Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"SANS Security Leadership Essentials For Managers with Knowledge Compress
at http://www.giac.org/registration/gslc

Using Influence Strategies to Improve Security Awareness Programs

GIAC (GSLC) Gold Certification

Author: Alyssa Robinson, lyssanr@yahoo.com

Advisor: Stephen Northcutt

Accepted:

Abstract

Even companies with extensive, well-funded security awareness programs fall victim to attacks involving phishing, weak passwords and SQL injection, presumably the primary targets of user education. Either their users don't have the skills to avoid these pitfalls, or they lack the motivation to apply those skills. Psychologists and other social scientists have studied the roots of effective behavioral change and have solutions to offer. By exploring personal, social and environmental sources of motivation and ability, security awareness professionals can attack the problem from multiple sides and give users both the ability and the will to make necessary changes.

© 2013 SANS Institute, Author retains full rights.

© 2013 The SANS Institute Author retains full rights.

"**Another characteristic of human nature – perhaps the one that makes us more human – is our capacity to do the unnatural, to transcend and hence transform our nature**" -M. Scott Peck (Psychiatrist)

Introduction, what are influence techniques?

Many of the problems faced by information security professionals could be solved, or at least ameliorated, if people acted differently. If only they didn't click the link in that email, didn't download "free" software and movies, picked long and complex passwords, refused to allow tailgaters, referred suspicious callers to the proper authority, and so on and so on, our jobs would be so much easier (or so we tell ourselves). Getting people to act differently, however, is a skill (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). It does not rely on verbal persuasion alone. Verbal persuasion can be a powerful and convenient tool, but if behaviors aren't changing, even when appeals are backed by powerful evidence, security awareness professionals need to have other tools in their arsenals. With 71% of attacks targeting user devices in 2012 (Verizon, 2013), a failure to motivate the employee could mean a failure of the whole security program (Spitzner, 2012).

For many of these activities, it is apparent that behaviors have not changed. Accounts of phishing activity have been documented as early as the mid-1990s. SQL injection has been a favored attack technique for fifteen years and is still number one on the OWASP Top Ten list. Certainly Kevin Mitnick was not the first successful social engineer when he started back in 1975, but competitors in last year's Defcon Social Engineering Capture the Flag still managed to obtain useful attack information for all targeted companies (Hadnagy, 2012). In Dave Aitel's incendiary 2012 article, he cited an average click-through rate in phishing emails of 5-10% even for large organizations with strong security awareness programs, encouraging readers to spend the money instead on penetration testing and perimeter defense.

Clearly, lecturing and other attempts at verbal persuasion haven't managed to effect all of the change we need; in the end, single-source strategies are rarely the answer to complex

© 2013 The SANS Institute Author retains full rights.

problems (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008)). In many of the cases listed above, end users do know about the dangers. Security experts have warned them, confused them, and filled them with Fear, Uncertainty and Doubt. And yet, the ever-growing breach statistics show that many people out there are not following through on what they have been taught. Pyschologists, social scientists and sales experts alike have studied the keys to addressing behavioral change and have some solutions to offer (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). These influence strategies are already being used by attackers, whether they are carefully constructing spear phishing emails to lure in unsuspecting victims or using social engineering to gather reconnaissance on target companies. The influence strategies themselves, however, are value neutral. They can be used instead to give the good guys the upper hand in the security awareness game, enabling users to operate technology safely (Spitzner, 2012).

What are the sources of influence?

People base their conscious decisions on whether they have the ability to do what is required and whether the effort will be worth it (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). Their unconscious choices are a kind of mental shorthand, a set of behaviors that have evolved to serve humans well in the most common or most dangerous situations (Cialdini, 2009). To really enact change, we must find the current sources of influence--whether they be conscious or unconscious, personal, environmental or social--that are keeping people from enacting vital behaviors (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). Personal motivations involve the feelings associated with an action, whether that means pride in a job well done, anger at being forced to do something or satisfaction at accomplishing a hard-won task. Social motivations come from peer pressure and interactions with others in a group, whether believing in the wisdom of the crowd or following an established leader. Environmental motivations can be very difficult to distinguish, coming either from the physical environment or the ways the culture of an organization rewards and punishes certain activities (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). How can a company claim to value its data security highly, for example, if employees are subtly discouraged from attending any security-related training with an emphasis on their total billable hours above all else? It is possible that just one of these motivational forces at work is stronger than all of the reasons we have outlined to change (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

© 2013 The SANS Institute Author retains full rights.

