Global Information Assurance Certification Paper

The "Human Element" – A Constant Challenge
Lyle Singular B. Ed
Assignment Version 1.4b
Submitted: July 30, 2003

ABSTRACT

Network security, as detailed in various research papers, covers a great many topics. Many topics are very granular and are researched extensively. The "Human Element" is a beast unto itself. Whether we deal with social engineering, appropriate passwords, workstation security, etc more and more elements ultimately fall to lowest common denominator, ie the end user. The issue of convenience versus security becomes the focal point for virtually all companies, large or small. How do companies address the "human element"? Is there training? Is the training targeting the right audience? Has the deficiencies in the audience been correctly identified?

The focus of this paper is to delve into the many facets of security from the "human element" and to address the need for entry level training, continuous education, and continual awareness. In other words, "little things can make a big difference"[1]

BACKGROUND

Past issues of security dwelt on the worker, their workstation environment and how to best protect their entry point into the network. This usually involved the selections of a password with a caveat to pick something reasonably difficult, log off your workstation when away from your desk, and don't leave "password reminders" lying around. Unfortunately, many companies still leave this orientation as is and have not progressed any farther. For others, their awareness levels are higher, and have perhaps more advanced training, but the ongoing nature of reinforcement is left out of the picture. The usual arguments abound, not enough money for training resources, not enough time, not worth the investment. It should be apparent to IT security managers that this issue is one of the more difficult ones to tackle as it takes time and preparation to sell training to management and keep it in focus. It is unique in its challenge, as all too often, management wants a "one-time" solution. The intangibles of human behavior simply don't sit still in one location making it easier to control the problem. Dealing with training and the vagaries of human control is a skill that is almost directly opposite to the skill required when dealing with a technical issue. Solving technical problems tends to attract the energy of an IT security professional as there are countless technical solutions to the myriad of problems they face when protecting their networks. Unfortunately, many IT managers view the problems at the end user level as so rudimentary, that it is difficult to relate to these issues and how they have to be addressed. The countless stories and tales

[1] Gladwell, Malcolm, The Tipping Point How Little Things Can Make a Big Difference (Boston, New York, London: Little, Brown and Company, 2002) Title.

that circulate the Internet from the "help desk" arena reinforce this view, and once ingrained it becomes difficult to relate to an employee who is an end user.
The following topics are the common areas that are subject to human error. Each has been summarized here to provide the backdrop on the issue of training, and will not be the focus of an in-depth discussion for the purposes of this paper.

SOCIAL ENGINEERING

If there is one topic that has captured the attention and resources of management security, it surely has been this one. The topic is well researched, and many scenario based training sessions have been created to bring this point home "Targets of Opportunity – Information Security: The Human Factor is an excellent resource from Commonwealth Films Inc. www.commonwealthfilms.com

A perusal of Sarah Granger's Social Engineering Fundamentals, Part II: Combat Strategies is another resource document on social engineering, but more importantly she addresses the need for training. (http://online.securityfocus.com/infocus/1533) The emphasis is on training, the more the better and includes retraining as a means of reinforcement.[2] Complacency becomes a significant enemy over time.

Social Engineering will be the largest component of your training requirement as it simply is the most difficult to effectively condition your employees to. Social engineering skills are only limited by one's imagination. If you take a brief look at the criminal and civil occurrences of fraud, and the methods employed, you will see many similarities. There will always be an "angle" that will be new as invaders will constantly work to improve their techniques. Recent reports in a variety of newspapers have described the new act of "war mumbling". We are all familiar with the war dialing and war driving, but now employees are faced with callers who speak with heavy accent in the language of the company (usually English). The frustration point that is reached by the Help Desk, or employee tends to yield what the caller is after.

As stated previously, this is a topic that is well researched. With the effect that Kevin Mitnick so ably demonstrated, it is a small wonder that IT Security pays a significant amount of attention to social engineering. The reminder here is that the Help Desk is not the only target of opportunity and that orienting and training employees across the entire company is the overall goal.

