Security Awareness Training: It's Not Just for Compliance

Research Report Summary

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

April 2014

Sponsored by:

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

Table of Contents

©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Executive Summary

Security is a key aspect of business in today's world. Announcements are made daily about new data thefts, breaches, and other related security issues, many of which originate as attacks against the workforce. Accordingly, the importance of the human component of security has become increasingly obvious.

The ***Security Awareness Training: It's Not Just for Compliance*** study, conducted by **Enterprise Management Associates,** is a groundbreaking research study examining the implementation of security awareness training across organizations. This research comes at a time when organizations are seeing an increase in data breaches and intellectual property theft. The study arms security and IT decision makers with insight on how to improve their security awareness training programs and why they should do it.

The EMA research study included over 600 respondents representing organizations ranging from 10,000 or more personnel, down to small businesses having fewer than 100 employees. Organizations also included public and private companies, government and non-profit groups. Respondents were evaluated collectively, by age group and organization size. Key findings include:

- More than 56% of personnel, excluding security and information technology staff, have not received security awareness training from their organizations.
- Small businesses with fewer than 100 employees accounted for the greatest percentage of untrained personnel, 44%, of the four primary organization size groupings in the study. This percentage tended to decrease as organization size increased, with enterprises having between 10,000 and 20,000 people having only an 8% untrained population.
- Employees predominantly received training annually, even though a higher frequency of training has been found to be more effective.
- Across all age groupings, employees perceived the top two security issues to be *information handling/DLP* and *web security*. Other perceived top security issues were *email security/phishing*, *HIPAA/HITECH/PII*, and *mobile security*, but the order of importance varied between age groups.
- *Online interactive* and *non-interactive training* accounted for the most common training delivery format, 45% and 47% respectively, edging out the *speaker/lecturer*, 41%, which until recently was probably the most common form of training delivery. Employees in larger organizations received training in multiple formats.
- Forty-eight percent of respondents reported their organizations measured the effectiveness of security awareness training, 18% said training effectiveness was not measured and 34% didn't know whether training effectiveness was measured. The most common forms of training "measurement" were training completion, 62%, and end of training testing, 55%. The term measurement is in quotes because mere completion is not as much a measurement of effectiveness so much as a measurement of attendance.

The research results clearly show many security awareness and policy training programs lack the delivery periodicity, content and quality that could increase retention thereby improving security decisions made by personnel and reducing risk in their organization. Company size, budgets and market vertical significantly impact the existence and maturity of the awareness training. Awareness training gaps were identified in organizations of all sizes. However, those with more than 1,000 personnel suffered more from training quality issues while those with fewer than 1,000 personnel were impacted more by the

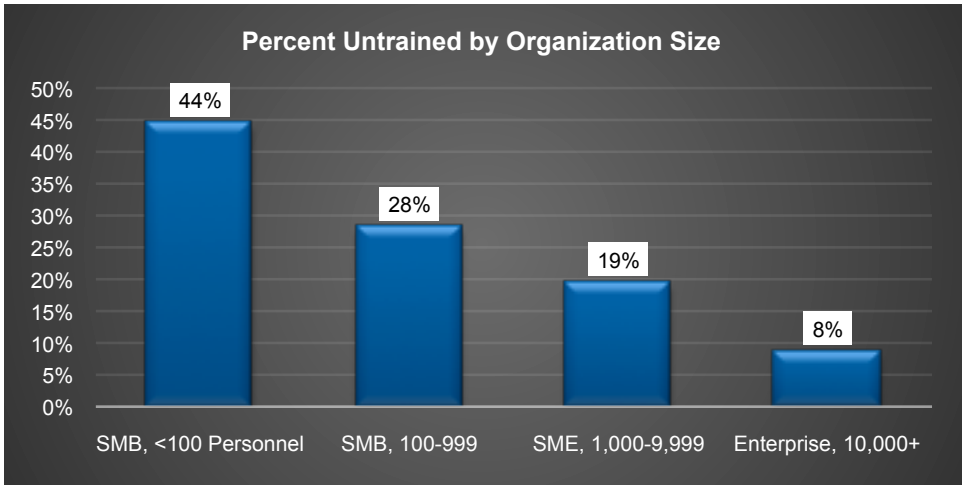
©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

lack of training programs. Larger companies traditionally have bigger budgets from which they can allocate more for training. Organizations in market verticals driven by compliance or regulation paid for training as a required cost of operating. In organizations where training was conducted, disclosed delivery methods often did not meet recommended educational or psychological standards for retention and application of material, which reduced training effectiveness. This lack of effectiveness wastes resources and increases organizational risk. The vast majority of respondents, 84%, recognized that they used the awareness training from work to decrease risk at home, therefore the lack of awareness training in the workplace directly correlates to an increased risk for personnel at home.