Vital Behaviors & Crucial Moments

"The primary purpose of security awareness is to change behavior." (Winkler, I. & Manke, S, 2013) One of the most important lessons that influence strategies teach is that to bring about positive change, security awareness professionals should be focused not on the big picture of what they want to achieve, but on what people must do. They must identify the behaviors they wish to change before they start trying to change them. Influence strategists call these keys to success 'vital behaviors'. Sometimes these vital behaviors are found through research, as in the case of diabetes, where the most successful individuals 1) test their blood sugar four times per day and 2) adjust their insulin in response to these controls (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). In other cases, the vital behaviors are found using the principle of "positive deviance": looking for the unique behaviors of those that have succeeded where other similar groups or individuals have failed. This model was used in the crusade to eradicate the Guinea Worm parasite in Sub-Saharan Africa. Doctors found two villages which drank from the same water supply, infected with Guinea worm larvae, but only in one of these villages did the people suffer from Guinea Worm disease. The doctors, from the Carter Center in Atlanta, noticed that women from the other village strained the water through their skirts, removing the larva and avoiding infection (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). Teaching the suffering village to enact this vital behavior was crucial in putting an end to Guinea Worm disease.

Equally important as identifying the vital behaviors that people must enact is identifying the crucial moments when they are most likely to fail in meeting these goals (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011). Whether it be a person new to exercise who falls off the wagon when he gets a case of the sniffles or a corporate IT user that lets someone tailgate through the back door because she doesn't want to seem rude, there will be times where people are far more likely to fail. If security practitioners can anticipate these moments and either give people tools to deal with them in advance or use personal, social and environmental factors to provide sufficient motivation at these key times, they will increase the likelihood that their users are successful. By keeping lines of communication open, they can also collect data on when and why people fail and use that feedback to improve the program (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011).

© 2013 The SANS Institute Author retains full rights.

So what are the vital behaviors in security? Internal testing and metrics around past incidents may put focus on the vital behaviors to target in a particular organization (Spitzner, 2012). This may include the behaviors that have led directly to a past incident or the recovery behaviors the organization needs to get back on track after mistakes have been made (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). Focusing on the types of risks that can't be fully covered by technical solutions and so need policy, procedure and education can also highlight vital behaviors (Spitzner, 2012). Augmenting organization-specific data are the in-depth breach reports published yearly by companies like Microsoft, Verizon and Trustwave, with a stake in the security space. These reports can highlight trends in the types of attacks that the Internet community is facing and help to focus the attention of security awareness professionals on current vital behaviors.

In the 2013 Verizon report, a breakdown of breach data across industry and company demographics shows that companies need to focus efforts in different areas to best cover the risks that affect them. That said, stolen and brute-forced credentials were breach vectors common to all of the targeted industries and demographics, with 76% of network intrusions analyzed for the report involving weak or stolen credentials (Verizon, 2013). Trustwave's 2013 Global Security Report similarly concluded that weak and default passwords were a notable risk. Their data from 2012 password breaches showed that the technical controls around password strength had limited effectiveness, driving most people to choose the bare-minimum 8 character password and allowing passwords to concentrate around key themes, with the top 100 baby boy names showing up in 20% of passwords, and the top 100 dog names in 16.7%. Baby girl names, US states, cities, and NFL and MLB teams all made impressive showings as well (Trustwave, 2013) These statistics point to following good password practices--picking passwords that are long, strong, changed frequently and not shared across multiple sites or people--(Spitzner, 2012) as possible vital behaviors to target.

29% of breaches covered by Verizon's report involved social attacks, including phishing . Phishing was the most popular social tactic across both small and large enterprises (Verizon, 2013). Phishing data from ThreatSim shows that in most organizations, an attacker needs to send only ten emails to guarantee that at least one user will click. Combine this with Trustwave data showing that not only do 1 in 10 spam messages contain either malicious attachments or links to

© 2013 The SANS Institute Author retains full rights.

malicious sites, but a full 10% of clicks to a Blackhole server result in exploitation and clearly this is a case where technical solutions do not provide full coverage of the risks for many companies.

Several other candidates for vital behaviors stand out in the data from 2012. Though most breaches (69% in 2012) are discovered when reported to an organization by a third party, end user reporting is the most effective internal method (still making up only 4% of breach discoveries). With average times before breach discovery stretching into months, improving this statistic could at least reduce breach impact; given that the time span between initial compromise and ex-filtration often spans hours or days, it may also reduce success of the initial breach (Verizon, 2013). Josh Corman, Director of Security Intelligence at Akamai Technologies has suggested that information security professionals begin targeting the "OWASP Top One", SQL Injection, rather than spreading efforts across the Top Ten (Roberts, 2013). Given that 73% of malicious infiltration cited in the Trustwave report used either SQL injection or remote access, this seems like a reasonable area of focus.