PASSWORD SECURITY

[2] Granger, Sarah Social Engineering Fundamentsl, Part II: Combat Strategies. http://online.securityfocus.com/infocus/1533

This topic never fails to generate discussion and disgust with IT Security Managers. If rigid policies are enforced, the administrative overhead goes up exponentially. Management will surely be inundated with complaints and then we are back to the convenience versus security argument. There is no ideal solution, but the issue certainly falls to training and reinforcement to shift the poor habits and practices to a higher level of security. This topic is so rudimentary to many in IT Security that the only solution that has been applied is to "talk about it". What other solutions have been advanced to guide your employees to a better level? Regardless of the "apparent stupidity" of the issue, examples of solutions are far better at reinforcing than a simple discussion. The issue of how these passwords are remembered and stored will be examined in the following topic on workstation security.

WORKSTATION SECURITY

One could suggest that certain components of this topic are a sub set of social engineering, however, its differing elements help set it apart. Employees are constantly reminded to ensure that their workstations are logged off when they are away from their desk. The simple use of a screen saver password simply isn't effective enough. It would be considered useful to encourage a shutdown when the work day is over, but this becomes a segment of the convenience versus security argument. Passwords are often left laying around that makes it easy to access the network. Some employees obviously feel that they are creative when it comes to "hiding" their passwords, but that notion can easily be defeated with proper training and orientation.

A second component that has crept into workstation security is the shift away from desktop models to laptops. Many corporations are investing in laptops for a variety of reasons. One, the cost difference is shrinking everyday, and making this solution more viable. Two, more and more employees are becoming mobile and therefore their needs (and demands) become a reason for this choice. Now we enter a whole new arena. Not only do we have to combat the usual vulnerability of access to the network, we also face a loss due to theft, and ultimately a network compromise particularly if it comes from a wireless environment. The issue of mobility will be discussed later, but at this juncture the emphasis will be on workstation security.

The obvious problem now is to ingrain into employees the aspect of theft and how to protect their machines. Even before that becomes an issue, is the company providing a locking mechanism to facilitate this need. If management and the employee have an issue envisioning that theft will occur in their office, go back to the lesson on social engineering and unauthorized visitors. If this topic still needs reinforcement contact the local police agency to see what they are dealing with when it comes to stolen laptops, specifically from office environments.

WIRELESS

Since we have already mentioned the issues of workstation security and incorporated laptops into that discussion, the natural lead from there is the wireless world. The engine that drives this decision is usually business and the need to be "always on, always available". This is considered a key to survival. If your company is still pondering wireless technology, a starting document could be The Seven Steps to Success in the Mobile Wireless Enterprise by F-Secure Corp. www.europe.f-secure.com/products/white-papers/7steps.pdf It simply states: " Prepare for the inevitable."[3] The corporate response has been massive with increases in cellular phone use at 5600 % between 1995 and 2000. It is estimated that there in excess of one billion cellular phone users today. More and more are we seeing the integration of "handheld devices" that integrate cellular capabilities with text messaging. The Blackberry from Research in Motion (www.rim.com/news/press/pr-25_06_2003-01.shtml) is an example of one company that has seen its growth increase dramatically because of the corporate world's desire to go wireless and always connected. It is estimated that there are over 700,000 Blackberry users alone in the corporate world. As a contrasting point to the corporate world's response to wireless devices, the law enforcement community, in particular the Royal Canadian Mounted Police, Canada's National Police Force, has very restrictive policies regarding the deployment and use of wireless and mobile devices. For many of these law enforcement agencies the deployment of laptops with suitable encryption and VPN capabilities was a significant step. All other devices, other than a wireless mouse is not considered secure enough to deploy. This obviously points to the security side of the "convenience versus security" equation. Threat and risk analysis is a daily facet of their existence.

It will be your company's downfall if you ignore security. For those companies that have deployed essential security, the mobility of their employees and the physical risk to the equipment has increased exponentially. Now we are back to the "human element". How do we control these issues, or at least mitigate them.

ENTITLEMENT and INTERNET SECURITY

This phrase has been borrowed to best capture a phenomenon that management and IT professionals seem to deal with every day. Internet access has driven corporations to make all sorts of decisions, be it for e-commerce or business processes in their day to day operations. Often the demand from employees is such that management gives in and provides access levels that open all sorts of access points of vulnerability. Again we are faced with convenience versus security. All too often convenience or perceived convenience is mistaken for productivity, and all too often access is granted without

[3] F-Secure Corp The Seven Steps to Success in the Mobile Wireless Enterprise www.europe.f-secure.com/products/white-papers/7steps.pdf

control. Some corporations are prepared to accept the risks, but they are usually the ones that can afford the best software/hardware solutions for IDS and the best IT Security people. The opposite end of the spectrum can afford only a fraction if that.