Summary Findings

The most glaring issue from the study was over 56% of the respondents said they had not received any security or policy awareness training from their organization. This is huge considering the worldwide emphasis on security over the last few years.

Seventy-two percent of untrained respondents worked for Small to Medium-sized Businesses (SMBs) with fewer than 1,000 employees. Forty-four percent of the untrained respondents worked for SMBs that had fewer than 100 employees. Though it indicates a large gap, it is not unexpected. SMBs not required to provide training for compliance generally focus more resources to operations, product/service development and delivery in order to gain revenue and market share. Many SMBs may mistakenly think their small size keeps them below attackers' radar, but in doing so leave themselves exposed to various types of employee focused attacks which could cost them everything. The potential cost of employees making poor security choices due to lack of awareness and understanding may go unrecognized until it becomes an actual cost of breach reparations. Because small businesses often do not have security staff and do not have an advocate for security awareness training, those organizations may not understand the risks they are leaving themselves open to.



©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Key Security Topics

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 organization.

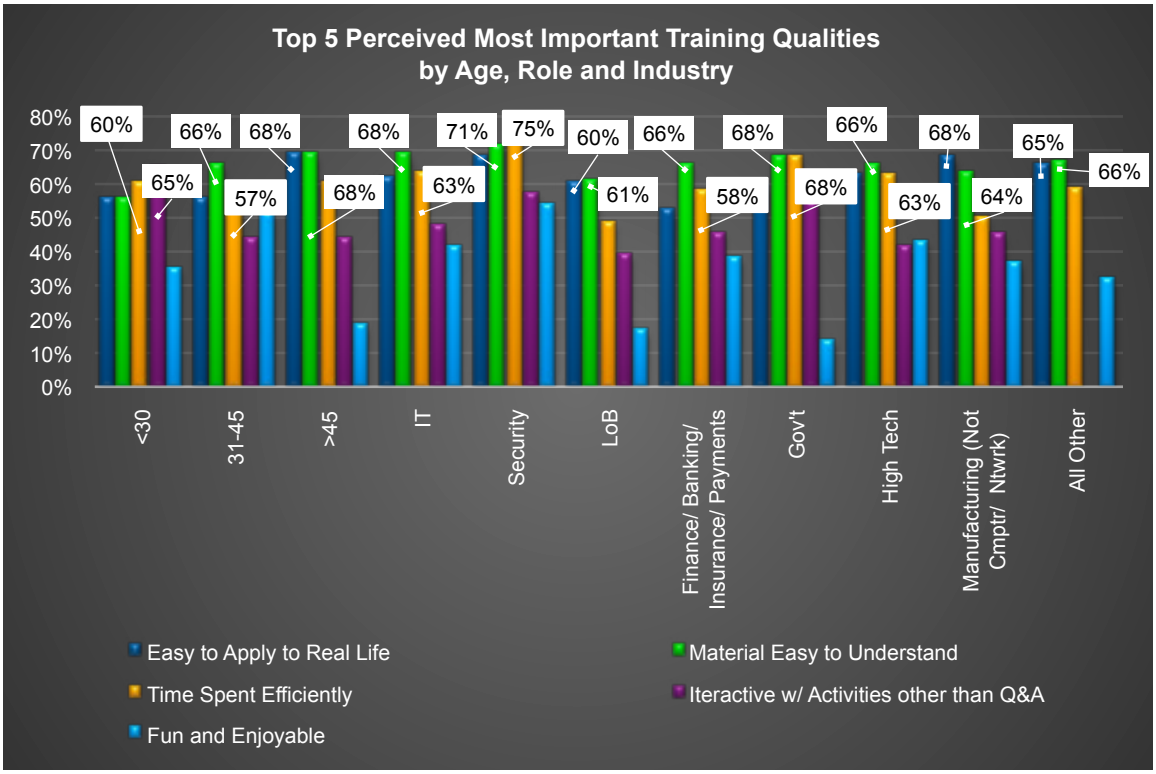
In descending order, the top five security topics on which training was provided are: *Password Management, Email/Phishing Security, Web/Internet Security, Physical & Office Security, and Privacy.*[1] The top five training topics perceived by respondents to be most important for security had strong overlap but also had some noticeable differences: *information classification/handling and leak prevention, web/internet security, email security/phishing, password management, and HIPAA/HITECH/PHI*. Evaluating the training areas identified, we find 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 are valid but organization should take the opportunity to understand what relevant areas employees feel they need more instruction on to provide better security for business assets and environments. Employees are fairly consistent in what they perceive to be needed most.

