Global Information Assurance Certification Paper

Scott Marchek
GSEC Version 1.3
5 Jan 02
User Security Training: Protecting Today's Network

Abstract

The core of an information security awareness program is training; some form of formalized instruction to impart information. This may be a classroom course, a software program, an extended briefing, a slideshow, or a printed package. It may be offered monthly, quarterly, annually or on some other repeating basis. User security training operates across these spectrums in yours and my organizations. This practical discusses developing a through core training program as a critical component of a user awareness program for implementing security policy. A training program should address "all" of the critical concerns of the organization, be content rich and interesting, and it should be delivered often enough to ensure both comprehension and retention by the users so that the information is known and can be appropriately implemented and acted upon when necessary.

Introduction

Who do security people love to hate even more than hackers and script-kiddies? The users, the irritating unwitting users who both provide us with hours of frustration and underwrite our paychecks; but why? Because they continually open virus infected e-mail. They unwittingly download spy-ware onto our network systems. They are forever walking away from their terminals while they are logged in. Yes, all of these are reasons we as security professionals love to hate our users. But whose fault is it? We are the trained professionals, we are the individuals who have conducted the risk analysis and read up on current threats. Have we properly imparted this information to our users? In most cases the answer is no. So we have no one to blame but ourselves.

With that said, there is something we can do about it. The core of an information security awareness program is training; some form of formalized instruction to impart information. This may be a classroom course, a software program, an extended briefing, a slideshow, or a printed package. It may be offered monthly, quarterly, annually or on some other repeating basis. It may contain large amounts of text, many facts, charts and graphs, or nothing but cliché statements and fluff. User security training operates across these spectrums in yours and my organizations.

Why this is Important

Network security has become of paramount importance to organizations around the globe as attacks from hostile agents and malicious logic increase at a seemingly exponential rate to directly compromise our critical operations. In some industries this is measured in millions of dollars, while in some others (such as the DoD) it is

measured may be measured in human lives. This focus establishes the criticality of user training. Users are the most important front-line sensor, as it's so frequently their terminals upon which difficulties occur. Consequently, user security training is crucial to the overall success of our operations.

Computer security professionals need look no further than current headlines to see why we need to protect our resources, the following are just a few examples:

> 1000 web sites defaced, James Middleton, 13 Aug 2001, http://www.vnunet.com/News/1124711
>
> Hell is 700 sites hacked in one minute, James Middleton, 13 Jul 2001 http://www.vnunet.com/News/1123915
>
> Experts crack 802.11 protocol, James Middleton. 8 Aug 2001, http://www.vnunet.com/News/1124574
>
> Students crack PIN protection system, 12 Nov 2001, http://www.compseconline.com/compsec/show/Products/COMPSEC/hotnews/hnnov01_4.htt
>
> Hackers steel account names/password from routers, 23 October 2001, http://www.compseconline.com/compsec/show/Products/COMPSEC/hotnews/hnoct01_30.htt
>
> The Shark Tank at Computerworld provides some excellent commentary on current IT events, frequently focused upon security. http://computerworld.com/cwi/sharktank/0,1130,NAV47-2057,00.html

Be this as it may, I had to look no further than my own organization to find a real world example of the value of quality user training. In May of 2001, the base commander coordinated to have a professional "Red Team" infiltrate and attack the base. They made it past the physical perimeter defenses, they hid in the bathroom of one of the building past closing and installed a sniffer on the wire of one of the network boxes, hidden in the drop down ceiling of one of the buildings. They walked up to an unattended terminal at a back corner cubicle and copied the pwl file off of the older Windows 98 system and acquired all of the passwords they needed. They crawled over the walls into the systems administrators office and found the new Win 2000 server he was starting to build, which didn't have appropriate security protocols in place yet, and gained Administrator access to the system. This wasn't all that they did (they did and tried some much more outrageous physical intrusions), but it was enough. They had us. It took them a little over a week.

