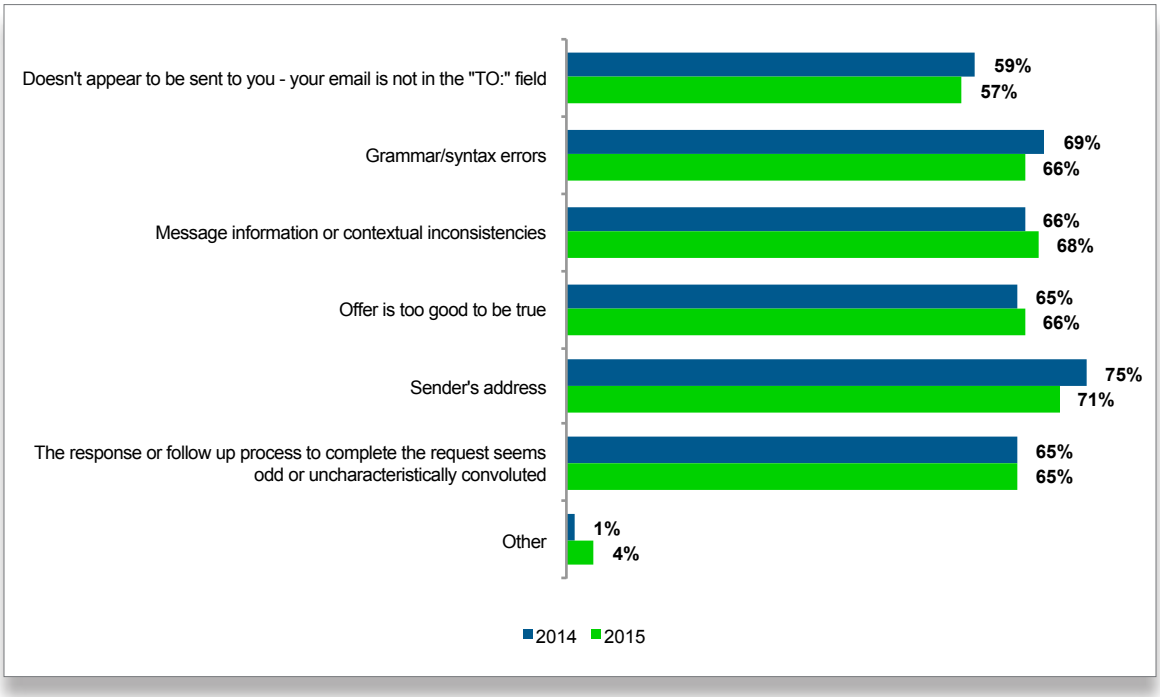

Figure 16. 2014 and 2015 Clues that Email Is a Phish

So why are so many links still being clicked? If the respondents are accurate about themselves as a group and their perceptions are relatively accurate about those who are trained around them, then the majority of link clicking is coming from individuals who are not trained. This makes the only significant solution to get the rest of the people trained.

Conclusion

The turnaround in the number of respondents claiming they have been trained is phenomenal. Moving from 56% untrained to 59% trained in a year shows nearly unheard of improvement. The major catalysts for this were the combination of negative media attention on the lack of training and the global visibility on the 2014 data breaches. Organizations began to understand that not only tools and process are needed to protect business data, but that people must also be addressed as a weak link. Attackers will exploit the weakest defense so all three of these aspects of business operations must be addressed to create true layered security.

Between 2014 and 2015 there have been numerous improvements in security awareness training programs. The sheer volume of increase is highly encouraging. The significant rise in programs in the SMB sector is excellent since that market was identified as the most underserved. Not only is there more education overall, the programs seem to be maturing in both delivery and how they measure the success of their programs.

Moving from live or computer-based lecturing to other more interactive methods that can provide personnel with more realistic content and fewer perceived training interruptions, thus reducing business friction and increasing participation. Though many programs still use attendance as a measuring stick for efficacy, there has been some migration away from this to gain more value from the program and truly increase their personnel's resilience to attack. This is most obvious in programs that provide ongoing or continuous training that delivered as part of the business operations. This training not only helps personnel recognize phishing messages in their various forms as they occur but also creates zero business friction while providing the person who made the error timely feedback on the mistake and how to correct it, thus following educational best practices. This in turn gives program management the best way to determine whether training is effective and provide leadership with return on investment (ROI). When conducted in the proper manner or environment, testing of this nature is very effective and can be repeated to track results on similar data sets.

Training vendors that wish to expand their opportunities must adapt not only their content but also their delivery to continue gaining ground in the smaller business sectors. Cloud delivery capabilities are a key aspect of lowering delivery costs and accelerating deployment for all organizations but will be most attractive and positively impactful to the SMB and smaller midmarket organizations that do not have the budgets, staff, and/or data center space to deliver the infrastructure in-house.

Post 2014 organizational management has a much clearer picture that breaches are not rare occurrences that only happen to companies that do nothing; they can and do happen to companies of all sizes and industry verticals. There is sufficient information available to the management team from both the analyst world and the media to aid them in making a calculated risk decision on the part of the business on whether they can invest in a security awareness program and if so, which vendor will provide them the best value based on their internal issues and budgets.

When evaluating a security awareness training supplier or program, organizations should choose a partner that, at a minimum, provides the following feature/functions.

- Training based on instructional principles that are effective.
- Programs that can accurately assess not only the collective group performance over time, but also individual comprehension so those with weaker understanding can be addressed as early as possible.
- Reporting capabilities that help program management demonstrate business value.
- Training has interactive delivery, is entertaining and engaging, and flexible to different learning styles.
- Deliver content that only addresses current threats but is also expandable to include new threats or business requirements.

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

3254-KnowBe4-SUMMARY.100515