Global Information Assurance Certification Paper

Social Engineering – For the Good Guys
James E. Keeling
July 16, 2001

Coming up with a topic for this paper was much more difficult than originally anticipated. Many thoughts came and went as many topics are covered over and over again. One place where there is a decided lack of coverage is the importance of a security policy and even more importantly, the necessity of buy-in with management, employees, and your security team. A security policy can be defined as: "The total set of security rules enforced by the network including hardware and software security mechanisms and controls."[1] Jim Kerstetter from PC Week Online had this to say about security policy effectiveness. "Security policies, deciding who has access to what, knowing how to use the security tools already in place and common sense are the best ways to stop the Huns at the gate. Ignore the human element, and all the unbreakable encryption, firewalls and sophisticated public-key infrastructures are useless."[2] The best of perimeter defenses, defense in depth, firewalls and intrusion detection are made impotent by a single individual who does not follow the security policy. Jim Williams from netsecurity.about.com also shows how important policy compliance is to the network security industry. "At the second annual Black Hat Briefings conference, one of the main points covered was that security falls short not because of a lack of technology, but rather because of failed policy."[3] The purpose of this paper will be to place due emphasis on this important issue. Consideration will be given to the importance of buy-in by management, employees, and the security team. Ways will also be provided to promote compliance within all three of these levels by the practical application of social engineering. The American Heritage Dictionary defines Social Engineering as: "The practical application of sociological principles to particular social problems." For a more hacker centric definition the Free Online Dictionary of Computing defines Social Engineering as a: "Term used among Crackers and Samurai for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security." Basically convincing people to do what you want them to. This is how hackers use social engineering to attack us. So, how do we use social engineering to protect ourselves? How to make the individuals involved want to follow the security policy. Essentially, "How do I make them as PARANOID as me?" The best place to begin is at the top, which is where our first group resides.

Buy-in to your security policy by management is paramount. The Site Security Handbook RFC had this to say about the involvement of management in security policy: "It is especially important that corporate management fully support the security policy process otherwise there is little chance that they will have the intended impact."[4] Essentially, if management does not support/enforce the policy very few will follow it. If at all possible the individual responsible for enforcing the policy should be management and NOT the security administrator. Unfortunately, many times, employees do no necessarily trust the security person. Also, as security personnel we normally do not have the adequate authority to enforce security policy. Fortunately, our mandate for security is almost always handed down by management, which implies at least some amount of buy-in from the very start. Often, the challenges come when managers are faced with either the cost or the extent of security measures proposed. So how to get management to buy into your security policy when they might be hesitant to do so? Like most people, management

tends to look out for what's in their best interest as well as the best interest of the company. We know that following the security policy is very beneficial to management. It is beneficial both from a fiscal standpoint as well as from a standpoint of responsibility. Security breeches can cost the company a fortune, and in some cases bring it to its knees. This alone is often enough to ensure buy-in from management. Management tends to look at the numbers. Here are some staggering numbers as posted in article in Darwinmag.com:

> "$6.7 billion—the cost to businesses for the first five days of last spring's "I Love You" virus as estimated by Computer Economics, a research company
>
> $125,000 per hour—the cost to companies for Web outages as estimated by Cahners In-Stat Group
>
> $142,000—the average cost of a network security breach in 1999 as estimated by the FBI (which found that 55 percent of U.S. companies experienced at least one breach that year)
>
> The FBI survey found that, on average, 41 percent of security-related losses are the direct result of employees stealing information from their companies. The average cost per internal incident? A cool $1.8 million."[5]

Place numbers in front of them. They will make the connection to losing possibly millions of dollars to the tenuous hold they have on their jobs. If following this tact seems to be returning fruitless, try to explain to them "As managers you are extremely important people and because you are so important, you have access to some of the most critical data the company has. Protection of that data is extremely important." This plays on vanity and pride. Some may call that a dirty trick, but that's social engineering for you. Try to instill in them the paranoia that you have come to respect. If you can do this and they internalize it, your battle will be mostly won. The most critical aspect of this course of action is tact. Adults are simply grown up children. Sometimes, children don't like being told what to do. This is where social skills are a must. Explain it in such a way as to make it appear as something they wanted to do in the first place. The following is an effective example of social engineering.

> A security expert who developed an excellent policy first successfully received buy-in from all of the VPs in a company. He then went to the President of the company and explained how pleased he was that the VPs supported the policy and were willing to enforce it. In fact he was so pleased that he thought that they should receive a bonus for their support of the policy. In effect saying that part of the VPs bonuses would be contingent upon their living up to their commitment to following, supporting, and enforcing the security policy for their subordinates. This is an excellent example of social engineering – for the good guys.

The importance of receiving buy-in from management cannot be stressed enough. If done right this will give your policy the backing necessary to ensure the last two groups fall into line. Some employees follow by leadership example, and some by "what's the consequence if I don't" mentality. Without sufficient backing from management you're fighting a losing battle. Security professional Ernest D. Hernandez had this to say about management involvement. "The most important element in a successful security policy is management support. When upper management buys into and makes a firm statement that network security is important, users

throughout the organization will take the security policy seriously."[6] Which brings us to the next group in our trio.

