Information & Computer Security

The pathway to security - mitigating user negligence

Sarah Elizabeth Kennedy

The pathway to security – mitigating user negligence

Sarah Elizabeth Kennedy
Lipscomb University, Nashville, Tennessee, USA

Received 6 October 2014
Revised 9 March 2015
Accepted 20 December 2015

Abstract

Purpose – Through the use of effective training techniques and exercises, employees and users can be educated on how to make safe information security decisions. It is critical to the success of a total information security program that users are trained properly as they are a major layer of defense against malicious intent. The current methods of training people about information security are failing, and the number of user-related breaches increases every year.

Design/methodology/approach – By researching and observing current methods and comparing other fields of study, this paper describes the best methodology for modifying user behavior as it pertains to information security.

Findings – Through effective training practices, user negligence can be mitigated and controlled, and the information security program can be better practiced throughout entire organizations.

Originality/value – By using an effective training method to teach employees about information security, employees become an invaluable part of a company's overall information security strategy. By using this method, employees are no longer the weak link in information security.

Keywords Training, Education, Information security, User education, Behaviour modification, User awareness

Paper type Research paper

1. Introduction

In a recent study performed by Symantec, employee negligence and system glitches account for 64 per cent of data breaches; this includes information mishandling, violations of regulations, inadvertent data dumps, stolen/lost laptops and wrongful access (Hamilton, 2013). In another study by Symantec, it was found that 62 per cent of employees think it is acceptable to transfer corporate data outside of the company on personal devices and cloud services, and majority of those employees never delete the data (Symantec, 2013). With proper, effective employee training and awareness programs, user negligence data breaches and data misuse can be prevented before it even begins.

The mitigation for most types of user negligence is proper training and education. Currently, employee negligence breaches are increasing with every study performed. Based on the data, current tactics of employee information security and internet safety training are not working to prevent these risks. Commonly, employee training is restricted to a list of best practices such as"use a long password", but an easy-to-understand explanation is not given as to why it is important to use strong passwords. This is a mistake, and employees do not make the important connections to understand why information security steps are critical to the success of the company and themselves.

Information & Computer Security
Vol. 24 No. 3, 2016
pp. 255-264

2056-4961
DOI 10.1108/ICS-10-2014-0065

The biggest challenge in the usefulness of this study is information security professionals' acceptance. Taking the stance that employees do not care why, does not work anymore. Not every employee will respond to education the same way, but telling employees scary stories of the internet and giving them an overused check list of best practices to follow is not effective enough to prevent the rising number of security breaches due to not understanding why the check list is important. To help our employees understand why, information security professionals need to change their idea of what their employees care about. Some employees will not care about information security at work, but if you explain to them how to stay safe and how to keep their children safe online, it will affect the information security skills they bring to work and begin the changes in information security behavior.

2. Areas of alternate research

Although information security awareness is a relatively new field, formal education has been around forever. Therefore, it should be encouraged to use educational studies to see what types of phrasing and tactics are the most effective for the majority of people. When beginning the study of user negligence mitigation, it is important to understand what works from other fields of study. By collecting research from other fields of study, this approach is well rounded and backed by evidence that has already been proven through the ages. In the relatively new studies on information security, professionals must not be afraid to pull materials from other fields; their data will allow us to completely understand our own.

User-based education occurs in drug use prevention, and research has confirmed that scare tactics do not seem to be the best procedures to follow to encourage people not to use drugs; educating and discussing the side effects and consequences seems to keep people from using. The same research can be applied to educating about information security. In these two articles, the research preformed agreed that over-exaggerated scare tactics do not work in the long term (Corwin, 2011) and (Goldberg *et al.*, 1991).