They were scheduled for two weeks of "covert" activity before they really began to "attack". The day after they visited our building several of my users called me, having noticed things out of place, unusual names in their login blocks, computer screens turned or left on, etc. Some of the tell tale signs that someone had been

there. The users natural assumption was that it was my help desk staff just working on their PC's to install updates or some such. But it was training to follow incident response SOP which caused them to call me. Their awareness caused me to have my staff review the logs 4 hours earlier than we would have otherwise. We caught them and locked them out, a week before they expected. Now the "damage" had been done, we'd been compromised, but the objective lesson of this story is two-fold: user training "saved" us from continued exploitation, and this event also highlighted for us the importance of more aggressive user training in those areas where policy implementation was deficient. This example clearly showcased to upper management the criticality of user training for success of our operations.

Purpose

The problem at hand is developing a core computer user security training program as a component of an overall awareness effort. This practical investigates how best to develop a network security user training process focused upon training methodology, frequency and content. Industry research, analysis and research I've conducted at my own organization will be used to help ensure the proposed solution design is thorough and complete to heighten the likelihood of successful implementation.

Background

Mike Cunningham's paper, *Acceptable Use Policy*, showcased the Computer Security Act of 1987 requirement for periodic training of all federal employees who are involved with the management, use, or operation of any Automated Information System (AIS). This is frequently mirrored by industry requiring trained employees as well. Continual increases in the skills, capabilities and number of hostile agents and malicious logic targeting our systems and users presents a very real threat to continued successful network systems operations.

The FY 02 USAF budget for IT defense is $1.8 billion (FY 2002 Budget). The primary focus upon USAF defense has been perimeter defense (firewalls), intrusion detection systems, cryptography, and adherence to sound policy. This seems to be mirrored by industry (Violino, 2001 and Levitt, 2001) and what is mentioned in the Security Essential course work. This occurs despite the multi-billion dollar impact from poor user decisions (Snyder, 2001). However, user training directly supports policy implementation, as it is network users who operate the systems on a daily basis. It is defense in depth in action.

Content

Users are acknowledged throughout the IT industry (e.g. Rash, 2000, Rovelto, 2001, Hayes, 2001, Frank 2000, Hayes, 2001) as the front line sensor of systems malfunction or perceived attack, thus sufficient security training is imperative to continued overall network operations.

The primary questions posed then are what to train, how and how often. My

background is with the USAF and a review of their standard training requirements (as provided by AFI 33-204 and AFCA Information Systems User Computer Based Training (CBT) module) includes the following subject areas:

Mission criticality	E-mail Use and limitation
Incident Response	Password policy
Internet Use and limitations	Media Marking
Anti-Virus use	Handling Classified data
PDA policy	Cell Phone policy
Copier/Fax policy	Backup policy
Certification & Accreditation	Classified STU III phone policy

These training areas compare fairly well with review of crucial user training areas from the industry as a whole. The following areas (in black) are matches from several industry training programs, with a few additional areas to consider (listed in red):

Password Protection	Email Security
Internet Concerns	Data backup
Physical Security	Virus Detection & Protection
Telecomm Fraud	Social Engineering
Computer Crime	Hacker Practices
Hoaxes	Denial of Service Attacks

(Dean, 2000, Hayes, Heather 2001, Hayes, Frank, 2001, Genusa, 2001, GoSCI, 2000)

In Oct 2001, I conducted a research project in my own organization to compare the elements in this initial list for effectiveness, importance and value added of each component. The results of this study demonstrated clear support for most of these training areas and elicited several other subjects for consideration, which concluded in the addition of the following to the list:

Network resource server storage rules
INFOCONS (activities in heightened security states) (this was a military study)
Home Anti-Virus (USAF policy allows users to take Anti-Virus program home)

In addition to ensuring subject inclusion, the training must be content rich. A frequent complaint I've received from government provided training is "why are you wasting my time with this drivel?" Getting everybody together for an hour-long briefing of tired cliché's or overly boring slideshows can do more damage than good by alienating your users. The users time is as valuable to them as ours is to us. Ensuring that the training covers all necessary subjects, but also does so in a useful and efficient fashion is crucial. Kenton Smith's practical, *Security Awareness: Help the Users Understand* and Harbinder Kaur's practical *Introduction and Education of Information Security Policies to Employees in My Organization* provide some excellent

detail development for some of these training areas, and example of content rich, yet succinct subject discussion.