Personal Factors

Personal motivation and its counterpart, personal ability, are the most powerful sources of influence (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011). While many security best practices are not inherently satisfying—who wants to reach for that two-factor token on every VPN connection--security awareness professionals can tap into this source of motivation by linking people's actions to their values. By giving people an image of their best selves, and showing them how to stay true to that image, enacting "secure" behaviors can be made inherently satisfying (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). In an e-commerce company, this may be the thought of saving consumers from the pain of fixing their credit after identity theft, while at a hospital or government organization, it may be an image of protecting patients or citizens from the damage that can result from an invasion of their privacy. This personal vision as a protector of the company, the consumer, the patient or even their own hard work can act as a mantra to repeat to themselves when the right way does not seem worth the effort and management isn't watching (Hemp & Stewart, 2011). When values align with actions, employees are more excited to work and more productive (Meyerson, 2011).

© 2013 The SANS Institute Author retains full rights.

The conscious and unconscious minds are often at odds when it comes to people's behavior. The unconscious mind is following established patterns for quick action, based on millennia of survival tactics and evolution. In many cases, people will have to overcome these patterns in order to form new habits (Hogan, 2005). If asked, the conscious mind will invent stories to rationalize these things that the unconscious mind is telling them to do (Hogan, 2005). After a person has made a choice or taken a stand, however, he will encounter personal and interpersonal pressures to behave consistently with that commitment. While he might have agreed to take some action because everyone around him was doing it, or because he felt a sense of obligation, people use their own actions, and those of others, to decide what kind of people they are. The desire to behave consistently will drive people to honor a previous commitment to an ideal or an activity (Cialdini, 2009).

Successful salespeople use this quirk of human nature to succeed, employing what they call the "foot in the door" technique. By getting customers to say yes to a small request, they are much more likely to say yes to a larger request down the road (Hogan, 2005). In a 1966 study by Freedman and Fraser, published in the Journal of Personality and Social Psychology, homeowners were far more likely to place a large, ugly sign on their front lawn in support of a cause *after* they had agreed to sign a petition for that cause (Cialdini, 2009). If security awareness practitioners can use the heroic self-image they have created for their users as data and privacy protectors and inspire them to commit to one small act--like pledging to install a secure password manager or turn on two-factor authentication--they then have the potential to get larger commitments. As users begin to think of themselves as people who are security-conscious, they then begin to act in accordance with this image. This image can be strengthened by asking users for the reason for their choice, as people are far more likely to accept responsibility for a decision when they believe they have made it without outside pressure (Cialdini, 2009). In many cases, these behavioral changes can lead to attitudinal changes; if you want people to say yes, get them to DO something (Hogan, 2005).

Another well-known sales technique, the contrast principle, may encourage users to take that first action. The idea behind this principle is that two different items, presented one after another, will seem even more different than they actually are. If a security practitioner is trying to sell an idea or a behavior, first present users with a more difficult, more unpleasant or more

© 2013 The SANS Institute Author retains full rights.

expensive behavior. The second request will seem much simpler by contrast (Cialdini, 2009). For example, a security awareness professional might ask that everyone at the company report their fellow employees that allow tailgating to management immediately. By contrast, a request that they refer anyone who attempts to tailgate to the front desk will seem far less unpleasant.

Even when people know that a certain task or behavior is good for them, that it is something they want for themselves or for their future selves, they will put off those tasks if they are unpleasant. Almost everyone wants to, in a hypothetical sense, floss, eat healthier, exercise more and watch less tv, but how many are making these choices when faced with a big bowl of ice cream or an extra hour in bed? For tasks where there is no intrinsic satisfaction--for example, changing passwords regularly--how can security awareness professionals find a way to make that behavior desirable (or, in some cases, undesirable) (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008)? Changing the emotion associated with an activity is a powerful way to motivate this change in behavior (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). "Vicarious experience", using vivid stories that allow the listener to become a participant by identifying with the characters, is a powerful technique for affecting this emotional change (Hogan, 2005). Research by Vittorio Gallese and others at the University of Parma discovered the existence of "mirror neurons" in the frontal cortext that map the actions, as well as emotions and intentions, of others into our own brains. This happens not just when watching others act in real life, but while watching movies or reading stories and imprints these sensory and emotional memories upon us (Gallese, 2010). A well-told story, full of vivid details, can help set context for why users must change behavior in a way they will remember, with full emotional context.

