Global Information Assurance Certification Paper

Social Psychology, Cognitive Psychology, Security and the User

Audra Burchfield

December 23, 2002

v.1.4b Option 1

1.0 Abstract

Most computer security incidents that companies encounter originate from the inside unintentionally. Employees are not aware that the program they think they are downloading contains malicious code such as a Trojan or virus. Likewise, non computer savvy users will not think twice before entering their password if in the middle of working, a window pops up saying they must re-enter their password to remain connected to the network, a probable occurrence if a Trojan has been installed on a computer.

For computer security operations to succeed, they need to be transparent to the user. Behaviors need to change. In order to change behaviors, one must look at the principles of social and cognitive psychology. This paper will address several security issues affecting the computer user and the practices currently applied to those situations. Possible solutions for protecting a computer system are also discussed.

2.0 Introduction

How many security breaches occur in the following scenario?

> John Doe reports to work at eight o'clock in the morning. As he enters his office, he holds the door open for another man who has forgotten his badge. John then proceeds to his desk and turns on his computer. A security warning banner pops up on the screen, however, John does not see the banner because he is flipping his keyboard upside down to looks at his password, which is written on a note. John enters his password and signs onto the network. John opens up his email and while it is loading, goes to get coffee. On the way to get coffee, John runs into his boss who wants to speak with him for 15 minutes. John returns to his desk and starts reading his email. He downloads a holiday greeting card that he received from a friend. In the afternoon, John is working on a report for his boss when a window pops up stating that he must put in a password to continue. John puts in his password and then remembers to save his work. At the end of the day, John shuts down his computer and goes home.

The possible security breaches in the above scenario include:

- Allowing a stranger entrance into the building
- Writing down a password
- Leaving a computer unprotected
- Downloading files from the Internet
- Giving out a password

These common incidents occur multiple times everyday. New technology is developed everyday to secure systems and prevent such incidents. A company or agency with the most up-to-date security technologies will still succumb to cyber attacks if the technology does not consider human behavior and if the organization's users are not sufficiently trained.

This paper will focus specifically on the government user, as there are currently many security standards and requirements, which government departments and agencies must follow.

3.0 Background

Federal agencies are required to comply with the Computer Security Act of 1987, Office of Management and Budget (OMB) Circular A-130, Appendix III, and the Government Information Security Reform Act (GISRA). These and other Federal Mandates were developed to keep information sensitive to the United States Government protected.

The Federal Government recognized the need for computer security in the Computer Security Act of 1987, stating that "Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use." (Computer Security Act of 1987)

In 1996, the OMB updated computer security standards for Federal agencies in OMB A-130, Appendix III, establishing a minimum set of controls to be included in Federal automated information security programs, which includes ensuring "that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system." (OMB A-130)

Although these mandates were in place, most agencies did not recognize the importance of these mandates until the tragic events of September 11, 2002. The terrorists' acts of that day and the new reporting requirements of GISRA have moved computer security to the forefront of every office of the Chief Information Officer.

The most recent reporting requirements for GISRA, date July 2, 2002, stated that "Protecting the information and information systems on which the Federal government depends, requires agencies to identify and resolve current security weaknesses and risks, as well as protect against future vulnerabilities and threats." (M-02-06)

Agencies are instructed to follow guidance from the National Institute of Standards and Technology (NIST). The NIST Special Publication (SP) 800-16 and draft 800-50 address security awareness and training. The NIST SP 800-16 states "Awareness is not training." (NIST 800-16) The OMB A-130, Appendix III requires agencies to provide "periodic training in computer security awareness." (OMB A-130) This statement could be interpreted to mean that displaying security awareness posters is sufficient to meet the awareness requirement. Using awareness activities alone, however, is not enough to change behaviors. All Federal computer system users should be trained in their security responsibilities such that the responsibilities become second nature and are not a burden to the user.