In the field of organizational psychology, many studies have been done to understand how employees react to different situations. Adam Grant, a highly respected professor of organizational psychology at Wharton, has published many articles that are helpful in getting ideas of what methods of education work for the greatest number of employees. Adam Grant has completed research on healthcare professionals hand washing and based on the way the bathroom hand washing sign is focused, it will encourage employees at hospitals to take more time and care washing their hands (Grant, 2011). He found that when the signs next to the hand washing station focused on patient care instead of personal care, "soap and gel use increased by 33 per cent per dispenser, and healthcare professionals were 10 per cent more likely to wash their hands". Healthcare professionals viewed patients as a vulnerable group, and, therefore, they need more protection. Signs about personal care did nothing to improve patient health. As a major part of an information security program is signs and posters, his research can be used to help to create more effective awareness campaign posters.

3. What training is currently being used and why is it not effective?

There are many tactics that information security professionals use; one of the most popular is check list of best practices to keep at their desks. We have all seen these more

times that we can count, and, overall, they are not effective in modifying the behavior and attitudes of employees. For example, top tips for staying safe online:

> Keep your computer software patched. Update operating systems, applications, and antivirus software. Be wary of suspicious e-mails from unknown senders. Use strong passwords. Use a different password for every account. Back up your data. Etc […].

Although check lists are a good tool for quick and easy steps to follow, they should only be used in connection with other education classes and materials. On their own, they are not a good way to present information security. There are no reasons given to explain why these steps are important, examples of what could happen or the chance of something happening if they are not followed. If examples are given, they are fear-filled stories of the most extreme experiences. The list is generally applied out of context with no applicable uses or examples of how to do any of it. For example, "back up your data". It is a very important step for recovering lost information, but, generally, the average employee will not know how to do this or if the company is already doing it for them; more information would need to be provided for users to take any action with this step. One-step solutions are ineffective in educating the average employee.

When information security professionals start an education session, they commonly begin by establishing a really scary story of hackers and then creating a superhero stance for themselves. We commonly want to be seen as the good guy who is there to save the day and protect against the evil hackers. It is usually seen as a confidence builder to have the audience swoon over your amazing technical skills, and it establishes the credibility of the speaker. Being the superhero is great, except that it makes information security seem like magic or an unreachable goal by the common user. It is important to frame information security as a task that everyone can do, that defeating the hacker is not just for elite IT people.

Early in our lives, we go through some form of formal early education. In these early learning classrooms, teachers do not start with educating students by telling them horror stories of mistakes and consequences of not learning a subject; they begin by teaching the basic skills needed for the tasks. For example, if a teacher is going through how multiplication works, they would not begin by telling you that if you do not learn multiplication, you will never succeed in mathematics or life, the consequence is that young children do not understand, and it is on too large of a scale to become manageable. They start by using games to introduce the child to some of the key fundamentals without actually doing math. Then, they teach the basic rules and processes. Eventually, the students will begin to practice on hand outs and quizzes, but it takes time for practice and reinforcement. Information security training should be done in the same way. Do not begin by the harshest consequences possible, begin by presenting fun stories and games to engage the students' minds and give them manageable situations.

Another major mistake with information security awareness training is that the employees only need to take the class or online training once a year. In many other disciplines or activities, if you want to get good at something, you have to repeat that action often and actively think about it to have an effect. If people run a marathon and at the end they consider how much of a struggle the running was, they do not decide that they should run less often to be more rested; they practice running more often and force their body to adjust to the changes. The same way can be applied in

information security training programs; if you only train your employees once a year, they will not be very good at using those skills in their job roles.