Finally, the content form should be delivered in a method which doesn't bore the user or chase them off with jargon heavy technical details. While your program may hit on all of the important areas, the delivery is important. Stories, such as those presented by some of the authors of GSEC practicals (Charles Coffey's Information Warfare – It's Everybody's Battle is an excellent example) can be very valuable at showcasing examples as well as explain a subject while still being interesting and possibly entertaining. Tying successful user practices with successful mission or business operations provides users with a sense of ownership and responsibility for their actions, a behavior crucial to the success of any training program. This leads well into discussion of the next aspect of running a training program: training methodology.

Training Methodology

The next question revolves around the best training delivery medium. Industry review identifies Slideshows, CBT, Web based training and traditional classroom training.

CBT and Web Based solutions highlight ease of use, economy of implementation, self-pacing for reduced mission impact and include testing to examine topic proficiency (http://www.flextraining.com/, http://www.thrnet.com/due.htm, http://www.eno.com).

Traditional classroom activity provides direct interactive capability along with the possibility of mass training, but comes with a fairly sizable mission impact (taking people out of their work place) and is priced on the high end for delivery and implementation.

In the research I conducted in my own organization, I compared each alternative in each of the following areas: Cost/benefit analysis, Risk factors, New systems training, Hardware/software, Personnel requirements, Maintenance, Ease of use, Mission impact and the results of the questionnaire. I'm presenting the finding here because I believe they will be of value in considering delivery methods for your organizations.

Cost/Benefit Analysis. The primary intangible benefits of the training are: reduction in compromised/lost data and protection from attacks. Tangible benefits include reduced systems down time from virus infections and attacks, and fewer prosecutions from crimes and mistakes by internal personnel. All three delivery methods are expected to return like intangible and tangible results. Where they differentiate is on the variable of development costs. Table 1 shows these in comparison.

Risk Factors. The three implementation methodologies vary little in risk factors, in that all are believed to have the potential to be successfully implemented, and introduce no new primary risks from their operation.

New Systems Training. The slide show option incurs no user training, and only training the security managers who will present the slideshow, a very low projected cost. The CBT option and the Web-based option require training for every user; however, this can be moderated with simplified GUI operations, detailed instructions

and useful help files. Table 2 shows the systems training comparison.

Hardware and software requirements. These are compared in Table 3.

Personnel requirements. These are demonstrated in Table 4.

Maintenance. Table 5 showcases a comparison of each option in terms of ease of maintenance and projected maintenance costs. As you can see, the low-tech slideshow comes out on top. Simple solutions frequently do.

Ease of Use. The proposed systems vary substantially in their ease of use for the users, as Table 6 showcases.

Mission Impact. This area is of high importance to upper management of my organization, and was deemed critical for acquiring and maintaining high levels of upper management support. Thus a double weighting factor was given to its results, which may be viewed at Table 7.

Summary of Factors. Summarizing the ratings of all factors (see Table 8) provides a slideshow as the preferred and "best" method (from my study), although a web-based program was very close behind. This suggests perhaps a web-based slideshow, which would combine the advantages of both of these methodologies, might be the "best" solution.

In addition to the weighted evaluation, I suggest the use of a questionnaire survey of the organization's personnel. It doesn't have to be very large to be scientifically valid and can provide a wealth of information on how the users see these subjects and value these proposed approaches. It also may help instill a sense of ownership in the process when employees can see their opinions being taken seriously and acted upon.

For implementation in another organization, I would suggest following this simple analysis to determine the "best" solution for your organizational needs. We as security professionals frequently find ourselves in the position of having to sell security to management. Going in prepared with the tools to show why your proposal is the best solution can be an invaluable in achieving the overall security program's success.

Duration and Frequency

Another factor for consideration is duration and frequency. Both users and upper management seem to overwhelmingly prefer short training of limited frequency, to limit inconvenience from the user's perspective and limit mission impact of taking up production time from the manager's perspective. This doesn't make this answer "right". For organizations with an active awareness program and at least one person dedicated to it's operation, perhaps annual primary/refresher training augmented with regular notices, emails and mini briefs will suffice. For other organizations, say without a dedicated security manager or operating with high employee turn over or bleeding edge technologies, a more frequent training regimen would be more appropriate. Frequency decisions should account for these variances with the ultimate goal of ensuring that the organization's users know what to do when the time comes: how to build appropriate passwords, how to notice unusual activity, who to call for incident response etc. Policy is useless without users who know how to implement it. Training should occur as frequently as necessary to achieve this goal.