These techniques can be especially helpful for the many users who experience a knee-jerk negative reaction when they are told they *must* perform some action, however benign. Salespeople use what is called an "Omega strategy", tempering this negative reaction by getting people to focus on the regret they will feel if they do not comply with the request and things go badly (Hogan, 2005). While personal experience is the most persuasive tool (Kim & Mauborgne, 2011), vicarious experience, using vivid stories, can be especially helpful when listeners mistrust the storyteller's credentials or motives; by identifying with the story's characters, the listeners themselves become a participant (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). Listeners will not merely empathize, but truly care about the results or consequences of their

© 2013 The SANS Institute Author retains full rights.

actions or inactions (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). By using vivid imagery to connect users with the regret they will feel if their inaction causes harm or leads to issues in their own life or career, and then giving them specific behaviors that will help them avoid that anticipated regret, they will have both the motivation and the ability to change (Hogan, 2005).

Social Factors; How we can be more influential?

Another powerful influence source available to security awareness professionals is peer pressure (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). In situations where people are uncertain about how to act, they are far more likely to look for "social proof"; the tendency is to assume a response is correct if many people are behaving that way (Cialdini, 2009). Concentrating on those with the most power to sway the crowd's mindset , the "influence leaders", will allow the message to move quickly through the organization. Influence leaders are people who are socially-connected and persuasive (Kim & Mauborgne, 2011), smart and open to new ideas (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). It is extremely advantageous to get the support of these influence leaders for a security awareness program, and even better for security professionals to become influence leaders themselves. According to Kerry Patterson in Influencers, influence leaders derive their power from four perceptions:

1. **They are knowledgeable and continue learning.** In general, people are only likely to carefully analyze arguments if they have a personal stake; otherwise they will accept the word of experts or those in a position of authority. (Cialdini, 2009). Here, the perception of competence is more important than actual capability (Hogan, 2005). Many factors are important in building this credibility. Security awareness professionals shouldn't hesitate to stress their own education, position or experience. Even though many in the substance-over-style security profession will reject the notion, neat, professional clothing carries authority that makes others more likely to follow the wearer (Cialdini, 2009). A fluid communication style demonstrates confidence and ease with the material, as does citing supporting evidence and being able to argue against one's own viewpoint to bring the listener around (Cialdini, 2009).
2. **They have others' best interests at heart.** It is difficult for a leader to influence anyone if his motives are mistrusted. People will be willing to accept the decisions of authority

© 2013 The SANS Institute Author retains full rights.

figures only when those leaders are seen as trustworthy, respecting the opinions of others in the decision-making process (Kramer & Tyler, 1995). When leaders are open to listening to their employees, employees will reward those leaders with trust, loyalty and hard work, giving them the benefit of the doubt when necessary (Garvin & Roberto, 2011).

3. **They are generous with their time and well-connected.** Historically, political outsider presidents have less success in their legislative agendas; because they haven't built up a network of indebted legislators, they have no one to call on in their hour of need. Humans have a hard-wired rule of reciprocation: "we should try to repay in kind what another person has provided us" (Cialdini, 2009). The sense of obligation to return a favor is so powerful that it works even when one person actively dislikes another (Cialdini, 2009). Frequent exposure, interaction and cooperation, however, are key factors in what makes someone likeable (Cialdini, 2009) and inspires others to comply.
4. **They speak their minds directly.** Confrontation and debate are essential and healthy: when employees are not able to talk about the real problems and the real reasons behind them, those problems will never go away (Garvin & Roberto, 2011). Influence leaders can help to create the environment where people give positive feedback about the right behaviors and confront the negative behaviors, by skillfully voicing the issues they have noticed themselves.

Many unconscious evaluations of a new person happen in the first 10 seconds upon meeting them. They filter into an overall "yes" or "no" reaction that can be very difficult to overcome later (Hogan, 2005). Mixed messages, either between words and body language or in other signals tend to make people uncomfortable and turn them firmly toward the "no" camp (Hogan, 2005). A speaker who claims to be open to questions while crossing his arms, for example, will shut down discussion right away. Many factors go into this overall judgment, including physical attractiveness, similarity in background or behavior, frequency of contact and associations or even just a smile (Cialdini, 2009). In general, people want to say yes to requests from people they know and like (Cialdini, 2009): at the Tupperware parties of the 1980s, an affinity for the host was 2x as important as affinity for the product in influencing how much gets bought (Hogan, 2005).

