



Case Study: 1200 Users, 11 Cities, in 7 Weeks ... and They Wanted to Come to Security Awareness Training

(Todd Fitzgerald)

Todd Fitzgerald, CISSP, CISA, CISM, is the director of information systems security and serves as the systems security officer for United Government Services, LLC (part of the Well-Point Health Networks family of companies), which is the largest processor of Medicare Part A (Hospital) claims. Todd is a member of the board of directors and cochair of the Security Taskforce for the HIPAA Collaborative of Wisconsin (www.hipaacow.org), a nonprofit corporation formed to promote sharing between Wisconsin health plans, clearinghouses, and providers. He is a participant of the Centers for Medicare and Medicaid Services/Gartner Security Best Practices Workgroup, the Blue Cross Blue Shield Association Information Security Advisory Group, a board member (previously) of the International Systems Security Association (ISSA) Milwaukee Chapter, and board member for the ISSA–Delaware Valley Chapter, serving Pennsylvania, Maryland, Delaware, and New Jersey. Todd has held various broad-based senior management information technology positions with Fortune 500 and Fortune Global 250 companies such as IMS Health, Zeneca (subsidiary of AstraZeneca Pharmaceuticals), Syngenta, and American Airlines, and prior positions with Blue Cross Blue Shield United of Wisconsin. Todd has authored articles on HIPAA security and frequently presents at conferences and association meetings to promote security awareness. Todd has earned a BS in business administration from the University of Wisconsin–LaCrosse and a MBA with highest honors from Oklahoma State University.

The true barometer of a successful training program is when the attendees are talking about it in the hallways, telling their co-workers how much fun they had, providing high marks on the feedback forms, and explaining the lessons that were learned in the training to their fellow colleagues. Even more gratifying to the instructors are the comments received from the training, such as “best training program ever offered at this company,” “absolutely entertaining and informative,” “taught a boring subject in a fun way!,” “kept me interested,” “excellent content and creative presentation,” and “fun and informative.” So how was this accomplished? Great instructors? Enormous security subject? While we would like to think that all of the above were available and present, the reality is that the areas



of true importance were (1) creating a singular message, (2) detailed planning, and most importantly, (3) keeping it interactive with audience participation. Let us explore the real-life specifics that were executed to achieve “strongly agree” evaluation results!

The Problem

The first step in embarking on any successful endeavor should be to define the problem. Where is the organizational pain? What topic area has not been fully addressed before? It is important to define a *singular* problem or, at most, a few concepts that are related together. Cramming training on all of the security issues into one session will cause frustration with the users and not provide enough time to deliver enough examples. To those of us working daily in the security profession, it is easy to lose sight of the knowledge and understanding that we have around the subject, and expect others to “just get it” by saying it once. The theme selected for training was Internet and e-mail security practices. By picking a theme, other security principles can be embedded into the message. In this example, copyright issues (downloading music and software), confidentiality, identity theft (sharing log-on passwords), and securing passwords were embedded into the theme without overloading the users.

Review Videos

Once the problem was defined, eight different free demo security videos were obtained and reviewed to select the one that would be most appropriate. The demo videos were all full length with the word “demo — not for training purposes” across the screen. Short 15 to 20 min videos are an excellent way to begin the training session.

Enter Creativity, Collaboration, and Conceptualization

Once the theme had been decided, it was time to discuss some conceptual ideas, being very open at this point. The security officer and two staff members contributed ideas to develop the training program during an initial brainstorming session. In our case, the security officer had an initial vision of what was to be delivered; however, this was shaped and changed based on the input of the team. At this stage, every idea is a good one! The key to this stage is understanding that it may turn out completely different from originally conceptualized, and that is OK! It was decided through this collaboration to give the security presentation a theme of “Why Gamble? Get.Net.Smart!” With this theme, the training could be



312 ■ *Managing an Information Security Program*

developed around the appropriate use of the Internet and e-mail and the risks to the individual and company for inappropriate use.

Toys, Toys, and More Toys!

Toys provide an excellent visual aid for training and people immediately have a perception that “this is going to be fun” when they walk in the room. The toy, game, and party stores are excellent places to roam around. It is also useful to not limit the toy selection to toys in the stores but to also use a search engine such as Google to locate items in quantities that are not available locally. Dollar stores are also excellent resources. To tie in with the theme of gambling and the Internet, 6 different colored, 12-sided, numbered, 8-in. foam dice were ordered from the Internet. At this point, it was unknown how they would be utilized, but that was OK! All that was known was that some sort of game would be created.

Initially, it was thought that there would be 6 tables of 5 people each (30 per session), and they would throw the dice at each other and then, based on the number, some activity would be performed. The key point here is to build on (1) number of people requiring training, (2) the theme, (3) the video, and (4) the toys. In keeping with the dice and gambling theme, while at a game store that was going out of business, we saw some dice marked at 70 percent off, or 30 cents for 6 dice. Again, not knowing exactly how these would be used but knowing that there would be about 60 training sessions, 600 packs of the dice were purchased as giveaways. Another toy store had some light-up dice that would also be excellent giveaways, so after purchasing one pack from the toy store, the distributor was contacted and a quantity discount price was negotiated on 1300 pairs of dice (an extra 100 pairs were ordered for new hires).

The video and toy ordering were among the first activities completed to support the theme of the training. Why? Because there may be longer lead-time associated with acquiring the toys depending on the product and quantity. There also may be internal organizational lead times to be considered in getting the purchase orders and payments through the accounts payable department.

The Training Scenario

After much brainstorming and roaming around party and toy stores, the training scenario was developed. A video on the appropriate use of Internet and e-mail would be watched, and then scenarios would be acted out with the use of props and 20- to 30-s segments of downloaded music clips. In preparation for the training, 12 scenarios of inappropriate Internet



activity would be matched with a music clip and props for the presenters to act out the inappropriate activity. As the attendees entered the room, they would draw a colored number (1 to 24), matching the color of the dice placed at their table, from a bag that would determine their assigned table. Assigning individuals to tables separates chatty friends, reducing people's anxiety about picking a spot, and helps people meet new co-workers. For each scenario, one of the presenters would draw a matching number from another bag and call on the attendee to roll the 12-sided, numbered, 8-in. dice on their table. The number shown on the top of the foam dice after the roll would be the number corresponding to one of the 12 scenarios of inappropriate Internet/e-mail activity. The instructors would then play the music clip and act out the scenario, while the person selected would have to guess the inappropriate activity. If they were unable to guess, the members of their table could help them out. After each activity was guessed, it was briefly discussed, explaining the inappropriate activity and risks to the business of the activity.

For example, the inappropriate activity may be viewing pornography, and the music clip used could be "Sexy Thing" by Hot Chocolate or "This Love" by Maroon 5, while the presenters wear purple wigs, beads, and interact with the audience, delivering the message of sexual harassment. Or a "clean" version of Eminem's song "Real Slim Shady" could be used to highlight identify theft, password sharing, and exposure to confidential information while the presenters are dressed in backwards-facing baseball caps, sunglasses, and blowup microphones, *imitating* the dance moves of the singer. Spreading rumors through message boards and e-mails could be highlighted through Fleetwood Mac's song "Little Lies" while the instructors, wearing Pinocchio noses, gossip with each other and the audience. Use imagination and creativity to develop the scenarios in advance. The key is to interact with the audience while acting out the scenarios, as well as tying them to the business risk after each music clip. It is useful to use a variety of songs from the present and past, and related to different regions of the country where you may be training. For example, the country song "Gambler" and playing 52-card pickup with a selected victim used to communicate Internet gambling was popular in northern Wisconsin training, as well as in our Virginia/West Virginia offices. Alternatively, using songs by the Beach Boys such as "Little Deuce Coupe" while pretending to drive little toy cars used to communicate "surfing the net" were most popular in the California offices. All the songs were well received across all regions.

During the playing of each music clip, it is important for the presenters to move around the audience, visiting each table and interacting with different people. This is what makes it fun for the participants. Putting beads around someone while "You Sexy Thing" is playing or staring at

AU: Meaning unclear.



314 ■ *Managing an Information Security Program*

someone close-up, or better yet, surprising someone with a 6-in. nose on your face usually brings laughter. If they are laughing, they are being entertained and are paying attention to the message. Sneaking up from behind people while wearing dark sunglasses and moving to the sounds of the James Bond Theme song for “007” can raise laughter while communicating the internal hacking and electronic monitoring capabilities related to a “spying message.”

Communication needs to be deliberate and in multiple forms as different people learn differently. We communicated through written words (presentations), speech, visual effects, and our body language. This is why the video and scenarios are so effective at reinforcing the message. After the training, people will remember the visuals and music and the have a higher probability of retaining the message.