Invariably there are more employees than managers. This may not appear to be true in some workplaces as it feels as though we all have at least 2 or 3 bosses to each worker, but mostly, that's just the general impression. So how to get all those employees to want to follow our security policy? There are many approaches to this group and most all of them are valid. Once again your ability to effectively convince your audience of the importance of compliance is paramount. Attempt to breed paranoia into them. Have them watch a snippet from the movie Hackers, in which a bunch of teens simply "dumpster dove" and walked around an office gleaning numerous passwords, as well as calling up a hapless security guard and receiving a modem enabled analog phone number. Another excellent scene is from the movie Wargames, where a war-dialer was used to find analog lines with attached modems. This is social engineering – for the bad guys. Now it is time to counter-act this with some social engineering of our own. Hopefully, as you put forth your security plan to the employees, you can garner some of the wisdom known as paranoia. It is a known fact that people who are paranoid pay more attention to things, and this is something we can use to our advantage. Most employees are completely unaware of the social engineering methods that hackers and crackers use. The examples stated above drive home points such as "Please don't write down your password on a sticky note and put it on your monitor," and "Don't give you're your login name or any information to anyone across the telephone." Bring home to them the reality and existence of hackers. More and more these days, it appears the situation is an "us vs. them" type of scenario. As adversarial as it may seem, this is essentially the truth. The problem many of us encounter as security professionals is that to employees, "them" is "us", the security team. Our own team often views us as adversaries. Just as we instinctively check our rear view mirror when we pass a state highway patrolman on the interstate, employees at times look upon us in the same way. So how can we effectively combat this trend? I personally believe that involvement is the key to buy-in. When you develop your security policy, involve individuals from the employees group as well as the managers group. The individuals you involve should be respected workers. Individuals, who are established, know the inner workings of their job, and know their coworkers. When they return to work, they will be the vanguard of the "followers of the policy" in the employee ranks. They will lead by example and help to ensure compliance. Bring the rest of their coworkers over to a more secure way of thinking. As security professionals we have an idea of the potential risks involved in not following a defined security policy, but as "civilians" most employees do not. In many cases, simple education can accomplish our goals here. The Computer Security Resource Center of the National Institute of Standards and Technology purports that "Internet security policy must be closely integrated and adopted into the organization's culture and environment through education (5.6). Users cannot follow policies they do not know about or understand. Training also supports individual accountability, which is one of the most important ways to improve computer security (5.7)."[7] What is in the best interest of the company is generally in the best interest of the employee. Better revenue for the company generally equals better raises/bonuses for its employees. Directly linking security breaches to dollars will go a long way toward receiving buy-in from the employee ranks as well as the managers. Some individuals do not respond well to this method though. And unfortunately as it may be, another option is open to us. A very wise man once said to me "When you ask yourself

if this is something you should do, ask the question 'Can this person fire me?'" After obtaining buy-in from management you might have exactly that sort of muscle to assist you in ensuring conformance. But be careful in this area, no tolerance policies can be very dangerous and should be approached with extreme caution. The Computer Security Resource Center had this to say about such policies. "While it is tempting to simply state that any such use must be for business purposes only, it is generally recognized that this type of policy is completely unenforceable. If a policy cannot be consistently enforced, non-compliance is inevitable and the policy will have no force as a basis for punitive action."[7] Always try to remember that we are supposed to be on the same team. Treat employees as such and you might be surprised by the reaction you receive. We have talked about managers and employees, the two groups that are thought of most commonly. But as we all know you should always avoid single points of failure, and that brings us to our last and final group, ourselves.

Your own security team can be your greatest asset and your greatest liability. To place it into perspective, imagine giving the keys to every office, every file cabinet, and every safe in your entire company to one person. In this case, it's sometimes given to a team of people. Trust is not only preferable it is a necessity. Well, trust begins at home, within our own family. If you successfully cultivate a sense of teamwork and belonging, a group dynamic will evolve that will serve you and your security policy well. Hackers use each other and the whole of the Internet as a resource. We need to work together and use all available avenues to equip ourselves effectively. Our field is so very broad this makes cooperation within our team that much more important. Your security team must function as just that, a team. Lack of communication is bad for any team, but especially so for a security team. A well-crafted security policy with extensive defense in depth can be a complicated thing. The key to effective implementation and upkeep is to utilize effective organization. I include both the security administrators with the network administrators because our duties so often overlap. Here is another effective example of social engineering.

> In this scenario, the security administrator teamed up with the president of the company and basically ensured his network administrators would support the security policy. The President called down to the network helpdesk on an unsecured phone line. "Yes I need you to change my network password and give it to me over the phone" he said. Luckily, the network administrator knew the security policy and regretfully informed the president of the company that while he was sorry, he couldn't give out a password over the phone. Upon hearing this, the president apologized and hung up. The president then went down to the help desk and asked for the administrator by name. When the young man stood up the president walked over to him and gave him $1,000 in cash. This was something that everyone in the room saw. The president addressed the network administrators commending this individual for following the security policy and then left. I believe it would be a safe bet to say that no administrator ever gave out a password over the phone after that. This is social engineering – for the good guys.