© 2013 The SANS Institute Author retains full rights.

Environmental Factors

The physical or cultural environment often influences choices without anyone realizing it, as in the often-cited case where larger plates cause people to eat more (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). To change behavior, the easiest thing to do may often be to change the environment and make the desired behavior easier to achieve. Conversely, the physical layout of a workplace can intimidate people, keep them from interacting--the best predictor of whether two people in an office will collaborate is the distance between their desks--or keep processes from working as intended (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). The environment or culture of the company may be forcing employees to unwittingly work towards a competing goal (Kegan & Lahey, 2011). Effective use of environmental cues can also serve to make the invisible visible, calling attention to relevant factors or reminding people of the way things should be done. In one hospital, administrators reduced costs by putting an actual price sticker on the much costlier latex-free gloves to remind people that they should only be used by those who need them (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). In the security arena, doors that close quickly, security cameras or obvious signs might cut down on tailgating, custom USB sticks might have photos of viruses to remind people to disinfect and security analysts co-located with other departments could encourage collaboration.

Teaching New Skills Effectively

What looks like a lack of motivation is sometimes really a lack of ability (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011). Spotting a phishing email, picking good passwords, preventing SQL injection; these are all simple things for users to do, if they have learned the techniques involved. Once the vital behaviors have been identified, security practitioners must give their users the skills to meet their goals and live up to their new self-image of security-minded data protectors. As teachers, security awareness professionals must break down complex goals in short, clear achievable steps. In basketball, for example, a coach teaches a player to keep his elbow in, not to "score more baskets" (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). Studies by Dr. Ethna Reid, founder of the Exemplary Center for Reading Instruction, on teacher performance showed that the best teachers alternate between teaching and testing the new knowledge and reward even modest improvements consistently with positive feedback (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). The

© 2013 The SANS Institute Author retains full rights.

effectiveness of practice is greatly improved by immediate feedback (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008) ; psychology professor Mihalyi Csikszentmihalyi describes that state that people enter when they are constantly challenged just enough to improve their skills as flow. This flow state is intrinsically motivating, pushing people to advance their skills quickly and "gamifies" the learning processes by engaging the competitive nature (Bizify Editor, 2012). In cases where individual progress can't be quantified, it is helpful to measure how the organizations behaviors have changed or how behavioral change may have impacted key security metrics, like numbers of virus infections or security incidents. Sharing these metrics with the organization can also give users something to aim for, turning progress into a game and adding a social influence into the mix (Spitzner, 2012).

Rewards and Punishments

It can be tempting to rely heavily on carrots and sticks to coerce users into following good security practices. Both rewards and punishments, however, can have unintended consequences. Rewarding people for an activity that they already enjoy makes that activity less desirable; the receiver of the reward begins to question the intrinsic value of the activity (Kohn, 1994). Even honoring certain employees that follow the new standards may backfire, causing others to feel resentful (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). What's worse, punishing those that don't comply may result in rebellion or learned helplessness among employees, especially when punishment is not administered consistently (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

In general, extrinsic rewards should not be the first strategy; use them only in conjunction with motivational strategies that encourage intrinsic satisfaction and social support (Kohn, 1994). Reward behaviors that support valued processes, with small, gratifying perks that are clearly tied to vital behaviors (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). Create short-term goals and celebrate small improvements in those vital behaviors, rather than waiting for the final goals to be achieved (Kotter, 2011). If penalties must be used, it is better to rely on the loss of a carrot than a stick (Lapowsky, 2013), as in most cases people will value something highly and work to keep it if they know it is something that can be lost (Schneier, 2008). If a yearly bonus, for example, or even just a perk, can be tied in some part to security goals, people will work hard not to lose that potential reward.

© 2013 The SANS Institute Author retains full rights.

An Example: Putting Influence Strategy to Work

Matthew is the head of the fledgling security awareness program at the fictional "X" Corporation. As a government contractor and provider of laboratory testing for genetic conditions, X Corp is subject to several compliance standards that require security awareness training. Matthew is determined to create a program, however, that's more than just a compliance checkbox. He has determined, based on X Corp's incident reports over the last year and on comprehensive breach reports that phishing and good password practices are important areas where he needs to focus education for X Corp's users.