4.0 Security Banners

In the introductory scenario, John Doe's computer displayed a warning banner that John Doe did not even notice. As stated in Public Law 99-474, all federal agencies must display a warning banner on the screen of information systems for the user to view before he or she logs on to the network. (Swanson, p48) The warning banner states that the system belongs to the United States Government and only those authorized access are allowed access and that unauthorized access can be punished by fines and/or imprisonment. Most agencies have implemented the warning banner, but not in a manner such that it is an effective tool. In many agencies, the warning banner flashes up on the screen for less than two seconds in a font and size that is nearly illegible. In addition, the banner is always there, never changing. Thus, the banner becomes synonymous with the start up processes that the user does not notice; only paying attention once the log in screen is present. In order to be more effective, the warning banner should be legible and require user input that the statement has been read. The banner should also be changed regularly so the user does not begin ignoring the message.

5.0 Passwords

In the introductory scenario, John Doe turned over his keyboard to find his password, which he had written down. He also later gave that password to an unknown person as he entered it into a pop-up window.

Passwords are the users' method of authentication with their agency network.

Agency password policies are stringent for good reason. Any password can be cracked given enough computing power and time. Agencies aim to have a user's passwords be strong enough such that by the time the password is broken, the user has already changed to a new password. Knowing an employee's password (and userID) gives a person direct access to that agency's network.

As new cracking technology is developed, the requirements on the user for a strong password increase. Human beings do not have the capacity to remember long complex passwords. Remembering a password is complicated by the fact that most computer users have multiple different long complex passwords that they are required to remember for different systems.

At this point in time, the requirement for a strong password in most federal agencies is that the password is composed of at least eight characters, which are a combination of letters, numbers, and symbols. The combination of characters must not resemble a word or name that can be found in any language. Computer system users are required to create new, completely different passwords every 90 days.

5.1 Depth of Processing

Wanting to remember a password will not help a user remember his or here password. Deep processing involves thinking about the meaning of the password. Shallow processing involves thinking about the surface characteristics, such as whether a letter is capitalized or not. Some studies, such as Thomas Hyde and James Jenkins' 1973 study of intentional vs. incidental memory showed that the depth of processing is the determining factor in memory, that wanting to remember something does not help one remember that something. A user must therefore be able to translate the password into something that can be processed deeply in order to remember the password. (Willingham)

Mnemonics are a popular framework for retrieval, devices used to aid memory. An example of using mnemonics is creating the password "2BoNt8,T!t? by transcribing the first letter of each word from the quote "To Be or Not to Be, That is the Question." While users are required to continue using strong passwords, they should be trained in the creation of specific mnemonics, a process that will aid in deep processing.

5.2 Seven, Plus or Minus Two

In his 1956 paper, "The magical number seven plus or minus two: Some limits on our capacity for processing information," George Miller found that the number seven appears to be a limit on human performance. Miller found that people could remember seven plus or minus two digits in a digit span task. This

research could be applied to the length of a strong password and the user's ability to remember that password. As long as the minimum length for a strong password is nine or less, the effect on users will be minimal. (Miller)

6.0 Social Engineering

In the introductory scenario, John Doe may have been a victim to social engineering when he allowed someone entrance to the office, when he left his screen open without protection, when he received a electronic greeting attachment from a friend, and when he gave away his password. Social engineering is the discipline employed to find the weakest link in the computer security chain.

Social engineering methods of attack can be both direct, such as a simple telephone call to a company requesting an employee's phone number, and indirect, such as a person developing a relationship with a company insider in order to obtain a lot of information.

In psychology, a schema is a pattern imposed on complex reality or experience to assist in explaining it, to mediate perception, or to guide response. Schemas help people determine what is and what is not appropriate in a given situation. (Kabay) Many security policies conflict with most people's schema, for example:

- Growing up, most people are taught to hold open the door for the person behind them. Users are now being told not to allow anyone in the door behind them unless that person has the proper badges, even if that person is familiar.

- People are taught that they need to trust the people they work with not to affect the availability or integrity of their work, whether it be on the computer screen or sitting on the desk. When a user gets up from his or her desk without protecting the computer by logging off or using a password protected screensaver, other people within the office have the opportunity to sit down at the computer and gain access to the user's files, view x-rated websites, send nasty emails, or worse. Policies are beginning to require that users use password protected screensavers when they will be away from their desk from 10 minutes to 2 hours or to log off if they will be away for more than 2 hours.