4. Best practices for training

To consider all the key information when training employees, use a set of best practices that can be used with any type of employee education. It is comprised from many sets of lists and explanations for teaching lifelong skills. It is important to use this list alongside other examples of education tips, just like any quick list. Some steps for effective training are stated below (Ferrara and Wombat Security Technologies, 2012) (Rubin, 2012) (Munson, 2013):

- *Train often and in small doses*: People are more likely to retain more about a topic when presented in small doses more often. It allows people time to consider the overall topic by presenting them pieces at a time. For example, when you teach people history, you do not tell them about every event in one 50-min session, you present a couple of events over many sessions. The same is true for information security; some topics may go well together and some need separate training sessions to actually influence changes in behavior.
- *Vary the concepts*: By presenting concepts in different forms or using different methods of examples or explanations, more people will be able to relate to one or more of the examples. It allows for a relationship to be built between the person and the example that applies best to them and to change how the person perceives the concepts. For example, present the idea of social engineering with Cinderella's story and play a game to see who can think of a movie where social engineering has been used.
- *Relate to well-known activities*: By creating examples around topics that are already well known to people, they can create connections with the new concepts, and they are not as overwhelmingly difficult to understand. It also allows the person to be reminded of the new activates each time he/she thinks about the others. For example, use an umbrella as a metaphor for antivirus protections, and every time the employees open an umbrella, they will think about protecting against computer malware.
- *Involve the employees with exercises*: When people are actively involved in activities, they tend to remember the experiences better. Always try to use an exercise that gets more people involved and out of their chairs, when possible. Remember to never humiliate an employee if he/she gets the answers wrong. For example, the exercise of showing people a few e-mails and having them vote on the one that is a phishing scheme or giving each team a few e-mail options and have the team explain why they picked that e-mail to the rest of the groups.
- *Tell useful stories*: When telling a story, people create emotional ties between characters and reactions. People are more likely to pay attention to a story than to a flat concept. If you are in a global company training session, keep in mind that some stories do not translate well to different cultures. Use useful stories and not just worst-case example stories; people like to escape into stories. For example, use a fairy tale story to relate to information security concepts.
- *Present opportunities for reflection*: People need a chance to create their own ideas and think through them before they can have an impact on their actions. Always

give time for people to consider their own thoughts. There is not one right way to practice information security, and they might come up with a concept that you have never considered before.

- *Reinforce training with follow-up materials*: After people think about the presented training session, they might have questions. When appropriate, give people resources to find information on their own and give them your contact information for follow-up questions. It is always a good idea to show them the internal policies and procedures' websites for company-specific information. Try to also give them website information that they can share with their families and friends; some child-friendly sites are always good examples.
- *Maintain focus on what is best for the customer and personal life, not just to protect the company*: When possible, focus the training materials on home life and keeping their family safe, as well as the customer safe. If people can apply concepts to their family and personal lives, the workplace information security procedures will be easier to establish. Always mention to parents that they should be having online safety discussions with their families. Phrase statements, procedures and polices around customer protection.

5. What can proper training prevent?

The main goal of any information security program is to make sure the company is protected if something bad were to happen and to be able to continue business. Through the use of a good information security awareness program, you can mitigate user negligence or lack of understanding in your employees.

Hackers have gotten smart against IT people, and they know that IT people put a lot of effort and control into technical systems, so they have found other ways around our high-tech controls. They play on a human's natural emotions to find a way around our technical barriers. This is also known as social engineering. It will be important for the success of the information security awareness training to discuss many forms of social engineering tactics. Hopefully, by making the employees aware of these situations, they can identify and prevent them. Social engineering is also a place where you can tie in connections to the employee's family. Although it is a worst-case scenario, a well-known example of social engineering is kidnapping. Parents educate their children not to go with people they have never met; similar to that, companies must train their employees not to give information to people they do not know. In both situations, the bad person is taking a person that is very important, similar to malicious people who take information that is very important to companies. Just remember not to overdo the worst-case scenario of social engineering; it is very easy to overwhelm people with paranoia with this topic.

By using well-balanced information security training, information security professionals can help alleviate the fear of the unknown when using the internet. Right now, people see the internet as the place where a lot of bad things happen. By educating them that it is possible to use the internet safely, they will become less frightened by using it properly or by following procedures to keep them safe.