When we look at "entitlement" we look at a characteristic that is difficult to deal with when it enters the workplace. There is a never ending shift in the line between what corporations offer, employees accept and then renegotiate. The traditional issues between labor and management are usually well defined, but the boundaries of internet access, the range of use and the laws of privacy are still evolving. The defining attitude of entitlement could almost be summed up in the following statement. "I work for you. You need to provide this to me to better do your work". With the Internet, it seems that the more that is offered, the more that is expected or wanted. The balancing act for managers will inevitably create either labor unrest, or an overloaded IT Security department, faced with an impossible task of properly securing the corporate network. The misuse of email, chat rooms, gaming rooms and newsgroups are all areas that have high risk and ultimately are subject to much human error. Even with the most secure environments, many users are completely unaware of the footprints they leave at web sites that they so blissfully "surf" while at work. All too soon they become the recipients of spam mail, including pornography, get rich quick schemes and an assorted other types of material that is embarrassing to the company they work for, let alone a potential threat to the security of the corporate network. The abuse of these services is soon evident and the headaches of dealing with them as well as the insecurities they bring are wide ranging. Commonwealth films, again has an excellent resource available to bring the point home. Get.Net.Smart Using the Internet and E-mail at Work details a number of scenarios in the work place environment.

IT EMPLOYEE SECURITY

To some, this would sound like an oxymoron. A survey released in April of 2003 from Comp TIA (www.comptia.com/research/whitepapers/summaries/securitystudywhitepaper3-03.pdf) argues that IT workers lack adequate security training[4]. This survey (taken across government, education, financial and IT sectors) claims that human error, rather than technology is at the root of most information technology security breaches. Aside from corporations that did not have security policy in place, some of the participants indicated that their own IT staff did not have security related training. Many had IT staff that did not have security certification.

An informal questioning of IT security managers by this writer, did in fact confirm that some IT staff had no security training. This could be exemplified by simple situations such as deploying portable devices (ie laptops) where they could be easily stolen, or were

[4] CompTIA Committing to Security: A CompTIA Analysis of IT Security and the Workforce. www.comptia.com/research/whitepapers/summaries/securitystudywhitepaper3-03.pdf

accompanied by the User ID and Password and left in plain view. Password deployment was cited a number of times which didn't necessarily mean that they were issued with the laptop. These were situations where an envelope clearly and plainly marked "User ID and Password" was left on the user's desk, without the user being present.

If we look further at this situation, especially one exacerbated by a lack of policy, what becomes of the corporation where wireless access points are set up with no security in place, and are primarily to facilitate a personal need of an IT department member.

The 2003 CSI/FBI Computer Crime and Security Survey addresses their question concerning physical security and the type of response they received. The question was characterized as being "overly broad"[5] and thus open to interpretation. That may be, but in light of the CompTIA survey, the answer should be obvious. Without security training how does one effectively define certain elements of security? The CSI/FBI document is available at. www.gocsi.com

TRAINING THE "HUMAN ELEMENT"

To this point we have discussed a sampling of the areas that are subject to the "human element" and some of the security issues that arise in each of these areas. There is no one easy solution to change this. Training is necessary, reinforcement is necessary and it must be combined with thorough policy.

A good starting point for discussion is the article on Symantec's website titled Behind the Firewall – the Insider Threat. www.symantec.com/symadvantage/017/insider.html The human element is the weakest link.[6] There are four main reasons identified why insiders cause security breaches.

1) Ignorance not knowing polices, lack of safe computing practices
2) Carelessness do not match their actions to policy after they have read them
3) Disregard acting against policy even when they know they are
4) Maliciousness a disgruntled insider, a deliberate act

If we examine the first three reasons, we should be able to find that these are "habits" or characteristics of the employees. Training and orientation can address these, but each one has different elements to deal with from an instructional point of view.