Information classification and web security were consistently the top two concerns across age groups, job role, and industry with the exception of high-tech, where email and web security flipped in priority. What is interesting is the consistency of the Top 5 perceived most important training topics across the age groups. Though not in the same priority, all age groups agreed on three of the most important categories. The differences in categories could be attributed to variable age differences; further analysis will be done in the full report for the study. One possibility is that the less-than-30 group are early adopters of technology and so are more aware of issues like mobile security, while the 35–45 age group may feel more concerned about identity theft due to their family and other financial commitments.

Training Attributes

Respondents were given a list of five options and "none of the above," and then asked to identify their top three choices in rank of preference, for most important attributes for training delivery. In general, most, 66%, thought the most important factor identified was "easy to understand," followed by "easy to apply to real life" at 61% and "time spent was efficient," 59%. The last two options were "interactive" and "fun/enjoyable." These results reflect the need for security training to be presented in a clear, non-technical manner that employees can apply to their environment. Even though educational research shows that training is significantly more effective when the recipients are engaged, become participants, and enjoy the session[2], the only group that ranked "interactive" as a priority was the less-than-30 age group, where it was ranked highest at 65%. It is possible that many respondents have not had access to interactive and/or fun training, and therefore have no experience from which to rank it.

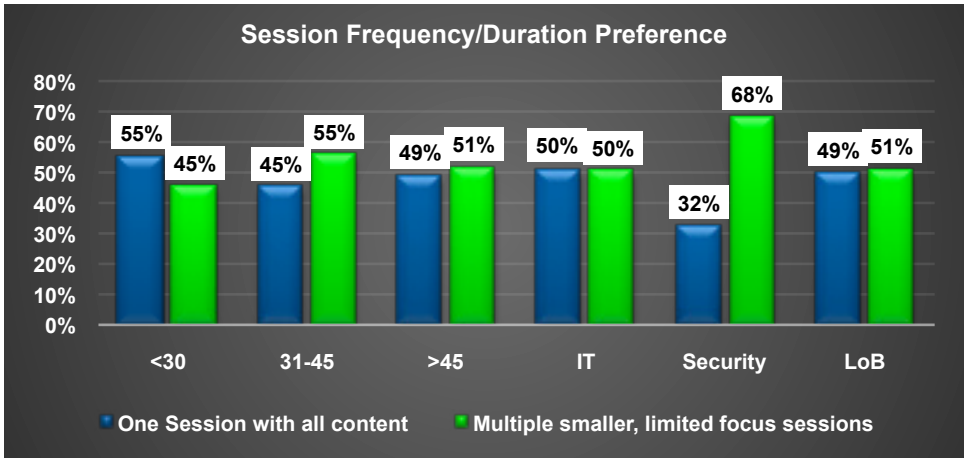
©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com



Session Frequency and Duration

Looking at the responses as an aggregate, the preference was very close at 48% preferring a single "cover-all" session and 52% preferring multiple shorter sessions covering less material at one time. Upon evaluating the training session frequency and duration, the respondents were separated by age and job role. Fifty-five percent of the respondents younger than 30 preferred to get their training in a single longer session with 45% preferring the shorter, more focused sessions. The group 31–45 years of age was split exactly the opposite. The rest of the groups, with the exception of security, were virtually equally split between the two. Security had the greatest divergence with 68% of respondents preferring the multiple shorter sessions. Studies on learning effectiveness indicate that training is better in shorter sessions with repetitive content that students can practice while they learn.[4] This external guidance should help organizations that are evaluating their current programs or constructing new programs to move to the shorter multiple sessions. Program developers/managers may also investigate programs that can deliver training on-demand over some specified evaluation interval, i.e. to be completed in a quarter, so employees can engage between workload peaks.