An information security professional's worst nightmare is being told that information security is too big of a task, and, therefore, the company cannot do anything about it. By using proper techniques for educating employees and management, people can be made aware that the program develops one step at a time and that the program

does not have to be perfect the first time through; similar to most areas, information security is a continuously changing and improving cycle.

Through a good employee training program, people can be made aware of the current policies in place and why they are important in a controlled environment. They can ask questions and even be encouraged to make comments on how they can be improved. Some polices employees just will not understand, such as having to lock their computer when the get up for a moment, and it is important to be able to explain why these policies are in place. This will also emphasize that information security is not just IT's job; it is everyone's responsibility. Mistakes in data protection affect everyone in the company, and, if everyone understands that, then user negligence can be stopped before it begins.

6. What exercises are effective?

The concepts behind information security can be very difficult to explain to users that do not have a passion or background in information technology. To educate users and other information security professionals, it has been found to be more effective to use analogies, stories, games, and real-world examples. If people can relate unknown concepts to processes they already understand, they will be able to apply the new information more effectively.

After any training activity is completed, remember to always give additional information resources and contact information for when people think of more questions to ask. Exercises will commonly lead to people to continue thinking about what they were shown or asked to do. If the activities were done correctly, people will want to talk about them later and might have additional questions and concerns.

6.1 Analogies – visual

Visual analogies are one of many tools to use to teach many different types of learners. As most people learn by doing, viewing or hearing, visual analogies can cover all methods. You can ask for volunteers to do an activity, you can talk though the situation and you can have visual props or images to use during an activity. Using a visual analogy for information security concepts makes the ideas less electronic and more hand held physical ideas. For example, password strength is a difficult concept to truly get people to understand the importance, so use a visual activity analogy, such as:

Begin by having three boxes or images of boxes in the presentation area. Explain to the group that the boxes are all the exact same and they are secured by a physical lock on the outside. Tell them about the three different types of "data" within each box (can be adapted to each type of business or departments):

(1) newspaper clippings;
(2) personal photos you share with family and friends; and
(3) bank account numbers and social security card.

Give the volunteers three different locks (or pictures of locks):

(1) a child's diary lock;
(2) a passphrase lock; and
(3) a finger print and combination lock.

Explain to everyone that the locks are like different levels of password complexity and strength. Request the volunteers to determine which lock should be used for each type of information. After they are finished, inform the employees that it is an information security best practice to use a different password for every account; it is ok to tell them you understand this is hard to remember, so sometimes password systems can be used to help remember passwords.

Review what locks the volunteers have assigned to each type of information: newspaper clippings would be your news website accounts; they need very little protection, so a shorter, less complex password can safely be used as long as there is no credit card subscription data attached to the account. This can be protected with the diary strength lock. Personal photos you share with family and friends would be your social media sites. They need a little bit more protection because people see these sites as their personal connections to friends and family. This would be protected by a passphrase lock.

Bank account numbers and social security numbers are crucial to the way our personal lives work. If these are compromised, it is very difficult to continue as normal; the same for a business if customer data or top secret blueprints are lost. These should be treated with the highest level of security and given a longer more complex password, even two-factor authentication if possible. It would be good at this point to talk about two-factor authentication, password complexity and passphrases. Explain that passwords are like lock and keys when keeping unwanted people out, they are only used to keep the bad person away for as long as it takes to change them or for the stuff on the other side to be void; they are meant to take time and be a distraction for the unwanted person.

This example for password complexity can be modified in many ways, from the examples of data and locks to the boxes (or systems) themselves depending on the subject you are wanting to emphasize on.

6.2 Analogies – metaphors

Metaphor analogies are effective tools that start with the most basic ideas that majority of people will understand. For example, most people took a health class at some point in their middle school or high school education, so using the human body to describe complex concepts is a perfect way for most people to make the applied connections between the ideas. For example, when teaching about cyber resilience, use the example of the human body.