Ignorance is easily altered with effective, timely information that helps guide the employee. New employees are especially vulnerable to this as they will be very weak if the company does not have any training policy/orientation in place. The key to effective training is finding the method that works best. Adults learn a variety of different ways,

[5] 2003 CSI/FBI Computer Crime and Security Survey
www.gocsi.com
[6] Behind the Firewall – the Insider Threat
www.symantec.com/symadvantage/017/insider.html

and all too often training relies on the standard lecture and presentation approach. This approach happens to be the least effective approach and approximates about 10% retention.

Carelessness is making a rather fine distinction between ignorance and disregard. This characteristic would suggest that the training received in the first instance wasn't sufficient enough to aid the employee. This shortfall can often be the result of assumptions made by training staff that the content being taught is so rudimentary that the employee was expected to make certain connections in the concepts. This obviously failed. We also make the mistake in assumption that once something has been read, that it has been understood. If this "reading" stands as a form of training it is a recipe for disaster.

Disregard really points to habits of a person. If they are disregarding policy with full knowledge, there will be other areas of concern that the company should have with this employee. This becomes a tough individual to educate. This is more about behavior modification and raising their levels of trustworthiness and acceptance of responsibility. From a training perspective, this will require a lot of time and energy. Does the company wish to accommodate this? Perhaps they need to find a new employee. Perhaps a closer look at the training/orientation, this employee received (or didn't receive) is required.

Maliciousness is beyond education. This person has already received a one-way ticket and this is where it is vital that policy be solid and strictly adhered when dealing with and dismissing these people. If the maliciousness has, in part, arisen because of some shortage in security training on the IT group, then there arises a need to address the training concerns with IT personnel. It could also be said that with these types of insiders there needs to be a committed criminal investigation. It really is necessary to prevent these individuals from surfacing elsewhere and starting the problem all over again.

Additional reading on the subject of "The Weakest Link" can also be found in an article written by Tom Standage for the Economist.[7] (www.cfo.com/Article?article=8027) In this article, the focus is on management based solutions rather than solely technology-based. The argument is that this can be cost effective. The issue remains. How are the concepts delivered and who delivers them. An analogy that is often used to deliver this message is the "neighborhood watch" program. This makes security everyone's business. The trick is to get the buy-in from the participants and this is the biggest stumbling block for any company. Granger points out in her article that orientation and training needs to convey a sense of ownership to the employee when it comes to understanding the confidentiality and the value of the information that they are to protect. This of course assumes that the company is prepared to invest in orientation and training. It is absolutely critical that new employees receive training and orientation. Learning by "osmosis" is a sure fire way to

[7] Standage, Tom. The Weakest Link The Economist Nov 1, 2002 www.cfo.com/Article?article=8027

get off on the wrong foot and result in a larger problem to correct.

A FOCAL POINT

As we move onto the next phase, we need to look at some source information that can serve as a guide. It is one thing to have all the technical skills necessary to manage a network, but it is an entirely different skill set required for training people. The following pages use two reference sources as a means to examine human habits and how to understand them a little better. The first is Malcolm Gladwell's, The Tipping Point – How Little Things Can Make a Big Difference. The second is Stephen R Covey's The 7 Habits of Highly Effective People. The goal is to focus on these points to provide a basic starting point when pondering training. There is one additional caveat. The issue of adult education and how adults learn has a remarkable amount of diverse literature. That is not the subject of this paper, nor is it the intent to establish a training model. Templates have a habit of falling short of the desired result. Each company will have unique problems in their weakest link and should seek individual solutions to them.

Now that as a company, we arrive at the decision to engage in training/orientation, particularly at the new employee stage, how do we make this information stick? Ultimately an individual in the IT department is going to be tasked with creating some training material and delivery model. Most individuals are not very comfortable with the idea of teaching. A good starting point for the employees who are tasked with this is the book, The Tipping Point by Malcolm Gladwell[8]. It can be extremely daunting to face the challenge of creating effective material, much less delivering it. Although Gladwell's book uses epidemics as a means of conveying his point, his information transcends multiple situations. He describes three essential ingredients that determine "The Tipping Point." One, the Law of the Few. This in effect is the messenger. The nature of the messenger matters. Effective messengers spread the word. Two, the Stickiness Factor. What makes the message stick? Three the Power of Context. This is our immediate environment. It is within these three points that "The Tipping Point" becomes evident. What point can be discovered that "tips" the employee to an effective understanding of security and the appropriate skills they need to practice every day.