Testing Component

Another question of a training program is that of a testing component. It's been my experience that training programs with a testing component are learned more thoroughly, than those without. If the user is expected to 'prove' comprehension, they frequently will pay closer attention to the material presented.

Some government recurring training requirements (Safety, Operational Risk Management, EEO, and Sexual Harassment Prevention) are simply provided as mass briefings with no testing. However, USAF policy does require a testing component to for "demonstrate information comprehension" for Information Security training. NIAP identifies, "Competent, independent security testing is needed by anyone who wants to design and build, market, procure, or employ products or systems requiring any level of security or trust."(NIAP, 2001) This is equally applicable to the system of training users.

Conclusion

A core training program is not the totality of an awareness program, but it is the core of it: the means of putting policy into action. Websites, regular e-mails, pamphlets, signs and lunch-time seminars may augment this training to round it out and present a complete program, however a well developed and through core training program is critical for implementing security policy. A training program should be thorough, addressing "all" of the critical concerns of the organization, content rich and interesting, and it should be delivered often enough to ensure both comprehension and retention by the users so that the information is known and can be appropriately implemented when necessary. This core training program is the vehicle for implementing the policies we've developed to ensure the application of defense in depth amongst the user community as the GSEC program descries.

References

Rash, Wayne. (2000). Training Users is Best Defense Against Viruses Like `LOVEBUG'. InternetWeek, 813, 80.

Rovelto, T. Rose. (2001). Security--an Issue That Should Concern You!. National Public Accountant, v. 46 no4, 30-32.

Dean, Joshua. (2000). Finding the Weak Links in Security. Government Executive, v. 32 iss1, 48-50.

Hayes, Heather. (2001). Loose Lips and Other Risks. Federal Computer Week, 18 June. http://www.fcw.com/fcw/articles/2001/0618/sec-feat3bx2-06-18-01.asp

Hayes, Heather. (2001). Prepping the Front-Line Troops. Federal Computer Week, 18 June. http://www.fcw.com/fcw/articles/2001/0618/sec-feat3-06-18-01.asp

Hayes, Heather. (2001). Security Training Checklist. Federal Computer Week, 18 June. http://www.fcw.com/fcw/articles/2001/0618/sec-feat3bx1-06-18-01.asp

Hayes, Heather. (2001). Pros and Cons of Computer-Based Security Training. Federal Computer Week, 18 June. http://www.fcw.com/fcw/articles/2001/0618/sec-feat3bx3-06-18-01.asp

Frank, Diane. (2000). Training the Security Troops. Federal Computer Week, 10 April. http://www.fcw.com/fcw/articles/2000/0410/sec-train-04-10-00.asp

Hayes, Frank. (2001). Big, Ugly Security: How to Make Security Less Annoying. Computerworld, 09 July. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO62041,00.html

Hayes, Frank. (2001). Secure Your Users. Computerworld, 24 Sep. http://www.computerworld.com/rckey73/story/0,1199,NAV47_STO64157,00.html

Genusa, Angela. (2001). 12 Keys For Locking Up Tight. CIO Magazine, 1 Mar. http://www.cio.com/archive/030101/keys.html

Ramirez, Charles. (2001). Cybercrimes Cost Businesses Billions. Detroit News, 29 May. B01. http://detnews.com/2001/technews/0105/29/b01-229644.htm

HQ USAF/XOFI. (1999). Information Security Program Management. Air Force Instruction 31-401.

HQ AFCA/GCLO. (1999). Licensing Network Users and Certifying Network Professionals. Air Force Instruction 33-115V2.

HQ AFCA/GCI. (2000). Computer Security. Air Force Instruction 33-202.

HQ AFCA/GCI. (2001). Computer Security. Interim Change 2 to AFI 33-202.

Air Force Intelligence Agency. (1994). The C4 Systems Security Awareness, Training, and Education (SATE) Program. Air Force Instruction 33-204.

HQ AFCA/GCI. (1998). Network Security Policy. Air Force Systems Security Instruction 5027.