Avoiding phishing and having good password practices are important, but they are not exactly vital behaviors. Much like the basketball coach must break down "scoring more baskets" into concrete actions like "keeping elbow in" that a player can practice, Matthew must decide what the key skills are for X Corporation's users to learn. For phishing avoidance, Matthew focuses on three vital steps: using a bookmark or typing in a known URL whenever possible, hovering over links before clicking if necessary and entering a dummy password. He repeats these key messages throughout the presentation, using the mnemonic "bookmark, hover, dummy pass". Matthew knows that X Corporation's users have logins to dozens of systems, both internal and external. Some, like their Active Directory credentials, they will enter multiple times a day. Others they will use once a week, once a month or once a year. While a federated authentication system would reduce the burden on users, one won't be rolled out at X Corp for at least six months. Matthew plans to teach users about how to create pass phrases for their common accounts and about using a secure password manager application, for which X Corp has an enterprise license, for the web-enabled and less common accounts.

Matthew knows that most of X Corp's users have heard about the dangers of phishing and about good passwords before. He has also seen the yellow sticky notes near keyboards and heard users complaining about the 60 day password rotation policy, so he does not believe they are sufficiently motivated to connect the dangers to their own behavior. Matthew understands that he must use all three sources of influence: personal, social and environmental, to drive home the message that these vital behaviors are important enough to enact consistently, even if there is a learning curve or a slight inconvenience.

© 2013 The SANS Institute Author retains full rights.

At Matthew's first Security Awareness training, attended by roughly half the company, he receives an introduction by the CTO. He is new to the company and needs to use the influence of this powerful and well-respected leader to lend some credibility. The CTO outlines not only his own support for the program, but gives an overview of Matthew's background and education, highlighting some key successes from programs he has managed in the past. X Corporation is a casual business environment, full of scientists and engineers, so Matthew doesn't go as far as wearing a suit and tie, but he does dress neatly and professionally. He has refined his presentation over the last month and it is smooth and polished.

He begins his presentation with a story about Emily. Emily is in school, getting her master's degree in education, very close to her lifelong dream of being a science teacher. She and her husband are also thinking of starting a family. Emily's mother had Muliple Sclerosis and died relatively young; Emily worries that she could face the same fate or pass it along to her offspring. Emily's grandmother also battled breast cancer, meaning an increased likelihood Emily might face the disease in her future. She opts for genetic testing, which her doctor sends to X Corporation's laboratory, to determine whether she is at increased risk for MS. Emily's uncle, who is interested in genealogy, has signed up for '23 and Me' a genetic testing service that allows users to share genetic profiles to look for relatives. Several scientific articles in the past few years have demonstrated the privacy risks of re-identification for relatives of people who use these services. Matthew reminds X Corporation of the discrimination Emily might face if a potential employer or insurer knew about Emily's increased risks for these diseases. X Corporation tested hundreds of samples daily for patients like Emily, protecting their privacy was a moral imperative. Failure to do so could also mean huge fines and other penalties for X Corporation and could drive it out of business.

When Matthew reached the part of his presentation that dealt with passwords, he again told the audience a story. This time, it was the story of a fictionalized X Corporation employee, Sue. Sue was a scientist working in a lab. She had a password to log into Active Directory that she used multiple times a day and had no problem remembering. She also had logins to the company intranet, the secure file sharing site X Corp used to send results to doctors' offices, the HR and payroll websites, the lab management system, several pieces of lab equipment, ordering systems for the lab and external support sites. That was just for work. Personally, she had

© 2013 The SANS Institute Author retains full rights.

Facebook, Linkedin, Google and all sorts of shopping sites. Last year, when Linkedin was hacked, she was forced to change her password for that site, but she was still using that same password for several of the internal systems. Matthew then shows lists of the most common passwords from breached sites over the last few years, including the password Sue used. He demonstrates how an attacker might use Sue's password to log in via the company VPN and then to the lab management system, grabbing Emily's test results, along with a thousand other patients. Matthew focused on the issues that X Corporation would face for the breach as well as Sue's personal feelings about her involvement. He outlined the ways in which Sue could have made different choices and avoided lots of problems for X Corp and its patients.

Matthew demonstrates in the training how to log into the secure password manager app and how to use it to generate and save secure passwords. He asks employees who would like to use the tool to help improve security for X Corporation to raise their hands, employing the power of social proof and then to add their name to a list, so that IT can help them install and add them to a mailing list. By making this commitment, the employees have stated that they are people who care about information security at X Corporation. This small step not only makes them more likely to respond to a larger request, it gives them a strong imperative to act consistently with this view of themselves. After the training, Matthew can use the new mailing list to send out tips on how to use features of the secure password manager. He can track how many people have signed up and publish per-department metrics in the security newsletter, fostering a spirit of competition. He can also train helpdesk personnel on common questions on the software, making it easier for people to use, and ask them to install for new employees.