©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

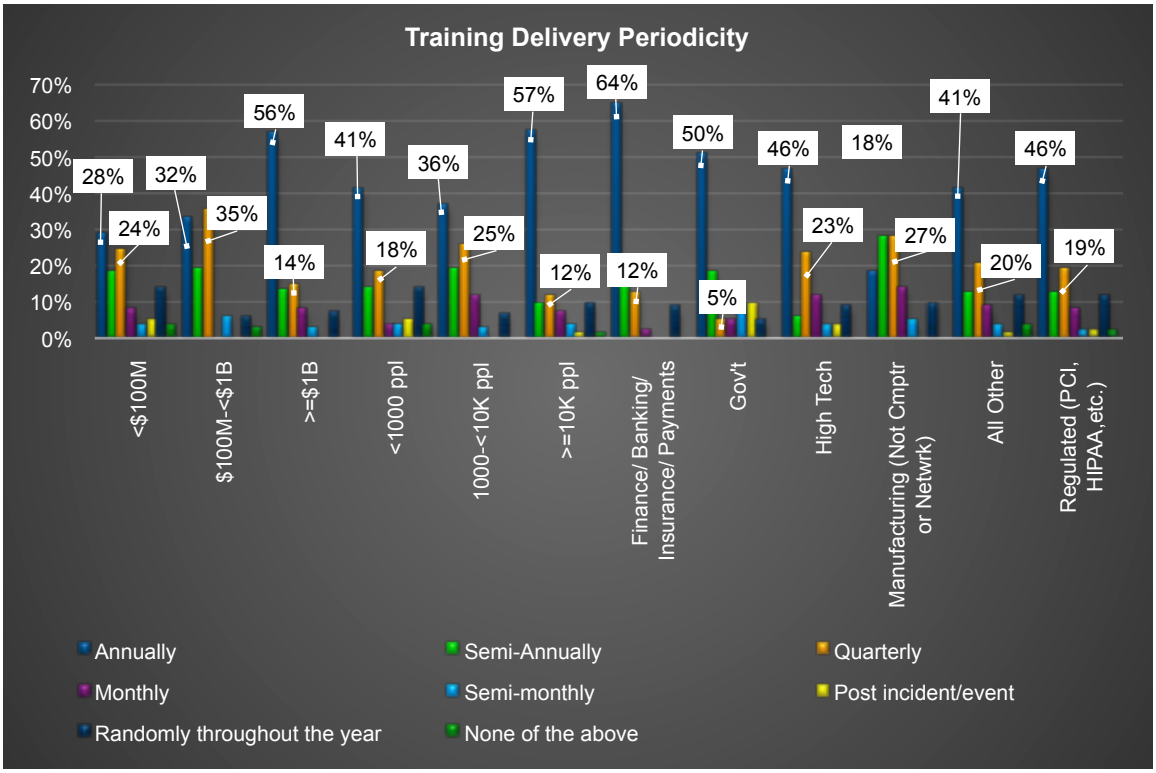


Session Periodicity

Research showed that 77% of organizations provide security awareness training on a quarterly to yearly basis. When analyzing the data broken out by company size, revenue and industry, we see that yearly delivery is the common leader across all divisions with the exception of manufacturing (non-computer or network related) where both quarterly and semi-annual training were more common. Quarterly training delivery is the second-most common interval with the exceptions of manufacturing, where, as previously mentioned, it was first, and in finance/banking/payments and government, where it fell to third, behind semi-annually. According to generally accepted educational and learning studies, training provided at that interval is unlikely to be remembered by the participants. Though there is variance in the number of repetitions required to learn something and in the ways people learn, a simple piece of information must be heard at least three times[3] by the average person to be able to recall it in short term memory and up to 20 times to commit it to long term memory.[5]

It is also useful to note that only 2% of organizations took advantage of training personnel post-incident. Proper "post-incident review" or "post-incident processing" is a standard in many processes from educational institutions to FEMA. NIST refers to it as "lessons learned."[6] It is recognized as one of the best means of improving performance after an incident or failure. When people recognize they have made a genuine error, not an intentional act, they generally want to fix it. Appropriate, timely feedback addresses this desire.