Humans already live with a system every day that is very resilient and is the best example for complete understanding of cyber resilience, the human body's resilience. Our body is under constant threat by the germs and illnesses in the world around us, not unlike our network and computer systems that experience uninterrupted bombardment of computer viruses and malicious intent. We protect our body from illness by washing our hands often, not touching germ-filled places and getting proper nutrition. This can be compared to using antivirus, not going to websites known for malicious intent and keeping our computer up-to-date with proper software.

When our bodies give us signs that we are becoming ill, we are aware of those signs and we take steps to ensure we recover, such as by taking medicine, calling a doctor and sometimes consulting a specialist. In a technology world, these steps would be compared to knowing what to look for when infected by a virus/malware or targeted by

a threat, and knowing the steps in place to notify someone for help and sometimes calling the information security team or law enforcement if the incident is extreme enough. It is important to understand the side effects of medicine so that you do not cure a cold and accidently end up causing cancer. Similarly, you do not want react to a minor computer problem and cause a complete system failure. When your body has recovered from being sick, your body creates antibodies to ensure it does not happen again, and you usually have a follow-up meeting with your doctor to make sure you are back to normal health. This can be compared to updating your IDS/IPS to look for the same type of threats and block them or updating your antivirus signatures and having a meeting with all people involved for an after incident improvement meeting.

6.3 Fairy tales – parables

Using fairy tale stories is an excellent way to get people thinking about information security. Most individuals are familiar with some form of common tales. The stories allow a person's mind to vividly imagine what the story teller is explaining. People are also more likely to remember the stories and the information security concepts because they can use the examples in the story and would be more likely to retell the explanation to others, such as their children, because they would also know the stories. Fairy tales can be used to explain concepts to IT professionals and employees in all business units.

One of the stories to use is The Three Little Pigs. It is an excellent story to explain concepts of having strong outer defenses, disaster recovery, defense in depth and risk mitigation steps. Another story that can be used is Cinderella.

Once upon a time, three little pigs went out into the world to seek their fortunes. They began their lives by building houses. The first little pig built his home out of straw, because it was the easiest thing to do. The second little pig built his house out of sticks, which was a little bit better than straw. The third little pig built his house out of bricks, but he had to build a chimney to be able to continue living in the home (risk acceptance). One night, a wolf came upon the first little pig's home and said, "Let me in, Let me in, little pig or I will huff and I will puff and I will blow your house in!". "Not by the hair of my chinny chin chin", said the little pig, and the wolf blew his house down and ate the first little pig.

The wolf then came to the second pig's house made of sticks and repeated the same process and blew the house down. But, the second little pig had been following the local news and knew what happened to the first pig and knew it could happen to him too. So, he developed an evacuation plan and a service contract with the third pig to come to the brick home if something bad were to happen. So, he did not get eaten because he activated his emergency plan and escaped to the third pig's home to continue living (disaster recovery).

The wolf then came to the house of bricks and tried to blow in the house, and he could not because the house was too strong (strong outer defenses); but, the wolf was sly and saw a chimney on the brick house, so he climbed up on the roof. The little pigs saw the wolf climb onto the roof so they boiled a pot of water in the fireplace (risk mitigation – monitoring the common openings and applying secondary defenses). The wolf fell into the pot, and that was the end of the trouble with the big bad wolf.

After telling the story of the three little pigs, it would be important to go back through the key concepts and explain how they relate to what people do on a daily basis. For example, risk acceptance/mitigation is used in the story when the third little pig makes

an opening in his defenses. In the IT world, you have to allow ports or doors open to allow people to actually use systems, and, when you do that, it is important to have a risk mitigation strategy such as watching the ports for unwanted connections.