Matthew has created a game for the next part of his presentation. He divides the audience into two teams and shows a series of emails, asking them to spot the phish. Each time a team correctly identifies a phishing email, Matthew asks a team member what clued him in to the phish. He asks how users should treat the email in every case. He throws out candy for correct answers. For incorrect answers, he spends extra time showing the clues and emphasizing that it is easier to defeat phishing by following the vital behaviors every time. After the training, Matthew secures management approval for monthly phishing simulations, giving users instant feedback and training opportunities in more realistic scenarios and giving Matthew metrics that he can use to track the success of the program. Matthew also teaches the users what to do if they have

© 2013 The SANS Institute Author retains full rights.

clicked on a link and suspect it wasn't legitimate. They can report the click in person, over the phone or using the helpdesk application and should include the suspected phishing message as an attachment. No user will ever be harassed or punished for the act of reporting this or any other suspected breach; by acting quickly, they can help limit the damage and keep others from falling victim to the same threat.

Outside of the training, Matthew is often seen walking through parts of the building far from his desk. He volunteers for projects that let him interact with lots of different departments and new people. He holds security "office hours" where people can ask questions or get help and stays up to date on the latest developments in both the security arena and the technologies used by X Corp. He convinces X Corporation management to include security in the yearly goal setting for other departments, so that employees can be rewarded for time spent making X Corp more secure. His network of contacts helps him succeed in his ambitious agenda and his program shows results. He has become an influence leader at X Corp and beyond.

Conclusion

Whether the data is payment card numbers, intellectual property or other PII, "valuable data makes businesses a target" (Trustwave, 2013). The key goal for a security awareness program is to reduce the risks that these targets face to an acceptable level, for both the rare, directly-targeted "advanced persistent threats" and the far more common, slightly less dangerous threats that cast a wide net (Spitzner, 2012). To do this, awareness professionals must increase users' ability, making the right things easier to do and the wrong things more difficult (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). They must also make it worth the effort to do the right things: using personal, social and environmental motivators that can connect them to their values, impress their peers and lead them gently in the right direction. Security awareness professionals can use the lessons of other successful change agents to create training and reinforcement that inspires, rather than scares users to exercise their new-found skills.

© 2013 The SANS Institute Author retains full rights.

References

Aitel, Dave. (2012, 07 18). Why You Shouldn't Train Employees for Security Awareness. *CSO.* Retrieved from http://www.csoonline.com/article/711412/why-you-shouldn-t-train-employees-for-security-awareness

Bizify Editor. (2012, 12 08). Gamification Theory: Flow [Blog post]. Retrieved from http://bizify.co/gamification-theory-flow/

Cialdini, R. (2009). *Influence: Science and practice*. (5th ed.). Boston: Pearson.

Garvin, D. & Roberto, M. (2011). Change through persuasion. In *HBR's 10 must reads on change*. Boston, Mass: Harvard Business Review Press.

Gallese, Vittorio. "From Mirror Neurons to Embodied Simulation." Arnold Pfeffer Center for Neuropsychoanalysis. New York, New York. 10 February 2010. Address, Retrieved from http://www.youtube.com/watch?v=PlV7F3MHuEk.

Hadnagy, C. & Maxfield , E. (2012). Social Engineering Capture the Flag Results: Defcon 20, Retrieved from http://www.social-engineer.org/resources/sectf/Social-EngineerDefcon20SECTFResultsReport-Final.pdf

Hemp, P. & Stewart, T. (2011). Leading Change When Business is Good. In *HBR's 10 must reads on change*. Boston, Mass: Harvard Business Review Press..

Hogan, K. (2005). *The science of influence: how to get anyone to say "yes" in 8 minutes or less*. Hoboken, NJ: John Wiley & Sons.

Kegan, R., & Lahey, L. (2011). The Real Reason People Won't Change. . In *HBR's 10 must reads on change*. Boston, Mass: Harvard Business Review Press.

Kim, W. & Mauborgne, R. (2011) Tipping Point Leadership. In *HBR's 10 must reads on change*. Boston, Mass: Harvard Business Review Press.

Kohn, Alfie. (1994). *The Risks of Rewards.* Retrieved from ERIC Database. (EDO-PS-94-14.)

