Can We Make Security Awareness Training Stickier?

By Kerry Anderson – ISSA member, New England, USA Chapter

Most information security practitioners, on occasion, have had some frustrations regarding the relative effectiveness of security awareness education, leading some to consider whether it is worth the cost because incidents created by end users continue to occur. This article discusses some techniques to increase the “stickiness” of security awareness training efforts and increase the return on investment.

Abstract

Most information security practitioners, on occasion, have had some frustrations regarding the relative effectiveness of security awareness education, leading some to consider whether it is worth the cost because incidents created by end users continue to occur. Some cynics have come to view some security awareness training efforts as little more than a means to an end in maintaining compliance with external regulatory requirements. There is often a tendency to put the blame on the users or lack of executive support rather than the training itself. Perhaps a more productive approach might be to find ways to enhance the retention of security awareness messages. Many training programs use repetition as a primary strategy and it is not always an effective way to incorporate conceptual learning with the objective of affecting long-term behavioral changes. We need to make the training “stickier” to increase the overall retention of security concepts and achieve compliance with behaviors that support this training. This article discusses some techniques to increase the “stickiness” of security awareness training efforts and increase the return on investment.
The primary issue with this type of compliance-for-compliance-sake-only training is that it demonstrates a tone from the top that information security is not valued.

However, even when organizations demonstrate a clear commitment to information security and invest in offering regular awareness education, some security practitioners may question its degree of effectiveness in preventing security incidents with a human protagonist as their root cause.

Recently, a series of articles have discussed the return on investment (ROI) that organizations receive by including security awareness training as a component of information security programs. Dave Aitel argues that money spent on awareness training is money wasted because incidents created by end users continue to occur. Aitel states that these programs are generally ineffective and unnecessary due to the deployment of effective and automated security tools. Ira Winkler, security expert and author, countered in a rebuttal article and made a strong case for the importance of security awareness training. Winkler stated that information security should not rely entirely on technical controls alone because attackers will seek out the chinks in these controls to penetrate security boundaries.

While technical controls have diminished some security threats once associated with end-user actions and inactions, such as failure to patch operating systems promptly or maintain current antivirus definitions, these improvements do not eliminate the need to consider the importance of the human factor in protecting the organization against cyber attackers. No technology is foolproof and if one were, it would likely not be cost effective or user friendly. Humans are very adaptive and innovative when faced with a challenge. This is especially true when individuals view a control as a barrier to productivity. In the beginning of his 2002 book, The Art of Deception: Controlling the Human Element of Security, Kevin Mitnick, infamous hacker and social engineer, uses the famous quote by Albert Einstein, “Two things are infinite: the universe and human stupidity; and I’m not sure about the universe.” No matter how much technology is applied to an issue, it only takes one human mistake or action to defeat the technology and open an organization up to attacks. However, human beings and their awareness of security issues is a significant asset to organizations. Employee awareness of data breaches is important; for example, a employee uncovered a breach after noticing unusual behavior. The book, The Cuckoo’s Egg, documents just such a case. Clifford Stoll managed computers for Lawrence Berkeley National Laboratory in California. While attempting to resolve a 75-cent accounting error, Stoll uncovered a hacker attempting to obtain defense data to sell to a foreign spy organization. The value of human judgment is why some technical controls require human input before initiating an extreme action or one from which there is no return. Information security awareness training is a layer in an effective defense-in-depth strategy. To quote Winkler’s article, “The return on investment for a security awareness program of this form can be huge, even if it prevents a single incident.”

The core issue may not center on the necessity of including security awareness as a component of an information security program itself, but rather the perceived effectiveness of this training. In the movie musical 1776, there is a poignant scene where John Adams reads a dispatch from George Washing-

---

5 http://www.imdb.com/title/tt0068156/.
Can We Make Security Awareness Training Stickier?

Kerry Anderson

12 – ISSA Journal

Fred Scholl, PhD, CISSP, CISM, CHP, is a security consultant based in Nashville, Tennessee. A member of ISSA Middle Tennessee Chapter, he may be reached at freds@monarch-info.com.

Reading Outside the Lines...