GoSCI (2000). Frontline. http://www.gocsi.com/db_area/frontline/FrontLinepromo.pdf

Snyder, John S. Jr. (2001) Business Impact Analysis for the Security Professional. May 16, 2001. http://www.sans.org/infosecFAQ/securitybasics/impact.htm

Violino, Bob. (2001). Information Security Spending Rising, But Still Inadequate, Study Says. Information Week. February 14, 2001. http://www.informationweek.com/newsflash/nf617/0214_st2.htm

Levitt, Jason. (2001). Security - The Enemy Within. Information Week. April 23, 2001 http://www.informationweek.com/834/secure.htm

Defense Budget Materials Amended FY 2002 Budget http://www.dtic.mil/comptroller/fy2002budget/index.html

NIAP (2001). Need for Security Testing. National Information Assurance Partnership. http://niap.nist.gov/background.html

Cunningham, Mike. (2001). Acceptable Use Policy http://rr.sans.org/policy/use_policy.php

Smith, Kenton. (2001). Security Awareness: Help the Users Understand http://rr.sans.org/aware/help.php

Kaur, Harbinder. (2001). Introduction and Education of Information Security Policies to Employees in My Organization. http://rr.sans.org/aware/infosec_policies.php

Coffey, Coffey. (2001). Information Warfare – It's Everybody's Battle. http://rr.sans.org/infowar/battle.php

Table 1

Cost-Benefit Analysis Comparison

Methodology	Projected Development Costs	Projected Maintenance Costs	Projected Operations Costs	Overall Rating
Slideshow	2 Weeks $1500	3 Days/Year $500	Sec Manager conducting Briefings $1,000 per year	1
CBT on the user desktop	8 Weeks $25,000	2 weeks/year $4500	Sec Manager tracking $4000 per year	3
Web Based Program	8 Weeks $25,000	2 weeks/year $3000	Web administrator maintenance $5000/year	2

*Ratings from all comparison elements will be compiled to establish best methodology

Table 2

New Systems Training Comparison

Methodology	Primary Projected Training Impact	Overall Rating
Slideshow	No User Systems Training Time. Security Manager Training only. **Low**	1
CBT on the user desktop	Moderate training requirement for each user & Security Manager & Helpdesk training to answer user questions. **Medium**	2
Web Based Program	Moderate training requirement for each user & Security Manager & Helpdesk training to answer user questions. **Medium**	2

Table 3

Hardware and Software Requirements.

Methodology	Hardware Requirements	Software Requirements	Overall Rating
Slideshow	Minimal: standard issue	Minimal: standard issue	1
CBT on the user desktop	Moderate: about 4MB per desktop	High: Development of standalone program	3
Web Based Program	Minimal: Hosted on existing server	Moderate: Web page development	2

Table 4

Personnel Requirements.

Methodology	Development	Operation	Overall Rating
Slideshow	Low: 1 person	Low: Sec Manager only	1
CBT on the user desktop	High: Software Development team	High: Every User	3
Web Based Program	Medium: Web Developers	High: Every User	2

Table 5

Maintenance.

Methodology	Ease	Projected Costs	Overall Rating
Slideshow	Low: 1 person	Low: Less than $1000/year	1
CBT on the user desktop	High: Software Development & recompilation	High: About $4500/year	3
Web Based Program	Medium: Web page Maintenance	Medium: About $3000/year	2

Table 6

Ease of Use.

Methodology	Ease of Use	Overall Rating
Slideshow	Low: No requirement of user, Security Manager action only	1
CBT on the user desktop	High: User operates computer program	3
Web Based Program	Medium: User navigates web page	2

Table 7

Mission Impact.

Methodology	Mission Impact	Overall Rating
Slideshow	Security Manager conducting briefings on demand, users briefed en mass where available **Medium**	4
CBT on the user desktop	Security Manager Results tracking only High hardware resource intensity User conducts training in their workplace at their own pace & as mission schedule allows **Medium**	4
Web Based Program	User conducts training in their workplace at their own pace & as mission schedule allows Automated tracking and operation **Low**	2

*Criticality of Mission Impact is basis for double weighted rating

Table 8

Questionnaire Results: Methodology

Methodology	Rating Results	Overall Rating
Slideshow	1 1 1 1 1 1 4	10
CBT on the user desktop	3 2 3 3 3 3 4	21
Web Based Program	2 2 2 2 2 2 2	14

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
SANS Copenhagen 2017	Copenhagen, Denmark	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