© 2013 The SANS Institute Author retains full rights.

Kotter, John. (2011). Leading Change. . In *HBR's 10 must reads on change*. Boston, Mass: Harvard Business Review Press.

Kramer, R. & Tyler, T. (1995). *Trust in Organizations: Frontiers of Theory and Research.* Thousand Oaks: Sage Publications, Inc.

Lapowsky, Issie. (2013, April). Rewards vs. Punishment: What Motivates People More? *Inc.* Retrieved from http://www.inc.com/magazine/201304/issie-lapowsky/get-more-done-dont-reward-failure.html

Merkow, M., Dudley, T., Vaughn, D., Gernand, V., Quade, T., Maughan, R., Pescatore, J., Merola, A. (2013). Hardening the human OS. *SANS Securing the Human*, Retrieved from http://www.securingthehuman.org/media/resources/planning/STH-HardeningHumanOS.pdf

Meyerson, Debra. Radical Change, the Quiet Way. In *HBR's 10 must reads on change*. Boston, Mass: Harvard Business Review Press..

Patterson, K., Grenny, J., Maxfield, D., McMillan, R., & Switzler, A. (2011). *Change anything: the new science of personal success*. New York: Hachette Book Group.

Patterson, K., Grenny, J., Maxfield, D., McMillan, R., & Switzler, A. (2008). *Influencer, the power to change anything*. McGraw-Hill Professional.

Peroco, Nicholas. *2013 Global Security Report* . Trustwave, n.d. Web. 8 Sep 2013. Retrieved from http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

Roberts, Paul. (2013 06 13). OWASP Releases New Top 10. Is That 9 Too Many? [blog entry]. Retrieved from http://www.veracode.com/blog/2013/06/owasp-releases-new-top-10-is-that-9-too-many/.

Schneier, Bruce. (2008 01 18). The Psychology of Security [blog entry]. Retrieved from https://www.schneier.com/essay-155.html.

Spitzner, Lance. (2012). *Securing the human: building and deploying an effective security awareness program*. SANS Institute. (Vol. V2012_0410).

Verizon Risk Team. (2013). *Verizon Data Breach Investigations Report*. Retrieved from http://www.verizonenterprise.com/DBIR/2013/

© 2013 The SANS Institute Author retains full rights.

Winkler, I., Manke, S. (2013). 7 Reasons for Security Awareness Failure. *CSO Security and Risk,* Retrieved from http://www.csoonline.com/article/736159/7-reasons-for-security-awareness-failure

© 2013 SANS Institute, Author retains full rights.

© 2013 The SANS Institute Author retains full rights.

Last Updated: July 4th, 2015

Upcoming Training

SANS London in the Summer 2015	London, United Kingdom	Jul 13, 2015 - Jul 18, 2015	Live Event
Community SANS New York MGT512	New York, NY	Jul 13, 2015 - Jul 17, 2015	Community SANS
SANS Minneapolis 2015	Minneapolis, MN	Jul 20, 2015 - Jul 25, 2015	Live Event
SANS San Jose 2015	San Jose, CA	Jul 20, 2015 - Jul 25, 2015	Live Event
SANS San Antonio 2015	San Antonio, TX	Aug 17, 2015 - Aug 22, 2015	Live Event
SANS Virginia Beach 2015	Virginia Beach, VA	Aug 24, 2015 - Sep 04, 2015	Live Event
SANS Chicago 2015	Chicago, IL	Aug 30, 2015 - Sep 04, 2015	Live Event
SANS Crystal City 2015	Crystal City, VA	Sep 08, 2015 - Sep 13, 2015	Live Event
Mentor Session - MGT 512	Calgary, AB	Sep 10, 2015 - Nov 12, 2015	Mentor
SANS Network Security 2015	Las Vegas, NV	Sep 12, 2015 - Sep 21, 2015	Live Event
Mentor Session - MGT 512	Charlotte, NC	Oct 13, 2015 - Dec 15, 2015	Mentor
SANS vLive - MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™	MGT512 - 201511,	Nov 03, 2015 - Dec 03, 2015	vLive
Security Leadership Summit & Training	Dallas, TX	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Cyber Defense Initiative 2015	Washington, DC	Dec 12, 2015 - Dec 19, 2015	Live Event
SANS Las Vegas 2016	Las Vegas, NV	Jan 09, 2016 - Jan 14, 2016	Live Event
SANS Security East 2016	New Orleans, LA	Jan 25, 2016 - Jan 30, 2016	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced