Global Information Assurance Certification Paper

Re-forging the Weak Link

User Training Why's and How's

Name: Frank Giachino
Date Submitted: 30 March 2004
Certification: GSEC
Version: 1.4b
Option: 1

Abstract

In spite of the efforts of myriad security professionals, software solutions, and perimeter defense strategies the weak link in any security scheme is always going to be the people it is designed to protect. In order to insulate the enterprise as fully as possible from outside threats it is essential to enlist the people we are working to protect, the users. This paper will describe some vectors from which users need to be protected and some ways in which the dedicated security practitioner can move the user community away from being a liability and towards being a contributing factor in the overall security strategy.

The Basics

It should be a truism at this point in the evolution of Computer and Network Security that a 'Defense in Depth' model is essential in creating and maintaining a secure IT environment. This model is equally applicable to the small business and the world-wide enterprise. In fact it is now the exception rather than the rule to find an entity which has no defenses at all at the perimeter, or no password standards. The multiple vectors of attack available to the determined hacker mandate multiple layers of defense in order to meet the critical minimums for a secure environment.

The weak link in any security plan is, and will always be, the end user. "*Even if you have very comprehensive IT security technology in place, all it takes is one careless, uninformed, or disgruntled person with access to your physical office space or enterprise network to open your company up to unnecessary risk*."[1] This is not to say that the end user does not care about securing his data. Quite the contrary, it is the end user who stands to lose in the event of a security incident. Rather the lack of knowledge and day to day involvement in security matters often leaves the user incapable of responding decisively to the latest worm, phishing attack, or network incursion. User awareness of security issues is one of the strongest weapons we have at our disposal in attempting to secure the enterprise.[2] Likewise it is unreasonable for the security professional to decry the 'ID 10 T' errors that allow the latest virus to get a toehold on the system. Staying abreast of current malware and systems breaches, procuring and deploying appropriate patches and securing the enterprise is a full-time job for IT security professionals; we can not expect our user community to take on the same burden. It is our job to make the basics clear, understandable and easy to apply to their daily work. While this is uncommon territory for many security professionals it is possible to obtain good results without creating a monumental workload for an already over stressed IT staff.

[1] Behind The Firewall
[2] Establishing a Solid Security Foundation

It is helpful to remember at the outset that the IT department is not an end unto itself. Computing services and data storage are simply tools that facilitate the real work of the business. In effect we are providing a service akin to the property manager on a construction site providing a hammer for the carpenter to use. It is immaterial to the carpenter how the wood was chosen for the handle, who affixed the head, who measured and assured correct balance. The important thing to the carpenter is that it *drives nails*. Every time. If the head flies off he won't be interested in hearing that it was the fault of some malicious fellow who snuck in at night and loosened it…he expects a tool he can safely use every day. It's our responsibility to keep the jobsite safe, not his.

It becomes more critical with each newly discovered threat that we encourage our users to be alert. The most important thing we can do is also potentially the simplest; communicate. It is not just a matter of having policies and procedures in place; we must engage the user community and facilitate their understanding in order to make any environment truly secure. This is not a technological issue, it is a people issue, and thus it often gets overlooked in the flurry of activity that marks the arrival of the latest worm, phishing attack, or DoS threat. Many security practitioners came to their positions by way of the technical side of the house, and thus "*employee education -- while "not sexy," … is really the linchpin for security*" [3]

Individual Responsibility

Despite the fact that the primary onus for security is on the security professional, the end user does have responsibilities as well. This is the area in which we can facilitate change that will result in real improvement in overall security. To continue the tool analogy, we may provide a hammer, gloves and goggles, but it must be the worker who acts responsibly by donning the gear and working safely. Similarly the end user must work within the policies and with the security tools that are provided. Since this does at times create some extra involvement for the user we need to educate them not just in what to do, but also why it is important. We need to be clear as to what the risks are to the user, their data, and the enterprise if they ignore or circumvent the efforts of the security team. "*An odd psychological factor about people and security is that even if people know how to do something, they often won't if they don't understand why*."[4] Policies regarding negative behavior and its consequences must be in place and widely disseminated within the user community in order to make enforcement a standard rather than an exception. Most people will react much more positively when there is a clear standard that all users are expected to follow as opposed to times when they see spotty enforcement. Often this sort of uneven application of the rules will be seen as a 'witch-hunt' and will be entirely counter productive.

[3] Panelists Offer Tips on Improving IT Security
[4] Weekly Security Planner

Once clear policies are in place, procedures are developed and implemented, and enforcement is uniformly and consistently applied, the job of securing the enterprise is still not done. Users must be trained, reminded, and encouraged frequently in order to keep security at the forefront of their minds. Following are some simple, practical ways to approach this.

Passwords

The first line of defense over which users have some direct control is the password. As with the workman and his tools, the user must be encouraged to use the locks provided for the tool chest. One would not leave thousands of dollars of tools in an open truck bed, how much less should we allow data worth orders of magnitude more than that to be left unprotected?

While this is one of the simplest and most important security steps that can be taken, it is also the one most likely to produce unhappy users. Passwords must be complex and of sufficient length in order to be effective. The goal is to make the time required for a brute force attempt so inordinately long that it will no longer be worth the potential intruder's time. The problem is that users don't like complex passwords. They are more difficult to create and more problematic to remember, and thus are more likely to be written down to avoid loss. There are two easy ways to deal with this.

First off, give your users some concrete hints on how to set a proper password. Developing a security handout that can be left with users when the support team has occasion to meet with the users is a great way to disseminate these and other hints and instructions. This can include the following password hints:

- Pick a phrase; "Mary had a little lamb"
- Take the first letter of each word "mhall"
- Add character sets (upper and lower case "mHalL"
- Add numbers and punctuation to raise the length to the required minimum "mHalL01!" [5]

These common hints may not seem like much, but to the user who has 'gotten away' with ineffective passwords for some time it may be that the only way to ensure change is to actually show him *how* to change. One must also clearly explain the risks of a weak password. "*Managers who want to stamp out weak passwords in their organizations should start with one simple step: tell users why weak passwords endanger their personal accounts and the organization's resources.*"[6] A recent situation with a high level user is a good case in point. The user had bullied help desk personnel into letting him use a weak password for years, in spite of a policy mandating password complexity and new

[5] Internal documentation
[6] Hold Your Own User Seminar

passwords every month. After 30 minutes of patiently explaining to the user why this would not be allowed to continue and what was at risk with his weak password he understood, but was still quite unwilling to work with a strong complex password. Until, that is, he was provided with a concrete way to develop a password that would both meet the company policy and be relatively easy to remember.

Another area that must be stressed with users is that passwords must remain secret. A policy must be in place and enforced that no one, not even high level support staff, will ever ask for a password. Users should be encouraged to not only keep their passwords secret, but also to report any attempts made to get them to divulge their password. Giving examples of some of the social engineering attacks that are prevalent today may help with the explaining the 'why' of this rule to your users.

In this case it is also necessary to educate and enforce policy with first and second level support. It's far easier to just ask for the users' credentials when trouble shooting an issue than it is to go to the desk side or take the time to create a new password and then set it to reset when the work is done, but absolute adherence is required on everyone's part in order to keep user passwords from being the 'low hanging fruit' that potential hackers will use to get inside the network.

Mailing Lists

Mailing lists are a similar and related risk vector for your users. Many people sign up for mailing lists, contests, and so called "*informative mailings from our partners*" without any idea of where the information is really going to be used. Most spam could be avoided in the workplace if users would simply refrain from using their work address for outside purposes. Encourage those who genuinely need to gather information from such sources to do so only from verifiably trustworthy organizations, or to set up a web-based email address with one of the many free services available. They can use these outside accounts for mailing list and related activities without the risk of inviting unwanted attention to their corporate email account. Setting up two outside email addresses for this purpose has resulted, in spite of the cancerous growth of spam in recent years, in only a couple of unsolicited emails arriving at actual work accounts each month.

Physical Security

On site physical security is not really an IT issue, is it? Probably not, but there are things that all users need to be encouraged to do in order to keep the integrity of the data that enterprises large and small depend upon. Strong passwords, encryption, and robust firewalls are of little use when the intruder has physical possession of the equipment. Employees must be alert at all times

to unusual activity. Strangers in the building must be challenged; all persons in secure areas should prominently display their badge or pass at all times.

For employees traveling with laptops, cell phones, and PDA's it is critical to stress physical security. Simple rules of common sense can make the difference between a productive trip and a disaster ending with confidential information in the hands of unknown persons. One security manager notes that "…20 to 30 mobile devices go missing from my company each year." [7] Users need to know that they should:

- Not check their laptops as luggage when flying
- Always keep physical control of their laptop
- Consider carrying their laptop in a non-descript bag instead of something that calls out "laptop!" A backpack or similar carry-on may be an option.
- When leaving their laptop while in use securely lock it to an immovable object with a high quality cable lock.

Clearly these are not revolutionary ideas, but they need to be stressed and repeated, even for the savviest traveler. On a recent trip to attend a security conference it was both amusing and appalling to note that of the 50 some attendees in the group, only a bare handful actually bothered to physically lock their laptops when they left the room. Hotel staff was in and out of the room unchallenged; and many times the room was completely unattended, and yet there were dozens of machines sitting unsecured on the desks…and this was a group of security professionals! Clearly this is a message that bears repeating.

Current Threats

One of the areas that will vary from organization to organization will be the determination as to which threats should be communicated to the end users. In most cases there is little to be gained in publicizing the latest TCP stack vulnerabilities or firewall holes, since most end users have little or no involvement in defending against that level of assault. There are many areas, however, in which the security professional can not successfully defend the enterprise without wholehearted cooperation from everyone on the network.

Virus protection is of course a 'front burner' issue with any responsible IT Security practitioner. Without this very basic level of protection the enterprise will likely spend more time fighting infections than conducting business. Several points must be understood by the users at the outset in order for them to understand their company's security policy and the dangers of malicious code being turned loose inside the network.

Current virus software must be required on *every* system in the enterprise. This

[7] Security Tools Search Falls Short

includes servers, laptops, and workstations and, by extension, home machines that may be used to access the corporate network. In any environment this should be a 'no discussion' issue. When a machine is found that does not have current virus software loaded and running on the network that machine should be removed from the domain. Furthermore in a truly proactive environment the machine AND it's user will not be allowed to connect again until the problem is remediated and the user has had a face to face meeting with his security manager to review and agree (in writing) to abide by the policy. This seemingly draconian measure will most likely not have to be enforced often; word will get around as to the seriousness of the issue.

Often users of resource intensive software will disable 'non-essential' software on their machines in an attempt to enhance performance. It should be clearly stated in the security handout that this is forbidden, and will result in removal of access privileges. A GPO can also be set to disallow machines not meeting the standard from connecting to the network.

Unauthorized installation of non-company approved software on company resources is yet another vector to be addressed with users. Simply including a ban on Shareware, freeware, and any other user loaded software will often not be enough. Users also need to be educated on the risks associated with spyware and the vectors by which they enter the system. Many browser 'assistant' programs include spyware that could potentially compromise the network.

It should go without saying (and thus you will need to repeat it loud and often), that point to point file sharing is against policy and forbidden. Quite apart from the risk of introducing malware to the enterprise there is also the risk of being the target of litigation if one of the more active copyright organizations decides to 'make an example' of the company. This must be a zero-tolerance issue if one is to protect the enterprise.

Social Engineering

Social engineering attacks attempt to gather information by low tech methods. The amusing con man of Hollywood movies is no longer just trying to trick the 'shill' out of a few bucks. There are dedicated people calling organizations of every type with intentions ranging from phone fraud to gathering information for a cyber-attack on the network. Users need to be educated on what to watch for, what information should not be released, and what to do if they suspect someone is attempting to glean information. When in doubt, instruct them to take contact information and promise to 'have my manager call you'. A great goal is to "*empower your employees through training to question fellow employees and do not assume anything.*" [8]

[8] Hacking Exposed

Simple Education

Once it has been determined that the user community needs to be educated, and which salient points need to be disseminated to each segment of that community, how does one go about it? Few companies are willing to fund an extensive education effort on the scale that many would like to see; in practice it's difficult enough to get funds allocated for the protective efforts that are already in place. The good news is that there are some very cost-effective ways to get your message across to your users.

The first thing to remember is to be creative. Emails filled with arcane jargon and long lists of "Do's & Don'ts" are not going to get very far in educating users, most likely they won't even be read. Below are some of the ideas that have proved effective, though none of them is a complete answer. A constant and consistent message to your users will have the best results. And don't be afraid to be blunt, fear can be a great motivator. When asked about encouraging employees to be safety conscious CIO William Farrow said "*We scare people*." [9] This doesn't mean you can not have fun with the seminar; in fact you should definitely plan for some light-hearted moments even though this is a serious topic. "*Many users will respond to a training session if it's entertaining. If you mix in a little fun with the training you're providing on a new IT initiative, users will respond positively and learn more*." [10]

The second point to keep in mind is that you are trying to teach non-technical people to be technically aware. In a discussion of teaching logic to the uninitiated it has been stated that "*when people can't understand basic concepts, it's usually because the terms in which the concepts are being presented is foreign and perhaps intimidating to them. put it into a context that the student can understand*."[11] It is quite easy to get your points across to your co-workers in IT, but can you make your point to the accountant down the hall? A true indication of your own level of understanding of a subject is how well you are able to teach it to someone who has no previous knowledge. If you can't make it clear to the CEO's administrative assistant why an eight character password is better than a six character password you need to go back and think about it yourself. A fuller understanding on your part will ease the conversion of your information into something that others can use.

First Things First

The first exposure employees get to IT security should occur on the first day they arrive at work. The Network Use Agreement and Acceptable Use Policy that is in

[9] Panelists Offer Tips on Improving IT Security
[10] End user training should be customized to fit the audience
[11] FoRK

place must clearly reference the security responsibilities of the individual. Full retention of the details of these policies may be low on this hectic day. Consider providing the user with hard copies to which they can refer at a later date. Also, requiring that each new user read the policies and agree in writing to abide by them will eliminate useless wrangling of the "I never knew!" sort later on.

Most organizations will also have a reminder notice set up in their login screen regarding acceptable use and possible monitoring by the IT department. This reminder can also serve as a memory jog regarding security. Consider modifying the message text to include the URL of your policy statements for easy reference. Of course long familiarity with the pop up will limit the efficacy of this message over time, but repetition is the key to user awareness. In an article discussing the molecular basis for learning, Dr. George Johnson states that "*It may not be the trendy way to learn, but repetition works."*[12]

And Second…

Another method useful in awareness efforts is to have a daily html pop-up window that is called as part of the logon batch file. This window can contain colorful graphics, active content, live links to current security topics, and any other brief content that could be presented on a security web page, if users could be enticed to browse to it. This window allows for frequent changes of data, essential in eliminating the boredom and the resultant lack of attention given to repeated reminders. The message should ideally be set to require a 'click-through' in order to clear the window. Users may not read it every day, but they are aware of it. Furthermore, relatively frequent changes, topics of current concern, and bright attractive graphics will increase that fledgling awareness as well as the overall level of knowledge that most users will retain.

Email Emergencies?

A great deal of discussion surrounds the need or wisdom of sending out an email alert to the whole user community when a new threat has hit the wire. Often such alerts generate more calls to the help desk than would be experienced if the threat were dealt with behind the scenes by the IT Security team. When to notify your users depends on several factors; how technical your users are, how much damage you may sustain from the threat, how vulnerable your organization is, and what actions you can reasonably expect your users to take. If there are concrete, practical steps that you can ask your users to take (or not take!) that will significantly mitigate the threat then a brief well worded message may be just the thing you need. If, on the other hand, there is little to be done outside of the back office, then you will succeed in nothing more than distracting users from their own work at best, and at worst you may take on the character of the boy who cried wolf (or in this case maybe 'The boy who cried

[12] Simple Repetition can have a powerful effect on learning

Worm!') so that future warnings are not taken as seriously as they should be.

If you do choose to send out email alerts to your users, create a blind account from which to send them. This should be an account that is not monitored and which will not receive mail. The body of the text should include any contact information for those who are dealing with the threat, if needed. A 'Good Housekeeping' reminder at the bottom of your alert can let users know that they can not reply to the message, and should delete it once read. This will cut down on unnecessary traffic on your system, though as stated earlier your helpdesk can expect some increased calls for clarification.

