A. Michele Parrish

Dr. Phil Lunsford

ICTN 6823

22 July 2015

Importance of Individuals in Information Security

ABSTRACT

This paper looks at the role of individuals in information security. The goal is to show that you and I are assets and liabilities when it comes to securing information. Many times we are the first line of defense whether it's in choosing a good password, not falling prey to social engineering or in how we configure a firewall. Individuals must understand that company security is their responsibility and need to consider themselves an important component in protecting the company's resources. They need to be trained properly in order to implement the correct measures to protect the confidentiality, integrity and availability of data. This paper will examine effective training methods and ways to motivate individuals to take security seriously.

INTRODUCTION

Information system security has taken a front seat in the minds of many individuals and companies. We hear on a regular basis of individuals having their personal information taken and used to obtain credit cards and companies having breaches in their security systems like in 2013 when Target had a breach during the holiday shopping season. Hackers were able to penetrate

Target's network by using the password of the heating, ventilation and air conditioning (HVAC) system. Once they accessed the HVAC system they were able to connect to other Target systems. They gained access to data for over 40 million credit card users and the phone number and email addresses for over 70 million customers (Crosman 13). Even the government is not immune to hackers. In early June, the United States Office of Personnel Management (OPM) announced they had discovered in early April that an attack on their network may have compromised the personal data of about 4 million current and former employees (Curran 1). While companies are concerned about security, not many are offering comprehensive security programs. A 2012 Ernst & Young Global Information Security Survey showed that the top-rated area of risk-exposure was "careless or unaware employees". It was ranked as first choice by 37 percent of respondents. However only 9 percent of respondents ranked "security awareness and training" as a top security priority (Kaspersky, Furnell 130). Companies recognize the importance of educating users but have not implemented programs to do so. The focus has been on technology to secure resources. In this paper I contend that educating users on security is just as important, or maybe more important, than technical measures that are put into place to protect a company's data, environment and resources. It is after all, people that choose, configure and implement the technical measures so it all comes back to the individual. Individuals can be a weakness in information security management but they can also, if trained properly, be the best defense. In this paper I will discuss the importance of properly educating users in a manner in which they can learn the most by looking at learning styles and differences in generations. I will explore key ideas that can lead to improved security in a workplace: making information security personal to the individual and by leading as an example. Lastly I explain about security measures that are people oriented.

EDUCATION

A company cannot expect an employee to automatically know what they need to do to keep the company's information and resources secure. The company should implement a security education training and awareness (SETA) program. SETA is "designed to reduce the incidence of security breaches by communication polity to employees, contractors, consultants, vendors and business partners who come into contract with its information assets and keeping them continually alert to these policy requirements" (Whitman, Mattord 541). This type of training may also be called information security education (ISE), information security training (IST) and information security awareness (ISA) (Amankwa, Loock, Kritzinger 248). No matter the name of the program a company implements, the goal is to educate the user on what they should and shouldn't do to protect the company's assets. Education is continuous and the following are opportunities for providing training:

- When a new employee is hired
- After a computer attack has occurred
- When an employee is promoted or given new responsibilities
- During an annual departmental retreat
- When new user software is installed
- When user hardware is upgraded

(Ciampa 590)

LEARNING STYLES

Security education is not a "one size fits all" activity. Just like with traditional learning in a classroom individuals learn differently and the difference in learning styles should be taken into account when developing a SETA program. There are four different learning styles (Rolfe, Cheek 176). They are discussed below.

Visual/verbal: This type of learner learns best with "visual information in the form of written language". Lectures that have good slides or a written outline work well for this learner. Textbooks and notes are also beneficial to them. They like to study on their own and picture information that they are trying to learn. Lectures and textbooks are recommended for this learner (Rolfe, Cheek 176).

Visual/non-verbal: This learner needs to be presented with visual information as a picture or illustration. Visual aids, pictures and diagrams are helpful. They like to study in a quiet room and do not prefer study groups. They visualize material that they are trying to learn. Most are artistic (Rolfe, Cheek 176-177).

Tactile/kinesthetic: These learners need the hands-on experience. They like to be physically active in the learning environment. They want to practice what they learn. Demonstrations, working through scenarios and practical examples help them learn (Rolfe, Cheek 177).

Auditory/verbal: Spoken language benefit these learners. Lectures, listening to information or group discussions appeal to them. They can remember information by hearing it. They may like to say things out loud as they are trying to learn the

information. Talking through examples to explain how they work are beneficial to them (Rolfe, Cheek 177).