As to the amount of money the president provided, it is miniscule compared to the potential loss to the company if a hacker had done the same thing and received the president's password over the phone. One point to pay special attention to is the background and abilities of your security team. "The success of any security policy depends more on the motivation and skill of the people administering the policy than it does on any sophisticated technical controls."[7] Often

times, your network administrators take on the duties of security administrators as well. This quote from Network Computing explains this issue "The bottom line is that the network administrator is not a security specialist. If a company wants to deploy its network administrator this way, it also needs to train him or her in security software, processes and procedures."[8] If you want your people to be security professionals give them the training necessary to be effective in their duties. This will also demonstrate your willingness to invest in your personnel and foster that group dynamic and work ethic we alluded to earlier. This is the most positive form of social engineering. It is the honest open effort that you put forth that will yield the greatest benefits from your security team.

I have endeavored to show how to effectively utilize social engineering to "encourage" those in your organization to follow the security policy. Compliance to the security policy by all three groups is essential to the success of any security policy. Management, employees and the security administrator(s) must act as a team for your security policy to be effective. It is much the same as the huge tower of cans at the local supermarket. If you were to grab a can from middle, the whole tower would collapse. Another more apt analogy would be the proverbial "house of cards." It doesn't matter from what level or from which angle you pull that card, all others are depending upon it. At the management level the greatest motivating factor is most likely the possible loss of either money or information. Trained managers understand the concept of risk assessment and management. Compliance and support from management is your top priority. Employee compliance is also essential to an effective security policy. The greatest general in the world is of no use without his troops. Properly training and motivated employees can be one of the most effective components in the defense of your network. Obtain buy-in from management to show the employees the importance of the policy. Use employee representatives as you fashion and implement the policy to provide trained and motivated leadership within their ranks. Avoid the over-use of no-tolerance policies in non-essential areas as it makes your policy more difficult to enforce. Remember that the employees are not your enemies and treating them as such can only hurt your efforts to implement an effective policy. Your network/security administration team is more than just a bunch of people you slap the label of "Security" on. They are the ones you rely upon to coordinate the protection of your information systems. They must be properly trained and prepared for the tasks they have set before them. They must be effective communicators as the complexity of their positions can be great. They must be trustworthy as you are entrusting the safety and security of your organization to them. Obtain buy-in from all three of these levels and you will find your policy to be effective. Many individuals in our business work almost exclusively with hardware and software. At times this leaves little room for social skills development. This is where we must diverge from the traditional geek persona. Another title for what we do might be "Social Engineer." As an effective social engineer there are many methods we can use as outlined above. Most of which rely heavily upon our social skills. Having an effective security policy is a necessity. Jim Kerstetter from PC Week Online relayed this story about security expert Ira Winkler:

> "Case in point: Winkler's recent bank "attack," in which he was hired to test the bank's security. The bank had three firewalls and was not easy to break into electronically. So Winkler picked up a telephone book. He also did some research on the Web, discovering the bank's domain and other Internet address information left on Usenet groups." After

some simple social engineering the article stated that "With that information in hand, the only equipment Winkler needed was a PC with a modem. 'Someone said I would have had the capability to make $2 million transactions,' he said."[2]

No business in the modern world can function without protecting their information. You cannot protect your information without the implementation of a good security policy. Good policy empowers people to do the right thing. Keep in mind that we are all on the same team. In the same "social circle" as it were. As security administrators we must use our social skills to effectively carry out our duties. Social engineering – for the good guys.

Bibliography:

Source #1
University of Toronto Computing and Networking Services
URL: http://www.utoronto.ca/security/lancsp.htm

Source #2
Kerstetter, Jim. "Security alert: Technology alone won't stop a break-in." PC Week Online. 31 July 1998
URL: http://www.zdnet.com/eweek/news/0727/31ebhat.html

Source #3
Williams, Jim. "How Secure Are You?" Netsecurity.about.com. 8 October 1998
URL: http://netsecurity.about.com/library/weekly/aa081098.htm?COB=home

Source #4
Site Security Handbook RFC
URL: http://info.internet.isi.edu/in-notes/rfc/files/rfc2196.txt

Source #5
Duffy, Daintry "Prepare for the Worst" Darwinmag.com. December 2000
URL: http://www.darwinmag.com/read/120100/worst_content.html?printer=no

Source #6
Hernandez, Ernest D. "Network Security Policy – A Manager's Perspective" SANS Information Security Reading Room. 22 November 2000.
URL: http://www.sans.org/infosecFAQ/policy/netsec_policy.htm

Source #7
National Institute of Standards and Technology Computer Security Resource Center
URL: http://csrc.nist.gov/isptg/html/ISPTG-5.html

Source #8
Schafer, Maria. "Not So Secure?" Network Computing. 11June 2001
URL: http://www.networkcomputing.com/1212/1212ca.html

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event