Disaster recovery programs are essential for companies to continue their business in case anything bad happens. If the second little pig had not planned and tested for the big bad wolf to come and eat him, he would not have survived (and in most versions of the story, he does not; but, my second little pig is smart). Most companies have a fire drill quarterly to practice their evacuation plan so that everyone knows what to do and remain calm; in IT, we perform similar tests on systems that have a the potential to fail. Creating, maintaining and improving outer defenses are very important in the information security world; it is the first line of defense against the outside world. After building the brick house, maybe the third little pig made repairs to any damage and planned to build a moat around his house to add layers of protection. IT professionals add more layers of security to the network such as password protection, firewalls, etc.

7. Continuation of research

Because of the lack of opportunities and restrictions on behavior analysis studies, this information is provided as a theory of improvement on the current processes and procedures that are currently followed in the field. In the limited testing and research done in other areas of study, these methods are the more effective in causing behavior modification and education in end-users than other less effective traditional methods.

In the future, there is room for improving these methods based on an official study of comparing multiple methods directly, but at this time, these methods are compared on a qualitative level.

8. Conclusion

Overall, using this method will be a step in the right direction for information security awareness programs to help eliminate user negligence in many forms. It is not a perfect solution or a set of exercises, but this field has room for a lot of improvements. By keeping concepts easy to understand, using everyday examples and keeping information security applied to personal lives, all people can learn and benefit from this approach. It is an information security professional's job to ensure that people outside of the field understand that information security is not just a technical-based responsibility; it is everyone's job requirement. Information security covers more than network and software security, it applies to protecting information in whatever form presented. Information security is not just important because we say so, it is important because it is the best thing for our customers. It is what we expect when we are the customer.

References

Corwin, J. (2011), "Do scare tactics work?", available at: http://pact360.org/blog/detail/do-scare-tactics-work (accessed 12 July 2013).

Ferrara, J. and Wombat Security Technologies (2012), "Ten commandments for effective security training", available at: www.csoonline.com/article/2131688/security-awareness/ten-commandments-for-effective-security-training.html (accessed 12 July 2013).

Goldberg, L., Bents, R., Bosworth, E., Trevisan, L. and Elliot, D.L. (1991), "Anabolic steroid education and adolescents: do scare tactics work?", available at: http://pediatrics.aappublications.org/content/87/3/283.short (accessed 12 July 2013).

Grant, A.M. (2011), "Patients' health motivates workers to wash their hands", available at: www.psychologicalscience.org/index.php/news/releases/patients-health-motivates-workers-to-wash-their-hands.html (accessed 12 July 2013).

Hamilton, R. (2013), "Mistakes are costing companies millions from avoidable data breaches", available at: www.symantec.com/connect/blogs/mistakes-are-costing-companies-millions-avoidable-data-breaches (accessed 12 July 2013).

Munson, L. (2013), "Information security training and awareness – paradigm shift required?", available at: www.security-faqs.com/information-security-training-and-awareness-paradigm-shift-required.html (accessed 12 July 2013).

Rubin, R. (2012), "Training in information security is vital, provided it's done right", available at: www.theguardian.com/media-network/media-network-blog/2012/dec/21/training-information-security-tips (accessed 12 July 2013).

Symantec (2013), "Symantec study shows employees steal corporate data and don't believe it's wrong", available at: www.symantec.com/about/news/release/article.jsp?prid=20130206_01&om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach (accessed 12 July 2013).

Further reading

Johnson, M. and Labs, J. (2010), "Risk management jeopardy", available at: https://jeopardylabs.com/play/risk-management-jeopardy4 (accessed 12 July 2013).

About the author

Sarah Elizabeth Kennedy received a bachelor's of Science from Murray State University's Telecommunications Systems Management program and a minor in Occupational Safety and Health in 2011. She received a master's of Science from Lipscomb University's Information Security program in 2013. Sarah's research is primarily focused in effective user education practices and improving security controls through understanding users' response to various types of awareness training methods. Sarah is currently a Security Vulnerability Engineer at HCA, Inc. located in Nashville, TN, USA. Sarah Elizabeth Kennedy can be contacted at: Sarah.Kennedy859@gmail.com