Learning Style	Learning Activities
Visual/verbal	• Visual representations of material (diagrams, flow charts, schematics, etc) • Color-code notes so everything on one topic is one color • Prepare summaries or outlines in your own words • Flashcards
Visual/non-verbal	• Visual representations of material • Color-code notes • See if there are any electronic displays of course material • Use symbol pictures and diagrams for words and ideas
Tactile/kinesthetic	• Hands-on practice • Highlight key points • Write down key words and concepts • Flashcards to learn steps
Auditory/verbal	• Prepare summaries or outlines in your own words • Study groups • Record training sessions/watch recorded training sessions • When studying, talk out loud

Table 1: (Rolfe, Cheek 177) and (Felder, Soloman)

Understanding learning styles are important to both learners and trainers. If a learner realizes how they learn they can develop new ways to learn and focus on the ways they learn best (Rolfe, Cheek 180). Trainers should make sure to teach material in multiple ways that would appeal to the different learning styles.

GENERATIONS

In a 1991 article Strauss and Howe stated that individuals of a particular generation have a "peer personality" and they share an "age location in history" so they tend to have the same mind-set (Johnson, Romanello 212). They have shared experiences like the Vietnam War or 9/11, shared "sacred space" like Woodstock that sustains a collective memory and shared mentors or heroes like Martin Luther King, Jr. (Johnson 2). Not all members of a particular generation may adhere to the characteristics of their generation but they have all lived through the same time period (Johnson, Romanello 212). The five main generations are Traditionalists (pre 1946), Baby Boomers (946-1964), Generation X (1965-1981), Generation Y or Millennial (1992-200) and Generation Z (early 2000s-present) (Johnson 2).

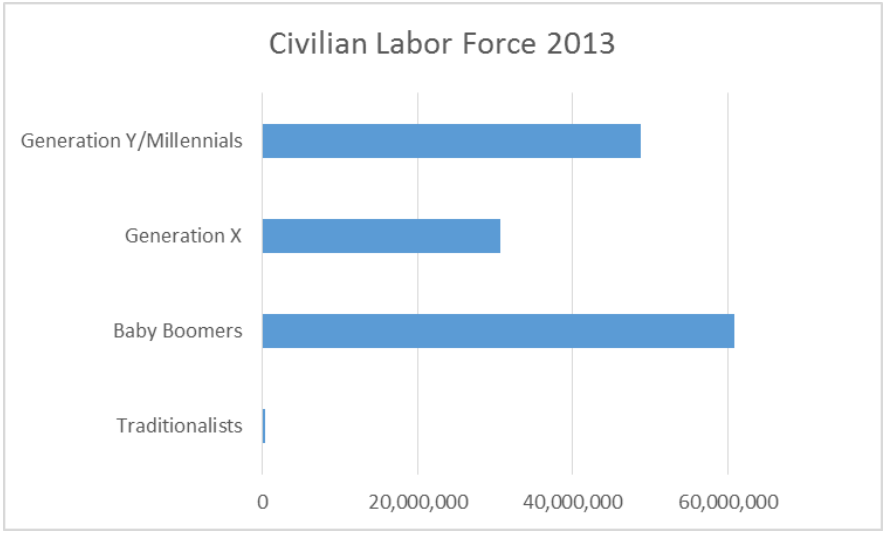

Chart 1: (Johnson 2)

Below are work place characteristics of each generation:

Traditionalists: They make up a minority of the current workforce because those that are living have retired. Most traditionalists are loyal and passionate about their job and have only worked for one employer. They like to be told what to do. They like structure and respect hierarchy in an organization. (Johnson 2).

Baby boomers: Boomers have been competitive their whole life and remain so in the work place. They are results-driven, focused on the job and tend to stay with an employer. Long hours and high levels of responsibility mean success for them. They will question authority and want to know why (Johnson 2).

Generation X (also referred to as latchkey generation): They are self-reliant and value informality and independence. They will work hard but desire a balance between their work and personal life so they want flexible work hours. They "thrive on diversity, challenge, responsibility and the ability to provide creative input". They will frequently change positions in a job and change jobs often. They like to work alone (Johnson 2).

Generation Y/Millennials: This generation shares many characteristics as Generation X but they take it to another level. They also seek a balance between work and their personal life. They are the generation that are most efficient at technology since they have grown up with technology. They are able to multitask. They want immediate feedback and praise from their supervisors who

should be involved in the Millennials' professional development. They prefer to work in teams and do it well (Johnson 2).

It important to understand generations and their work place characteristics and to understand how they view education. We can then develop education programs that take those characteristics into consideration. Baby boomers did not grow up with computers so therefore they are not tech savvy but they are willing to ask for help and accept it. They have a fantastic work ethic and will show up for each training session early and prepared (Johnson, Romanello 213-214). Generation X only want to learn things that they have to know for their job. They want the material presented to them in a way that is easiest and quickest to learn (Johnson, Romanello 214). Lastly Generation Y are computer savvy, want immediate feedback and access to information 24/7. (Johnson, Romanello 214).

Generation	**Training Considerations**	**Training Issues/Methods**
Traditionalists	• Less tech-savvy • Prefer in-person interaction	• Lecture-based training supplemented with written documentation
Baby Boomers	• Prefer in-person interaction • Want to know exactly what they have to do	• Lecture-based training with written documentation • Note taking • Open to self-paced training as long as resources are available

		• Tend to print training manuals and documentation instead of accessing them online
Generation X	• Dislike meetings about meetings • Hands-off supervision works best with them • Want to learn in the quickest and easiest way possible • Only learn what they need to know for job	• Short, easy assignments • Wants to know exactly what will be on tests • Flexibility in class time so self-paced learning works best
Generation Y/Millennials	• Are tech-savvy • Are collaborative • Want immediate feedback	• Online training • Web-based lectures • Group projects

Table 2: (Johnson, Romanello 213-214) and (Johnson 3).

MOTIVATION

Along with training individuals based on their learning styles and generational characteristics, organizations must also motivate their employees to follow through with the security education they have acquired. For example, Traditionalists will follow security practices because that is

what they have been told to do, other generations will not so companies must provide other means to motivate them. Baby Boomers want to know why they are expected to follow security practices; how does it affect them? Leach describes three kays to improving user security behavior (690). The three keys are senior management and peers demonstrating proper procedures, allowing a user to use their common sense and decision-making skills and a user having a strong psychological contract with the employer (690).

If time and effort has been taken to educate employees about proper security measures that should be taken to protect a company's assets but then those measures are not modeled, an employee will see no reason that they need to follow the protective actions. For example, if employees are trained that they should lock their office door whenever they leave the office and make sure that all company data is secure (files put away and computer locked) but they go past their supervisor's office and the door is open with the supervisor nowhere in sight along with computers files pulled up on screen and paper files open on the desk, they will think that it is not important to close their door and secure company data. The more they see actions that are in direct opposition of what they were trained to do, with no repercussions, the more likely they will be to not follow the training. If it's not important for the employee's supervisor or co-workers to do then why should the employee follow the policy? Modeling of appropriate security behavior must start at the top (Leach 690). This is especially important for Baby Boomers and Generation X (Johnson 2).

There is no way that users can be educated about every security incident that can happen. Security education should teach users about basic security principles and policies. Users should

learn enough that when faced with a new situation that can use their "security common sense" and make their own decision about what is right and what is wrong. Education may involve working through scenarios where employees use their decision making skills. Feedback and support should be continuous during the education process and with any real-life situation (Leach 690). Millennials crave the feedback and while Generation X like to make their own decisions (Johnson 2).

The last key is that employees feel a need to comply with a company's expectations and to behave in the way the company wants them to behave. This is called the 'psychological contract'. An employee will honor this contract as much as they feel like the company is honoring their end of the contract. How does a company honor their obligations? This varies from employee to employee (Leach 688). For a Traditionalist they are loyal to the company because the company gave them a job and a way to provide for their family (Johnson 2). Generation X is concerned about obtaining new skills and experience so they can move on to another job (Johnson 2). How much money they are making is important to the Baby Boomers (Johnson 2). For every generation part of the contract relies on the first key; the behavior must be practiced by managers and co-workers (Leach 691).

MEASURES

While there are many different security measures that can be put into place to help protect a company's resources there are a few that are people centric. The final section of my paper discuss these measures and best practices for each.

Security policies: Policies "deal with the processes and procedures that the employee should adhere to in order to protect the confidentiality, integrity and availability of information and other valuable assets" (Vroom, von Solms 192). Basically it outlays what should and should not be done by an employee in reference to security. These policies should be written in a manner in which they can be understood by users. If a user doesn't understand a policy then they will not be able to implement. Training on the policy should be provided. Lastly users should be able to contribute to policies. If a user has a vested interest they are more likely to follow the policy.

Password management: Passwords are an easy and many times a first line of defense in data protection. Users should be educated about creating strong passwords and managing their passwords. According to Campia a strong password:

- Does not consist of dictionary or phonetic words.
- Doesn't use repeated characters or sequences.
- Doesn't use personal information including birthdays, family member names, names of pets or addresses.
- Is not short. It should be more than 15 characters in length.