The One-Hour Agenda — Don’t PowerPoint Them To Death

The training was also limited to a one-hour session. It is difficult to hold someone’s attention to a subject that is not considered his or her primary job or interest for longer than that time. PowerPoint slides are a great visual tool, but for this type of training, they were used sparingly and only to frame the beginning and the end. The following agenda was determined:

- *Introductions*: 15 s, keeping the training light.
- *Video*: 20 min, but ask them if it is okay to watch an hour-long video and get their reaction; then tell them it is only 20 min.
- *Exercise Recall of the Video*: 15 to 20 min. Don’t explain what they will be doing until after they have viewed the video; keep it vague at this point. This is where the 1 to 12 scenarios are repeated
- *Questions and answers*: 5 min.
- *Evaluations*: 5 min; actually takes less time.
- *Drawing*: 5 s.

After all of the attendees have drawn their numbers and are seated at the table with the matching colored dice, it is time to go briefly through the agenda. The agenda is intentionally 50 min in length, as it is a good idea to add a few minutes for scenarios that may run a little longer or to allow for questions that may come up during one of the scenarios. It is also advisable to start each session 5 min late and to tell everyone to be prompt in attending the sessions. Why? Because there will always be a few individuals that will be late, and this minimizes any distractions; the latecomers will also be able to receive the entire presentation. As a general rule, if someone arrives more than 5 to 10 min into the video (25 to 50



percent), it is acceptable to tell him or her to return for another session (however, in small geographic offices with only one session they will have to get the most out of the time remaining in the session).

Logistics: Success Is in the Details

This cannot be stressed enough. To really be successful, especially across geographic locations, the program must be rigorously planned so that the proper communication, facilities, equipment, materials, and people are engaged. Multiple spreadsheets were used to manage the process.

Pretraining Planning

Coordination in advance is necessary to conduct successful training included:

1. Determine number of individuals in each location, training materials needed, and order training supplies 4 to 6 weeks before training starts to provide ample time for receipt of materials.
2. Preparation of one-page PowerPoint slide to launch training with theme. Send out 3 weeks before training.
3. Recruit coordinator in each office to help with room scheduling and times (1 to 2 months before training).
4. Negotiate training times with each office (1 to 2 months before training).
5. Negotiate special training sessions for groups with phone coverage (e.g., customer service) that may limit their availability.
6. Identify hotels near each office (one month before training).
7. Determine schedule and make flight and hotel reservations.
8. Review video and create associated spreadsheet with inappropriate activities and the music and props that will be used for each scenario one month prior to training and continuously improve during training; new ideas will surface.
9. Prepare individual office sign-up sheets, evaluation forms, and sign-in sheets one month prior to training.
10. E-mail notification of training three weeks prior to training, with another notification reminder one-week prior.

Class Sizes and Scheduling

With offices ranging from 15 to 600 people spread across 10 cities in 7 states, the number of sessions and attendees per session varied. The



316 ■ *Managing an Information Security Program*

optimal class size for interactive training appeared to be in the 20 to 24 range, so sign-up sheets were limited to 24 people. Individuals would typically add their own lines and sign-up if the session was full, so the rooms were set up in advance to handle 30 people (6 tables of 5 each) to handle this situation. This avoids moving chairs around at the last minute and after class starts. If it is known that something could happen, it is best to plan for it ahead of time.

The sessions were 1 hr in length with 30 min between each session. This was necessary as 15 min are needed for resetting the room with evaluation forms and candy, putting the props away, and setting up the computer for the next session. Another 15 min were reserved so that the instructors would be ready for the early birds who get to the sessions early. There is no time to go back to your desk and look at e-mail.

Four sessions each day were scheduled for the larger locations, avoiding the lunchtime period and the end of the day, if possible. People get antsy around these time periods and are thinking about how hungry they are or if the session will end in time for them to pick up the kids. Optimal session times that worked were 8 to 9 am, 9:30 to 10:30 am, 11 to noon, and 2 to 3 pm. More than four sessions can be taxing on the instructors; finishing by 3 pm each day permits some time to handle e-mail and other daily activities. In locations where customer service representatives needed training and needed to be on the phones, the training was shifted to begin at 7 am. For the larger locations, class sessions were held across a two-week period (preferably noncontiguous) and scheduled on different days to increase the likelihood those individuals would be able to attend.