©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com



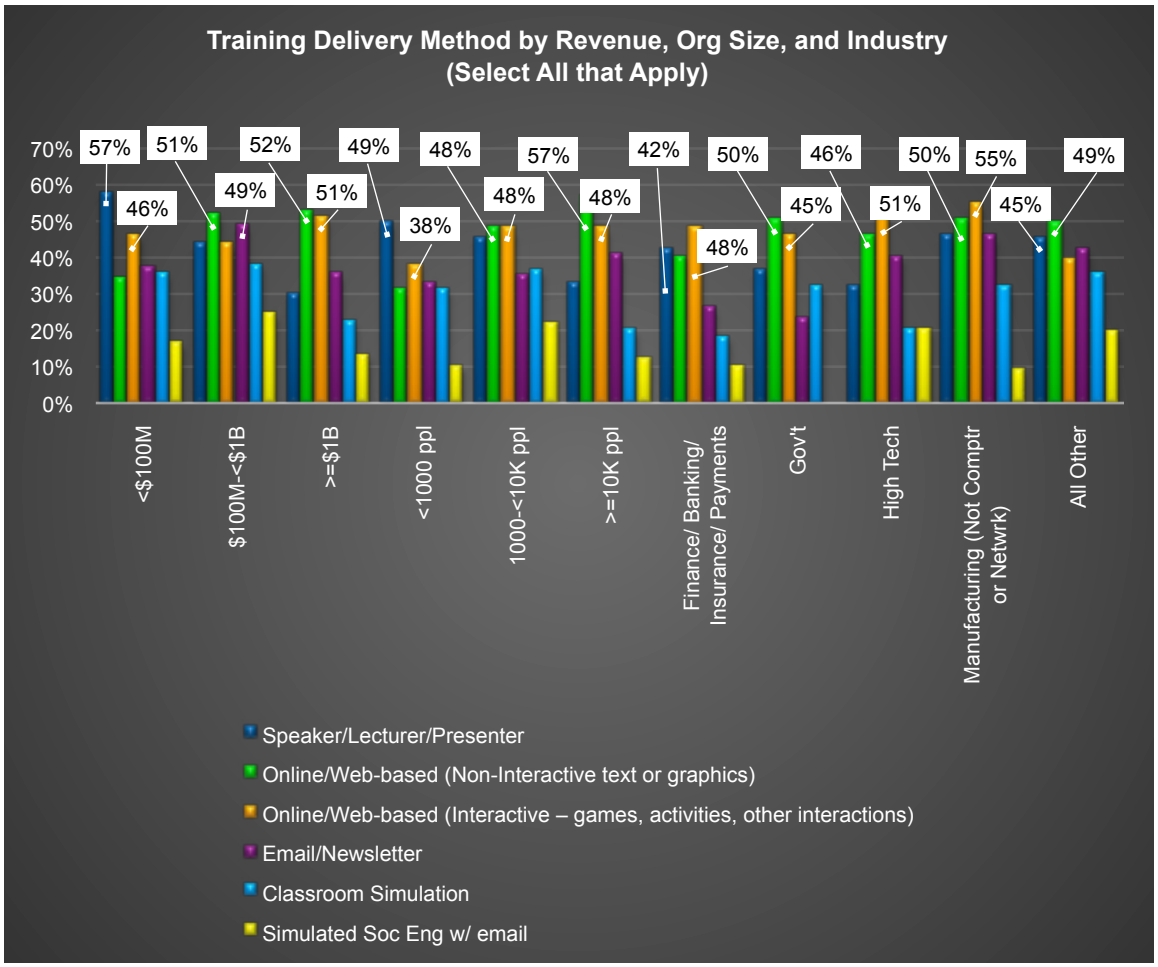
Training Delivery Method

Evaluating the data as a whole, there was no significant leader in training delivery method. Below we have listed the top six methods identified, leaving out the "social engineering with paper and calls" and "other" categories because they trailed behind so significantly. In the graph the top two methods for each group are labeled. Online web-based, non-interactive was identified as the primary aggregated response with 47% of respondents' votes. Surprisingly, 45% of the respondents said they received some form of online interactive training. Prior to the study one of the major hypotheses was that this training format was not widely used.