- People are taught to trust their friends. When email attachments such as greeting cards are sent from friends, people do not believe that the attachment would be malicious in nature. Malicious attachments are mailed both intentionally and unintentionally. Over the past couple of years, the message has gone out not to open attachments from strangers. That message is changing to not to open attachments that are from strangers or from familiar people without first scanning the files for viruses.

- People believe that a window that pops up on the computer screen is a result of processes in the computer. Many people do not know that the only screen they should put their password in is the initial log-in screen. If a window pops up, telling a user that the computer will log off if they do not enter their password, he or she is likely to enter his or her password, especially if that user has not saved what he or she is working on recently. Users need to know that the only time to enter their password is when logging in or turning off screensaver protection. Users need to know that no person should ever ask another for a password, not even the help desk. Likewise, the help desk and supervisors should never ask a user for their password.

7.0 Possible Solutions

Although many IT salesmen would tell you that all of the breaches incurred in the introductory scenario could be made non-issues through their technology, this is not true. The implementation of a strong, easy to read policy through awareness, training, and reinforcement, in addition to the proper implementation of technological solutions, is the only way to minimize security.

7.1 Technical Solutions

Technical solutions that are options available in an agency's current operating system should be employed where applicable. Most companies and federal agencies have, or are in the process of, migrating to Windows 2000. With Windows 2000 and other new operating systems, employees without administrator access can be easily prohibited from downloading programs. If this were the case in the introductory scenario, John Doe would not have been able to download the electronic greeting and thus would not have downloaded a deadly executable.

Some agencies and companies are taking away floppy drives and CD-ROM drives from employee workstations to prevent downloads. Taking away methods of download will not work in all business areas. To protect the network, a company must determine the risks and compare them to the business needs.

There are many other technical solutions available for many of the widely known security threats. Note though that if the technical solutions to security problems do not include training, the solution will be improperly implemented and thus will not effectively protect the system.

7.2 Awareness

As stated in NIST Special Publication 800-16, the purpose of awareness is to focus attention on security. Awareness, although the only thing required of users according to NIST 800-16, is not sufficient to change security behaviors. In awareness, the user is the recipient of information. Awareness aim to make the user aware of the importance of information security through activities such as brief presentations on security topics, posting of information through posters or trinkets, sending out information in newsletters, warning banners, etc.

Awareness is best accomplished through metacognition, such that users think about what they know and what they do not know, and make the correct and not necessarily the most logical choices. Thus, a poster regarding allowing others entrance into the computer lab would make the user question what the policy is, what their current practice is, what he or she should do regarding allow others entrance, and what other information he or she may be lacking to make the correct decision.

Continued awareness activities employed properly will help assure a metacognitive environment.

7.3 Training

Training is an activity that leads to a skilled behavior or performance. Training, according to NIST 800-16, should be role-based and applied to those people with specific IT security responsibilities.

There are many ways of designing training, such that an Agency can receive passing grades from the Inspector General's office; however, not all are effective. The most effective training occurs in a classroom that allows interaction with an instructor and subject matter experts and includes examples, exercises, and case studies that facility metacognition. This training will be given in context, or at a time such that the student will immediately use the knowledge and behaviors he or she has acquired.

Unfortunately, classroom training is not always cost effective, especially when the target audience is an entire agency of 1,000 or more people. Many agencies are accomplishing training through subject matter expert lectures or computer based training that does not allow for interaction. Basic user training can be effectively accomplished through computer based training if the training is properly designed to allow for user interaction and metacognition. In addition, agencies need to provide time for users to complete the training, online or classroom.

In designing training, classroom or computer based, the course design team

should run a pilot and employ the feedback from a general user who does not have a broad IT background. This will provide information regarding course friendliness, usability, and effectiveness. The easier and more entertaining the training is, while containing all the information an agency wants its users to know, the more transparent the changing of user behaviors will be.

7.4 Reinforcement

Many computer security executives assume the only way to instill good computer security behaviors is to punish those who commit security incidents. Changing behaviors, the goal of a good security awareness and training program, cannot occur through negative reinforcement alone.

Negative reinforcement, albeit not as powerful as positive reinforcement, should be used. Negative reinforcement, often termed "making an example," should be used for serious security breaches such as downloading pornography on a work computer.

Positive reinforcement can be applied through performance reviews. Security behaviors should be an aspect of annual performance reviews, for both the general user and the skilled technician.