(487-488)

Users should have different passwords for each account they have to have a password for. These passwords should never be written down or shared with others. Passwords should be changed periodically. Many administrators will configure software programs so that a user is forced to change their password at a specified time and may require the new password to be unique, one that has not been used previously (Ciampa 482).

Social engineering: Social engineering is the "psychological manipulation of people into performing actions or divulging confidential information" ("Social Engineering (security)"). There are many different social engineering techniques but three common techniques are impersonation, phishing and tailgating.

Impersonation means to pretend to be a person and then "play out the role of that person on a victim" (Ciampa 68). An example would be that an individual pretends to be a member of the organizations' IT department and calls an employee and says that they are going to be upgrading UPS systems and will need to bring down the servers for a specific period of time and they want to make sure to not bring down the server your research is on. They ask you to confirm the name/IP address of your server. Since you don't want to not have access to your data you provide that information to the supposedly IT professional. Not an individual has information about the server your data is on. This is a first step in being able to gain access to your data. Users should be taught to not give out any personal information about themselves or company assets. If they truly believe the person is a member of the IT staff then ask for their contact information and call them back after you have checked with supervisors.

Phishing is "the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication" ("Phishing"). One type of phishing is phishing emails. Signs to look for that indicate that the email is not legitimate is bad spelling and/or grammar and emails that contain threats (that

something will happen if you don't do what the email directs you to do). Phishing emails may contain images of valid vendors and may have links that look valid but if you hover above the link it will actually redirect you to another site ("How to Recognize Phishing Email Messages, Links, or Phone Calls").

Tailgating is when a person follows an authorized individual into a building or location in a building (Ciampa 73). As individuals we have been taught that the polite thing to do is to hold the door open for the person behind you but in restricted access locations we should not do this. We should authenticate ourselves and be allowed access and make sure the door is closed behind us. If the person following us has the correct credentials and authorization they will be able to access the location. They will not think you are being rude because they have been educated about tailgating and the risks.

CONCLUSION

Information security is important today's world and is gaining in importance. More emphasis will be placed on security education in the future. We must make sure to not only educate users in what they are allowed to do and not do but we must find a way to make security a priority for them and part of every task they perform. When information security becomes second nature we will be able to ensure the confidentiality, integrity and availability of data.

Works Cited

*Amankwa, Eric, Marianne Loock, and Elmarie Kritzinger. "A Conceptual Analysis of Information Security Education, Information Security Training and Information Security Awareness Definitions".Infonomics Society , 2014. 248-252. Print.

Ciampa, Mark. *Security Guide to Network Security Fundamentals*. 5th ed. CENGAGE Learning, 2015. Print.

Crosman, Penny. "Target Breach Was Months In The Making." *American Banker* 179.23 (2014): 13. *Business Source Complete*. Web. 20 July 2015.

Curran, John. "CONGRESS FUMES OVER OPM HACK, OFFERS FEW NEW SOLUTIONS." *Cybersecurity Policy Report* (2015): 1. *ProQuest.* Web. 19 July 2015.

Felder, Richard, and Barbara Soloman. "Learning Styles and Strategies." *Felder & Soloman: Learning Styles and Strategies*. Web. 18 July 2015.

"How to Recognize Phishing Email Messages, Links, or Phone Calls." *What Is Phishing*. Web. 19 July 2015.

*Johnson, Peggy. "Generations in the Workplace." Technicalities 33.3 (2013): 2-4. ProQuest. Web. 21 July 2015.

*Johnson, Susan A., and Mary L. Romanello. "Generational Diversity: Teaching and Learning Approaches." *Nurse Educator* 30.5 (2005): 212-6. Print.

Kaspersky, Eugene, and Steven Furnell. "A Security Education Q&A." *Information Management & Computer Security* 22.2 (2014): 130. *ProQuest.* Web. 19 July 2015.

Leach, John. "Improving User Security Behaviour." *Computers & Security* 22.8 (2003): 685-92. Print.

"Phishing." *Wikipedia*. Wikimedia Foundation. Web. 20 July 2015.

Rolfe, A., and B. Cheek. "Learning Styles." *InnovAiT* 5.3 (2012): 176-81. Print.

"Social Engineering (security)." *Wikipedia*. Wikimedia Foundation. Web. 18 July 2015.

Vroom, Cheryl, and Rossouw von Solms. "Towards Information Security Behavioural Compliance." *Computers & Security* 23.3 (2004): 191-8. Print.

Whitman, Michael E., and Herbert J. Mattord. *Management of Information Security*. Fourth ed. CENGAGE Learning, 2014. Print.