Direct marketing companies have discovered to their loss that it is easy to reach customers, be it by phone (telemarketing), fax, junk mail, email, etc. How do you get the customer to stop and read the advertisement and then have them act on it or "tip". Probably the biggest barrier that faces companies in terms of delivering the policy and training expectations is the "clutter problem". We inundate employees with information that we expect them to read, absorb and then practice effectively and constantly. We often treat this approach as our training method. We no longer have enough "stickiness" attached to our information. How many times does the employee use the "delete" key to effectively handle this clutter?

[8] Gladwell

The final point that Gladwell incorporates into his writing is the "Power of Context." This refers to our immediate environment. Numerous researchers in sociology and psychology have studied and tested this theorem for decades. One of the foremost proponents of this theory is Stephen Covey, which he explores in his book The 7 Habits of Highly Effective People. [9] Covey promotes the idea that you change people's behavior by changing people's picture of their roles; a paradigm shift. Covey's book gives an excellent starting point when trying to come to terms with people, their habits and the roles they play. To make learning stick, Covey first promotes that you as the individual (teacher) learn deeply, then teach it almost immediately afterwards. If you are thrust into a position of teaching, you will hold the concepts of security to a much greater depth than if you are merely the student. The final step is to live it yourself. If you can practice security as you have learned it and taught it, you will be better and the personnel around you will be the beneficiaries of your practices.

To use an example of one issue of security, we will examine password security. Virtually every IT manager wants to see company employees use a password of at least 7 characters and a mixture of numbers, letters and symbols. Why is it then, that employees habitually use (where companies allow it) passwords of lesser length, no mix or their User ID as their password, or even the word "password"? Why would an employee find this difficult? When you question them individually, you would probably find that they can tell you the 7 or 10 digit phone number of at least 20 family and friends without consulting a directory or data organizer? Research psychology refers to this as channel capacity, which is essentially the amount of space your brain can hold certain types of information. The natural limit tends to be around 6 or 7 characters or categories. Gladwell (pg 176) [10]points out that Bell Telephone understood this concept when they wanted to engage in numbers that we as long as possible, and still have people remember them. Why should corporations accept less?

As elementary as it may appear, companies rely on their employees to make the "right" choice when it comes to selecting a password. Have these employees ever been challenged to shift their focus and look at this issue? With this natural capacity to successfully engage in 7 digit passwords, why not utilize a few memory exercises that will assist this capacity. Learn to mix it up a little. Take some time to develop and practice some patterns that are easy to follow that will allow the employee to alter their password slightly, but maintain as much integrity as possible.

To refer back to the beginning of this page, it was pointed out that overwhelming employees with material will reduce the effectiveness of your message. As long as we continue down this path, we will be forever tasked with managing the issue of insecure passwords. Gladwell hypothesis that when people are overwhelmed with information

---

[9] Covey, Stephen R. The 7 Habits of Highly Effective People. (New York: Simon & Schuster: 1989) Sound Ideas™ Adapted for Audio

[10] Gladwell, pg 176

they develop immunity to traditional forms of communication.[11] People actually turn to people in their lives for advice, and information. These people are the ones whom they respect, admire and trust.

Many companies are relying on pop up screens to remind people of policy, some may actually engage in quizzes and others will supplement electronic information with good old fashioned pamphlets and flyers. It should be apparent by now that if we are depending on the employee to read, how much is actually read, and how much is absorbed. Why not focus on the simple things and see what type of big changes can be brought into your company. Focusing on the small things is cost effective as it does not rely on "big dollar campaigns."

A second example that can be looked is the aspect of internet security, whether it is email, chat rooms, or newsgroups. Although employees can be made completely aware of the various outcomes of their activities, fear is not a motivating factor. Social psychologist Howard Levanthal conducted fear experiments in the 1960's. [12] (Gladwell, The Tipping Point pg 96). He established that although test subjects were well educated on certain topics, the ominous warning of a negative outcome did not motivate the subjects to change their behavior. One only has to ponder the 90's version of the HIV/AIDS epidemic to gain a sense of how behavior can become immune to an obvious outcome.