Rewards, money or small trinkets, are also examples of positive reinforcement. Brian Kelley, CEO of iDefense, conducted a security check on one finance company by going across the street from the building with the company's security officer. The two used binoculars to spy on the employee computers. One employee noticed what the two were doing and closed the blinds and called the security officer. On Kelley's recommendation, the security officer presented the employee with a $500 reward. The story spread, making employees aware that practicing good security is not just a hindrance. (Conrey-Murray)

8.0 Conclusion

Computer systems are complex to operate and secure. As Gene Spafford, director of the Purdue Center for Education and Research in Information Assurance and Security, stated, ""The only system that is truly secure is one that is switched off and unplugged, locked in a titanium-lined safe, buried in a concrete bunker, and surrounded by nerve gas and very highly-paid armed guards. Even then, I wouldn't stake my life on it." (Sebold)

The goals of computer security are confidentiality, integrity, and availability. These must be accomplished through the mitigation of security risk based on business operations. In order to mitigate the risks, a number of solutions can be applied. Policy is the root of all possible solutions, therefore, it is important to have a well written, easy to read and understand policy. Technical solutions are

not all encompassing and as a computer needs a human operator, effective awareness and training activities for people will always be needed.

If John Doe had been properly trained and practiced the proper security behaviors, the introductory scenario would have looked more like the following scenario.

> John Doe reports to work at eight o'clock in the morning. As he enters his office, a coworker who has forgotten his badge asks to be let into the office. John tells the coworker that he needs to go to the main lobby and obtain a temporary badge and access key. John then proceeds to his desk. He turns on his computer, recognizes the security banner, and then enters his password from memory in order to sign onto the network. Before going to get coffee, John makes sure to turn on his password protected screensaver. On the way to get coffee, John runs into his boss who wants to speak with him for 15 minutes. John returns to his desk, unlocks his computer, and opens his email. He ensures that the attachment to an email from a friend is free of viruses before downloading the file to his machine. In the afternoon, John is working on a report for his boss when a window pops up stating that he must put in a password to continue. John recognizes that the computer should not be asking for his password and calls the help desk. The help desk determines that before changing his behaviors, John had downloaded a Trojan to his computer. The system is cleaned and John goes back to work. At the end of the day, John shuts down his computer and goes home.

References

Blakey, Elaine and Sheila Spence. "Developing Metacognition." ERIC Digest. Syracuse: ERIC Clearinghouse, 1990. URL: http://www.ed.gov/databases/ERIC_Digests/ed327218.html

Conry-Murray, Andrew. "Securing End Users for Attack" Network Magazine. Volume 17, Number 10. October 2002. p28-32

Daniels Jr., Mitchell E. "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Actions and Milestones" OMB M-02-06. 2 July 2002. URL: http://www.whitehouse.gov/omb/memoranda/m02-09.pdf.

Kabay, M. E. "SOCIAL PSYCHOLOGY AND INFOSEC: Psycho-Social Factors in the Implementation of Information Security Policy" The Risks Digest. Volume 15 Issue 16. 19 October 1993. URL:

http://catless.ncl.ac.uk/Risks/15.16.html.

Miller, George A. "The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information." Psychological Review 1956: 63, 81-97. URL:http://psychclassics.yorku.ca/Miller/

Office of Management and Budget. "Circular A-130, Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," 8 February 1996. URL: http://www.whitehouse.gov/omb/circulars/a130/a130.html.

Sebold, Charles. "My Fortune File." URL: http://www.livingtorah.org/~csebold/fortunes

United States Government. "Computer Security Act of 1987" 11 June 1987. URL: http://csrc.nist.gov/secplcy/csa_87.txt.

Willingham, Daniel B. Cognition: The Thinking Animal. Charlottesville: UVA Printing and Copying Services, 2000.

Wilson, Mark et al. "Information Technology Security Training Requirements: A Role- and Performance-Based Model." NIST Special Publication 800-16. Washington: US Government Printing Office, 1998. URL: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

Swanson, Marianne. "Guide for Developing Security Plans for Information Technology Systems." NIST Special Publication 800-18. Washington: US Government Printing Office, 1998. URL: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event