As the data was separated there were some notable variations. First, online interactive training was most used in finance/banking/insurance/payments, manufacturing and high-tech verticals; it was within one point of tying for first in the >=$1B revenue category. Second, speaker/lecturer was most prevalent in organizations with smaller revenue or personnel count. These organizations also tended to have training delivered by internal personnel who provide training because it is assigned to them, not because it is their primary function, and lecturing is one of the easiest formats to provide so this was not unexpected. Third, when evaluating companies by revenue, 49% of respondents representing the midrange revenue category ($100M to <$1B) said they receive training via email/newsletters a great deal. This was the only category in which email/newsletter was ranked second.

The fact that online interactive training was represented far higher than expected is encouraging because that method provides better learning than the non-interactive. On average, participants who take these sessions remember no more than 20% of what is relayed.[7] As an additional impediment, during non-interactive types of training, trainees often multi-task with work or entertainment, further removing them mentally from the training.

©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

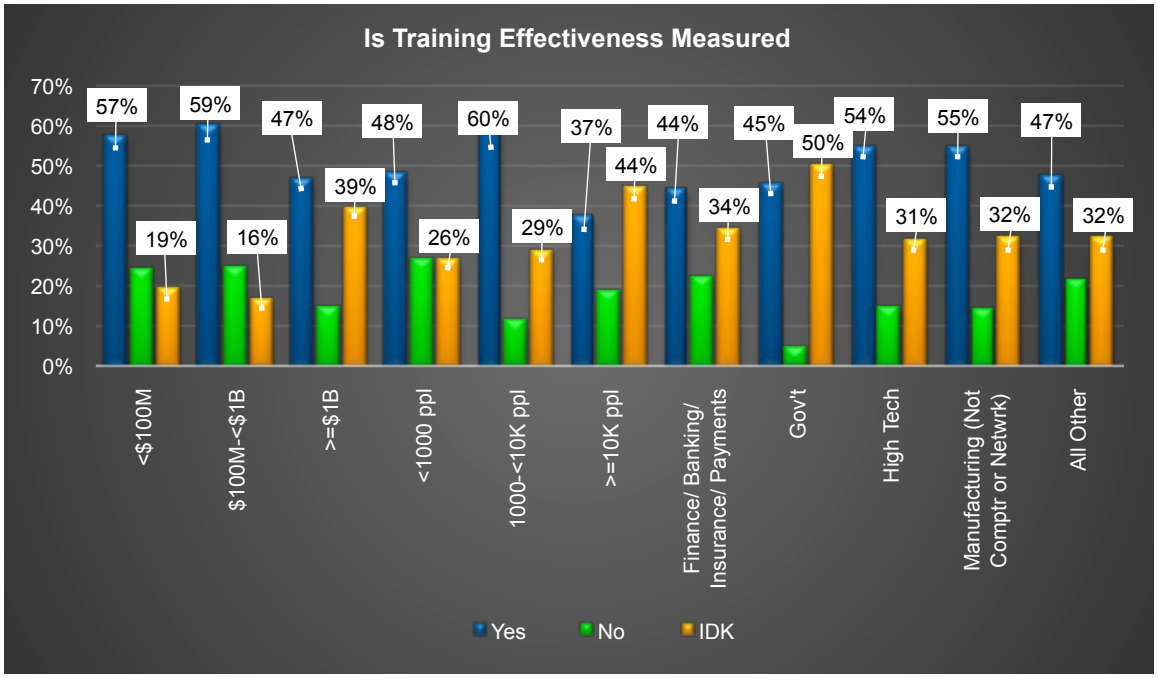


Training Measurement

According to survey respondents, 48% of organizations measured training effectiveness. Thirty-four percent of respondents had no idea if awareness training effectiveness was measured. This is consistently higher than people who knew training was *not* being measured—identifying a significant problem. This could mean organizations are not effectively communicating measurements and metrics to their general employee populace, or that the users do not find metrics interesting and aren't paying attention.