By Frederick Scholl

ISSA member, Middle Tennessee, USA Chapter

Betraying the Gods

The ancient Greeks were obsessed with secrets in their mythology. Consider the tale of Sisyphus, banished to Hades to roll a rock up the same hill forever. His crime: revealing the secrets of Zeus. Or consider the tale of Prometheus: he was punished for not revealing his secret to Zeus.

A modern epic tale of secrets is told in Andy Greenberg’s page turner of a book, This Machine Kills Secrets. The book traces the history of WikiLeaks, from a technical side, people side, and political side. On the technical side are the challenges of safely using any anonymizer in the face of challenges of nation-states or other determined organizations. Readers will not miss the irony of leaking DOD secrets through Tor, a system developed and originally patented by the US Navy. Greenberg provides detailed profiles of his cast, and the human challenges of securing leaked information from further uncontrolled secondary leaks. These challenges ultimately, as he says, caused the secret-killing machine to turn upon itself. Greenberg’s book is itself only a chapter in the continuing privacy saga. The Supreme Court recently refused to hear the AT&T NSA wiretapping case, thus upholding legal immunity for telcos. On the other hand, alleged leaker John Kiriakou was recently convicted with sentencing early next year; the trial of Bradley Manning continues.

A theme of This Machine Kills Secrets is the difficulty of providing anonymous communications through technology. Organizations such as GlobaLeaks have taken up the cause of creating tools to make this possible for average users. However, news headlines involving four-star generals illustrate the difficulties of using technical means to assure anonymity. We will still need thoughtful individual action and laws to insure the transparency of our organizations. Security technology alone will not make this possible. Large doses of trust and courage will still be required.

About the Reviewer

Fred Scholl, PhD, CISSP, CISM, CHP, is a security consultant based in Nashville, Tennessee. A member of ISSA Middle Tennessee Chapter, he may be reached at freds@monarch-info.com.

These words may summarize the feelings that even the most committed security practitioners feel after communicating awareness messages that appear to have limited impact on user behavior. There is often a tendency to put the blame on the users rather than the training. Perhaps a more productive approach might be to find mechanisms to enhance the retention of security awareness messages.

Many training programs use repetition as a primary strategy. This repetition strategy may be summarized as, tell them, then tell again (repeat as often as necessary). While this strategy may be an effective technique for memorization of the multiplication tables, it is not an effective way to incorporate more conceptual learning with the objective of affecting behavioral changes.

In the book, Made to Stick: Why Some Ideas Survive and Others Die,7 authors Chip Heath and Dan Heath discuss why some ideas endure while others quickly fade into the ether. Certain ideas get “legs,” such as urban myths, celebrity stories, and bad jokes. By incorporating certain elements of “stickiness” into security awareness training programs, it may possible to increase both the overall retention of security concepts and achieve compliance with behaviors that support these ideas.

Using some of the following techniques may increase the “stickiness” of different components of an information security awareness program:

1. Keep your message simple
2. Avoid FUD and security “voodoo”
3. Keep it current, fresh, and tangible
4. Avoid statistics
5. Use storytelling
6. Make it actionable

Keep your message simple

It is possible in trying to offer effective security awareness education that we fail to communicate the fundamental reason for the training. We may include important points, such as defining Personal Identifiable Information (PII), data privacy laws, compliance regulations, and strong passwords, but fail to mention that the end game is data protection. If we communicate the overall purpose of the training, the other components of the training can fall in line as supporting that key objective rather than a bunch of disparate actions that need to be taken. The message needs to be explicitly stated at the outset, such as “we need to protect our data.” This mes-

sage serves as a “theme sentence” for the rest of the training, and it helps participants organize supportive activities under a central “heading” in their brains. Sometimes we tend to create separate topic “containers” to learners’ minds, such as passwords and compliance, rather than the goals that they support. A core message may increase the flexibility, extensibility, and cost-effectiveness of training rather than giving it a narrower focus. It allows successive security awareness training events to reference and build upon each other.