To take this one step further. Companies that rely on the fear strategy to "educate" their employees will find that they spend a lot of time responding to and attempting to control the actions of their employees. Confrontation will become a norm. Serious enough breaches result in firing, but then we are right back to where we began in the first instance. Now we have a new employee to educate.

Internet safety and security training needs to accomplish at least two things. One, information about safe practices is provided. Two, the employee needs to experience a paradigm shift or the change in context. Can education meet the challenge of shifting the employees' view of their role? One approach would be to have their internet activities examined during the orientation and relate it to their home activities. Point out that if they can follow certain safe practices they learn at work, their risk factor also decreases at home. An analogy that could be given here is where employees are requested to take CPR training as part of the work environment. Many are resistive. However, if they can be made to realize the benefit of CPR training as it relates to their personal lives, ie saving their children from choking, or an elderly parent from a heart attack, they are likely to be a much more responsive and attentive student.

If we can change or instill a habit in our employees we achieve the effectiveness that we desire. If the employee can leave their training session with three things; "I know what to

[11] Gladwell pg 271
[12] Gladwell, pg 96

do, and I know how to do it, and I want to do it" [13] we have given them the skills, knowledge and attitude to deal with Information security. The purest goal you could achieve with this topic is that your employees become disciples of Information security and your own version of "Neighborhood Watch" starts working for you.

POINTS TO PONDER: THE IT PERSPECTIVE

Now that we have reached the point where we have all of these security issues to deal with that involve the human element, how do we as IT managers make sense of this and what direction do we travel? IT Managers have to avoid the pitfall of managing to the point where they are simply putting out fires. If we fall into the trap of reacting to every security breach that involves the "human element" we will never accomplish the level of security that we desire. If we view ourselves as proactive, then it is time to look at leadership. Do we have our beginning with the end in mind. [14] Covey describes this as the "Leadership Habit". Firstly we need to make a careful examination of our costs that relate to security breaches, involving the human element. Second, a full evaluation of the type of breach that occurred and the training that exists in the corporate structure. Third, indulge in some creative thinking and look at training possibilities outside the norm. There is a lot of information that tells us how much we are affected by the weakest link, but not a lot that looks at the traditional training models and whether or not they work. (Unless you're a software vendor)

The first issue is easy. Most companies are quite adept at doing cost analysis when it comes to loss. The next step flows from here. Is the training (if it exists) addressing the breach? Is the messenger effective? Is the message sticky enough? Does there need to be a shift in context? Has complacency set in? If we do not have an answer to any one of these five questions, why not explore something different. All of this assumes that you have some buy-in from your company for training. If you are having a problem in that regard, it could be advantageous to point out that management's current solutions are costing them money.

[13] Covey
[14] Covey

Works Cited

Behind the Firewall – the Insider Threat Winter 2003 Issue 17
URL: http://www.symantec.com/symadvantage/017/insider.html

Commonwealth Films Targets of Opportunity – Information Security: The Human Factor
URL: http://www.commonwealthfilms.com

CompTIA Committing to Security: A CompTIA Analysis of IT Security and the Workforce. April 2003
URL:
http//www.comptia.com/research/whitepapers/summaries/securitystudywhitepaper3-03.pdf

Covey, Stephen R. The 7 Habits of Highly Effective People. (New York: Simon & Schuster: 1989) Sound Ideas™ Adapted for Audio

F-Secure Corp The Seven Steps to Success in the Mobile Wireless Enterprise March 2000
URL: http://www.europe.f-secure.com/products/white-papers/7steps.pdf

Gladwell, Malcolm, The Tipping Point How Little Things Can Make a Big Difference Boston, New York, London: Little, Brown and Company, 2002 Title.

Granger, Sarah. Social Engineering Fundamental, Part II: Combat Strategies

January 9, 2002
URL: http://online.securityfocus.com/infocus/1533

Research in Motion June 25, 2003
URL: http:// www.rim.com/news/press/pr-25_06_2003-01.shtml

Standage, Tom. The Weakest Link The Economist Nov 1, 2002
URL: http://www.cfo.com/Article?article=8027

2003 CSI/FBI Computer Crime and Security Survey
URL: http://www.gocsi.com