An interesting lack of knowledge occurs in government and organizations over ten thousand people. Each of those groups has a greater number of respondents indicating they did not know if effectiveness was measured. This could directly relate to organizational size and compartmentalization making communication of measurements difficult, or perhaps measurement really isn't taking place.

©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com



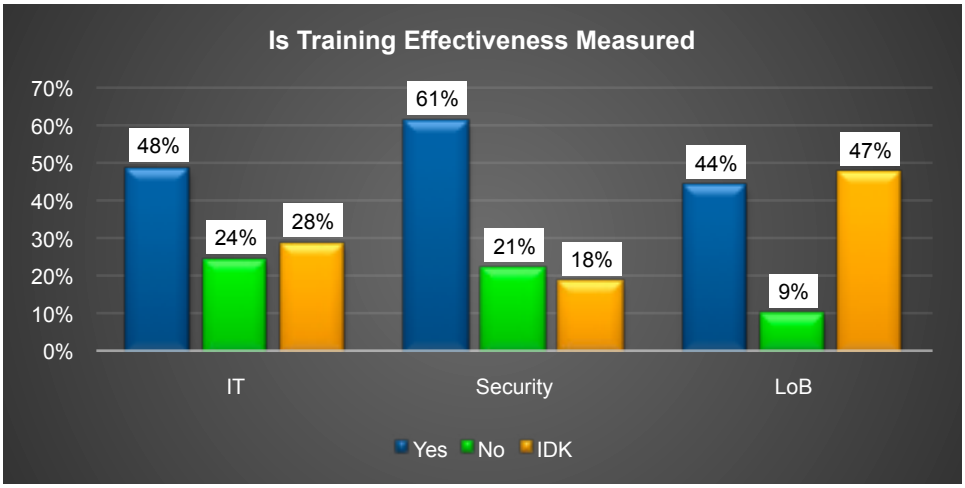
When we compare these possibilities to the second graph which calls the responses out by role, it demonstrates even further that there is a disparity between what is being measured and what is being communicated. Note that 47% of the Line Of Business (LOB) personnel are unaware of any measurements of effectiveness. Security has a significantly higher awareness of program measurements than anyone else, including IT. Given that Security is usually a part of the awareness program and measuring its effectiveness, this is the most accurate indicator telling us that programs are indeed measured in most cases, but the proper communication is not there. This is a serious gap that needs to be addressed by making a good communications mechanism a key indicator of the awareness program toolset.

Lastly, the 18% of organizations that are presenting awareness training and are not measuring its effectiveness have no quantitative way to assess if their training dollars are well spent, or training is making a difference in reducing the risk exposure within their workforce.

Having poor or nonexistent measurements leaves program managers without the data they need to support continued investment in the program.

Combined, sixty-two percent of the participants said that their awareness training programs use completion as a program effectiveness measurement and 55% said they are evaluated by a post training poll or test. Training completion is important for compliance. In organizations where awareness training is voluntary, poorly tracked, or not tracked at all, low completion rates also can be indicative of lack of satisfaction with or low prioritization of training. This is generally caused by a low perception of value.

©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com



Use of completion, rather than participant performance, to gauge program effectiveness indicates that organizations either do not understand how to measure individual/program effectiveness or that they are performing training more to meet a regulatory or contractual requirement than to actually improve their security posture and reduce risk. Completion, as compared to the other methods listed, gives no insight into any aspects of employee understanding, retention, or adherence to what has been taught. With limited budgets and time, it is understandable that other measurements may be overlooked; however, by itself, completion provides no insight into the effectiveness of training programs; it merely indicates the program had "butts in seats."

Post-training testing is better than mere completion but can be biased as a measurement depending upon how it is implemented. In non-interactive online sessions where there is a test at the end, participants will often speed through to get to the test questions, then return to the video speeding through it with a goal of scanning out the answers quickly to get back to work, rather than learning the topic. This approach also negatively impacts knowledge and retention.