**Avoid FUD and security “voodoo”**

What is the fastest way to lose your credibility with your audience? The answer is using FUD (fear, uncertainty, doubt). Many of us have had the experience of seeing a security practitioner use FUD as the primary tactic, usually supported by a number of statistics. The biggest issue with FUD is that it has been overused. The use of FUD as a primary security awareness strategy can lead to the creation of a “security theater,” a term introduced by Bruce Schneier. It describes a scenario under which the security controls proposed offer the perception of improved security, but in actuality does little or nothing to enhance the security. Some may argue that some compliance regulations, such as PCI-DSS, may promote security theater rather than an appropriate security awareness program and practices based on actual known risks. Security theater can put the focus on trivial procedures rather than on core behavioral changes. An example was a program that spent a great deal of time and money training employees to use a small placard when they left their work area that told visitors not to leave any materials for them. One might argue that some incremental security enhancement was derived from this practice. However, leaving items in employee’s mail slot in the unguarded mail area provided no more security than leaving items on their desk. In fact, it provided unauthorized individuals with the information that could potentially diminish security.

I love articles about innovative cyber attacks, such as turning common household objects into Wifi antennas. This stuff can be fun to discuss. It does create some immediate attention. However, highlighting this type of information may do more harm than good. I like to refer to these types of attacks as “security voodoo.” Sure security voodoo attacks can occur, but their potential for widespread application remains limited. Case in point, the articles in 2008 regarding the ability to cryogenically freeze RAM to bypasses disk encryption and read volatile memory. I remember one security analyst that frequently told this story to end users, stating that a $7 can of compressed air can defeat encryption. While this may be technically true, it is not a likely risk scenario. The net result could be decreased use of encryption in general because it is not viewed as an effective safeguard. While it might be sat-


---

**Discover the Power of Information at RSA® Conference**

Cybercriminals are on the lookout to uncover security weaknesses in your organization anywhere and anyway they can. To stay one step ahead of threats you need access to the latest security innovations and insights.

At RSA® Conference 2013, you will learn from a diverse array of experts as they provide their perspectives on the state of the security ecosystem and uncover how understanding the bigger picture can prepare you. A delegate pass gives you access to:

- **21** dynamic tracks with 7 new ones including CISO Viewpoints, Enterprise Defense and Security Mashup
- **450+** track and keynote speakers
- **350+** leading-edge exhibitors in our expanded Expo
- **275+** information-packed sessions over five days

**Register Now!** [www.rsaconference.com/issa](http://www.rsaconference.com/issa)

**Save $400** before Friday, January 25, 2013
Can We Make Security Awareness Training Stickier?

14 – ISSA Journal • January 2013

©2013 ISSA • www.issa.org • editor@issa.org • All rights reserved.

It is also important to consider themes and examples used in the training to make sure they are relevant and not dated. Bob and Alice need to get cooler and in touch with the times.

isos, blogs, and social media into your training arsenal. Make it real by providing tangible examples of security scenarios. Include concrete details to make the example more realistic and memorable. This aids in creating visual images that enhance recall.

Avoid statistics

Just say “no” to statistics or use them sparingly. Statistics may assist in underscoring a point, but they are often overused and difficult for participants to put into a meaningful context. If a statistic is used, giving its source increases its credibility. In general, very few participants are going to remember statistics after they leave the training session.

Use storytelling

People like stories and use stories to relate information. Before written language, early peoples used stories to pass down their history, promote cultural norms, and teach important knowledge. Security awareness training can use stories to make a point or teach a concept. Many participants in classes I have taught tell me how they remembered a concept because of a story I used to illustrate a point. The favorite was the importance of locking devices when I told how I left my unlocked VPN connection to tend to my younger nephew only to find my three-year-old nephew about to send my manager an email in “French” (his term for a page full of random characters).

Storytelling offers many benefits such as:
1. They are entertaining
2. They can be tailored to suit different audiences
3. They can be used to depersonalize a contentious or uncomfortable issue
4. They make the message more memorable

Stories create images in the mind that can improve retention and recall. Stories can help make ideas stick in memory. In their book, Made to Stick, authors Chip and Dan Heath explain why certain stories, such as urban legends, are remembered and passed along. One factor may involve vivid images in stories that engage multiple areas of the brain associated with memory.

I have had the pleasure of hearing Ira Winkler present a number of times. He is a master of memorable presentations using popular culture images and famous stories as unifying themes, such as spies in the movies Star Trek or The Wizard of Oz. We can relate to these images and they make the concept easier to recall even years later. Winkler includes many details in his stories that paint a strong visual image of the situation, which serve to increase retention in memory.