Handouts

A little time spent creating a colorful work aid to be left at the users' desk side is a particularly easy and effective way to increase security awareness. It is quite easy to hit the 'high points' in a simple tri-fold flyer. Some suggested points to make could include:

- User Responsibilities
- Common sense security
- Security policies (include the URL if you have these posted on your network)
- IT security contacts
- Password creation hints
- General security links

Take the time to make this readable, and remember it is a handout, not a sequel to 'War and Peace'. Keep the points brief and limit the content to what is easy and reasonable to expect the user community to understand and implement.

Live Training

Face to face training can also be of great importance. Many times there will be questions that are common across the breadth of your user base that, if answered individually, would take all your time away from the task at hand; protecting the enterprise. Lunch time 'Brown Bag' sessions are a great way to give your users some direct attention and to answer their questions, while at the same time getting your critical message across in a way that can be more readily accessed by your users.

To facilitate internal face-to-face training, first develop a list of potential attendees. This can include problem users with whom you've had to deal in the past on security issues, project or department leads, administrative staff, or people in more vulnerable job classifications. Perhaps you may want to target your sales staff and have a session on IT security while traveling. A session on acceptable use and virus issues may work well for corporate office staff, especially those who have legitimate needs to spend their time on the internet

and on email with people outside the organization. Once you have identified your potential audience you can send a targeted email to this group, inviting them to attend.

When you do hold your sessions remember: these people are giving up their lunch hour to listen to you. This is not the time to brow beat them for past mistakes, or to make them feel inferior for not understanding all that you do about IT security. They have shown an interest and made a commitment to helping you do your job, treat them accordingly. And try to make things fun - an hour of detailed lists, threat vectors, and virus examples will not only be terribly boring, but will not lead to any change of behavior, except for the lack of any response to your next offer of a seminar.

Consider using simple rewards as well. You don't need to spend a fortune on this; it can be as simple as a laminated copy of your security goals. For users who completed an end-of-session questionnaire perhaps a token gift or public recognition would be in order. A 'Certificate of Completion' often makes people feel like they've accomplished something with their time, and you will have gained valuable allies in your ongoing efforts to maintain a secure enterprise.

And that, really, is the bottom line. Information security must be a team effort in order to succeed. The time and effort spent to enlist those who are truly on the front lines will pay big dividends in the long run. There is a certain satisfaction to reading about the latest threats in trade magazines rather than learning about them first hand.

References

Coe, Kathy. “Behind the Firewall – The Insider Threat, Part 1” eWeek Online, 5 March 2004. URL: http://www.eweek.com/article2/0,1759,1543245,00.asp (10 March 2004)

eWeek Labs, “Establishing a Solid Security Foundation”, eWeek Magazine, Volume 21 Number 11 (15 March 2004): 44 – 45

Anthes, Gary. “Panelists Offer Tips on Improving IT Security”, Computerworld, 15 March 2004, http://www.computerworld.com/securitytopics/security/story/0,10801,91226,00.html (27 March 2004)

Bard, Shelly. “Week 6”. Weekly Security Planner. 22 January 2004. URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci945781,00.html. (12 Feb 2004)

Internal Document. Password Hints developed for user training, Employer of submitter – can not be released. December 2003.

Norton, Dana. “Hold Your Own User Seminar on Creating Strong Passwords”. Techrepublic.com. 18 June, 2002. URL: http://techrepublic.com.com/5100-6317-1039049-1-1.html?tag=series. (20 Feb 2004)

Thurman, Mathias. “Security Tools Search Falls Short”. Computerworld.Volume 38 Number 12 (22 March 2004): P. 36

McClure, Stuart; Scambray, Joel; Kurtz, George. Hacking Exposed. Berkeley: McGraw-Hill/Osborne, 2003. 590-591

Norton, Dana. “End user training should be customized to fit the audience.” Techrepublic.com. 12 July, 2002. URL: http://techrepublic.com.com/5100-6317-1038874.html. (16 Feb 2004)

Hong, James. “How do you teach fundamental logic…” Online discussion list. FoRK. 03 May 2001. URL: http://www.xent.com/FoRK-archive/2001.05/0139.html. (28 March 2004)

Johnson, Dr. George. “Simple repetition can have a powerful effect on learning”. Textwriter.com. URL: http://www.txtwriter.com/Onscience/Articles/repetitionlearn.html. (28 March 2004)

Last Updated: May 30th, 2017

Upcoming Training

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
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
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 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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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 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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 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
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
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
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event