In looking across the data, one note of encouragement is that in all of the evaluated groupings, "change in response to attack simulation" was identified as a method used to measure either program or individual effectiveness. (There was no separation between these in the study.) The percent of respondents indicating this method was used ranged from 38% to 50%. This was unexpectedly high. Because we did not expect to see this level of response for this type of measurement, we did not have questioning to drill down into the details of this area. That is something that could be investigated in a future study.

Other methods of measurement included in the survey were: *change in business losses*, *number of help desk calls* and *changes in malware infection rates*. Help desk calls were indicated as a measurement of program effectiveness in 35%–45% of the cases by revenue and organizational size. It was present in all verticals, but was lowest in the government sector with only 20% of respondents indicating its use. Malware infections were also used as a measurement across all measured categories. Their use was indicated by respondents ranging from 25% in manufacturing environments to 53% in organizations exceeding ten thousand people. Both help desk calls and malware infection reports can have bearing on

©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

the organizational security posture, if measured properly, but can be tricky to interpret. For example, an increase in support calls/tickets may reflect employees calling due to heightened security awareness; or that they haven't had updated training and are calling in some new issue that they have caused.

In evaluating a measurement system for awareness training effectiveness, it is important to find tools that will allow for iterative measurement of both individuals and the program. Tools should have the ability to provide feedback to the recipients on the areas they need to improve in and to the management on where the program needs to focus to reduce risk most.

Conclusion

With all of the news around security breaches and data losses, it would seem logical that organizations would place a higher priority on security awareness training. With 56% of the respondents indicating they have not had security awareness training, it either must not be a priority or business leaders do not understand its value. When executed and measured properly it is very valuable for risk reduction. Humans are regularly demonstrated to be the weakest link in security. Even organizations with strong technical controls have to rely on their personnel to make good choices. Without training they *will* make bad choices, putting the business at risk.

Organizations that have smaller budgets for technical controls require higher human awareness and diligence as a compensating control. Organizations with poor technical controls and poor human awareness are playing a risk game, whether they acknowledge it or not, and given current trends, will suffer a breach if they have anything of value. If an organization chooses to not have a security awareness training program, that decision should be a calculated risk on the part of the business, not merely a cost cutting method.

For organizations that have made the decision to provide training, it would stand to reason that they would want to get as much value out of their training dollars as possible; however, this does not seem to be happening consistently. Organizations continue to provide training using very traditional models such as presentation and lectures or online videos and slide shows. These are generally only 20% effective in aiding retention of material. Providing training at quarterly or longer intervals is too infrequent to reinforce the training knowledge and does not meet any sort of recommended educational standards to maintain retention.[8] This significantly reduces training effectiveness, equating to lost time, effort, productivity and money on the part of those organizations.

Of the metrics included in the survey, training completion was the predominant measurement used for training effectiveness. Completion is a key metric for proving compliance. It may also offer some insight into trainee satisfaction because completion rates may be low if training is viewed negatively. However, using completion, without underlying performance measurements, to gauge program effectiveness provides very limited information and may indicate organizations are conducting awareness training so they can "check the box" rather than improve security and reduce risk. Program managers should evaluate how their measurements can demonstrate program impact and individual understanding.

The best way for organizations to determine whether training is effective and providing a Return On Investment (ROI) is to use training methods which allow the employee to demonstrate measurable understanding and progress. 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.

©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

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

- Training is based on instructional principles that are effective.
- Programs should be able to 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 are included for training personnel and management.
- Training has interactive delivery, is fun and engaging, and flexible to different learning styles.
- Content must be able to address current threats and be expandable for new threats or business requirements.

(Endnotes)

1. In the original release of the summary report this list was incorrectly reported. The list presented was from sub group >45 years old.
2. http://voices.washingtonpost.com/answer-sheet/learning/why-fun-matters-in-education.html
3. http://www.psychotactics.com/blog/art-retain-learning/ See, "learners retain approximately"
4. http://wiki.answers.com/Q/How_many_times_must_a_person_hear_new_information_to_retain_it
5. http://www.ask.com/question/how-many-times-does-it-take-to-memorize-something
6. http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
7. http://www.ask.com/question/how-many-times-does-it-take-to-memorize-something
8. ibid

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 its 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.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2014 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

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

2880-Wombat_SUMMARY.040814

©2014 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com