Session Planning for Each Location

When training across multiple geographic locations, there are many details that cannot be performed until arrival at the location. It is important to provide plenty of time outside of the training to make this successful. Arriving at the first session in the morning at least one hour in advance is necessary to: (1) setup the LCD projector and computer, (2) test and verify that the music volume is appropriate, (3) distribute evaluation forms to the tables, (4) distribute chocolate to the tables, (5) setup the dice on the tables and any other visuals around the room, (6) double-check that the props are all there and hidden from attendee view, (7) configure the room tables, and (8) check the sign-up sheets for attendance numbers. By ensuring that these details are taken care of in advance, when the participants enter the room, the instructors are available to meet and greet each person and have them draw a number from the bag instead of trying to get set up while people arrive.



While each video was being viewed, the instructors would sit at the back of the room and match up the numbered cards (1 to 36) between two bags; one bag that the attendees picked from, and the other that the instructor used to draw the next number. Because there would never be exactly 24 people in a session, by matching the numbers that were left (not taken) and removing them from the instructor bag, this eliminated the possibility of wasting time by calling out a number that did not exist. Time is important, as there is only 1 to 1.5 min per scenario. Although the sessions were planned for 24 participants to sign up, numbers 1 to 36 were used to be able to handle up to 36 people. Upon reviewing the sign-up sheets prior to each session, higher numbers were removed from the selection (e.g., 31 to 36 or 25 to 30) so that when the participants chose a number, they would be evenly distributed to one of the six colored tables.

99 Percent of Evaluations Returned

The common experience with evaluations is that few people fill these out. However, out of approximately 1200 people trained, 99 percent were returned! This is not by accident, but rather planning. In the beginning of the presentation, the evaluation forms are mentioned, and at the end of the presentation the instructor said “Please fill out the evaluation forms and in return we will provide you with a pack of light-up dice.” Additionally, it is effective to stand at the door and hand out a plastic bag containing the dice and a card stating the inappropriate Internet activities and the associated risk to the business to each person. The participants place their evaluations on the chair next to the instructor by the door, affording them anonymity. It works. It is also important to have the evaluation present in front of them when they sit down at their table and to give them a few minutes to complete it.

Makeup Sessions

In the smaller locations where one or two sessions were held, it was not feasible to hold makeup sessions due to the interactive nature of the sessions. In the larger locations where individuals had ample opportunity to attend, plenty of sessions (20 to 25) were scheduled. For the 10 percent who could not attend a session, the video was placed on the server at each location, and the users were sent an e-mail containing a makeup packet that included some expanded slides to cover the interactive piece, together with a quiz required to be completed within three weeks. License agreements were negotiated with the video vendor to remain compliant



318 ■ *Managing an Information Security Program*

with copyright laws. This was an effective method of ensuring that training was completed for everyone, while minimizing the time involvement of the instructors for creating makeup sessions.

Final Thoughts

Training the associates is arguably the best use of the information security budget. Taking time in this very important step to make it fun, delivering a focused message, and highlighting the importance of information security will provide a return on investment unmatched by other efforts. Not only will the associates enjoy the training and learn, they will also be much more likely to view information security as critical to the business and be willing to be on alert for those items that they see are in conflict with the policy. This results in increased user awareness and reporting of those items as security incidents that can then be corrected. The rewards of delivering an interactive program are tremendous to the participants and the instructors. Before the training is even over, the participants are asking, “How will you top that next year?” and the instructors are already thinking, “What can we do next year?” By having fun, everyone wins.

Obtaining Executive Sponsorship for Awareness and Training

(Michael J. Corby)

Michael J. Corby, CCP, CISSP, is Director, META Group Consulting. He has over 35 years of experience in IT strategy, operations, development, and security. Mike has successfully managed large projects and developed flexible IT infrastructures and sound security organizations for hundreds of the world's most successful organizations. He is also the founder of (ISC), Inc.,² the organization that established the CISSP credential. In 1992, Mike was named the first recipient of the Computer Security Institute's Lifetime Achievement Award. A frequent global speaker and author, he formerly held executive positions with several global consulting organizations including Netigy Corporation and QinetiQ prior to joining META Group Consulting in July 2003, and was formerly CIO of a division of Ashland Oil and of Bain & Company. A business owner for over 15 years (M Corby & Associates, Inc.) and a community supporter, he has established a reputation for creativity and excellence in