Make it actionable

Give participants a takeaway action to help cement the concepts presented. Each of us has a primary, preferred learning style. Visual, auditory, and kinesthetic are the three most common learning styles. While we all have a preferred style, by combining elements of more than one learning style, we can increase retention and comprehension. By utilizing techniques, such as storytelling, we can engage visual and auditory learning modes. The net result is increased comprehension and retention of learning. In addition, as any training instructor can tell you, knowledge that is not actively used soon after training, soon starts to fade. This is a learning phenomenon called “storage decay” in which memories that are not utilized are forgotten. The “forgetting curve” states that over 50% of learned information is quickly forgotten. However, learned and used knowledge sticks around for a long time. For example, if you are taking a word-processing class and then do not use it for two months, you will likely forget most of what you learned in the class. This can be summarized as the “learn then do” model for knowledge retention.

Giving security awareness class participants an actionable takeaway, such as making a list of work responsibilities dealing with sensitive information or sending an encrypted email, can increase the retention of the information presented in the class; then send a follow-up email after completing the requested action. The performance of an action also utilizes an

|
|---|---|---|---|---|
|1. They are entertaining | 2. They can be tailored to suit different audiences | 3. They can be used to depersonalize a contentious or uncomfortable issue | 4. They make the message more memorable |

9 Millennials, an abbreviation for millennial generation, is a term used by demographers to describe a segment of the population born between 1980 and 2000. Sometimes referred to as “Gen Y”– http://whatis.techtarget.com/definition/millennials-millennial-generation.

10 “Bob and Alice” are frequently used in security examples and diagrams.


12 http://www.raleighcharterhs.org/faculty/akoch/Documents/7/Memory.doc.
influencing technique called “commitment and consistency” by social psychologist Robert Cialdini, a leading expert in the psychology of compliance, in his book, *Influence: The Psychology of Persuasion*. When individuals make a choice or take an action, it creates internal and external pressure to behave consistently with that commitment. When you verbally commit to an action, it increases the chances that you will follow through with it. This can increase the “stickiness” of security awareness learning activities.

**Increasing the “stickiness” of security awareness training and the “Velcro theory of learning”**

Some types of learning are innate to us, such as language acquisition. However, we struggle with others, especially learning that utilizes abstract concepts, such as mathematics or security awareness. While we can try to make learning more fun, there is no substitute for study and practice. Authors Chip Heath and Dan Heath discuss the “Velcro theory of learning” in *Made to Stick*. It is difficult to get things to adhere to a smooth surface. However, with experience, our learning surface develops a rougher surface, like the little hooks on Velcro. Anyone that has any experience with Velcro knows its tendency to pick up bits of materials when it is exposed to them. This stickier surface facilitates additional learning by making it easier for new information to become attached and create connectivity with existing knowledge. The techniques discussed in this article will assist in adding “hooks” to improve the probability of security awareness training being retained and building a foundation for future training to leverage. The net result would be an increase in return on investment that organizations reap from their security awareness training efforts.


**About the Author**

Kerry Anderson is an information security and electronic records management consultant with more than 15 years of experience in information security. Kerry is a graduate of Anna Maria College’s Executive MBA program, Bentley University’s Masters in Computer Information System program, and Norwich University’s Masters in Information Assurance program with highest honors. She has spoken at numerous events and authored articles for industry journals. Kerry has been awarded the CISA, CISM, CRISC, CGEIT, CISSP, ISSMP, ISSAP, CSSLP, CFE, and CCSK. She is an adjunct professor in Clark University’s Cyber Security Graduate Program. She may be reached at kerry.ann.anderson@verizon.net.

---

Data Security at your Fingertips

Protecting your data has never been easier with Apricorn’s Aegis Secure Drives

- AES Hardware Encryption
- Secure PIN or Fingerprint Access
- Software Free Design
- No Admin Rights Needed
- Works on any Host

- Portable Drive
- Desktop Drive
- Biometric Drive
- Flash Drive

©2013 ISSA • www.issa.org • editor@issa.org • All rights reserved.