Global Information Assurance Certification Paper

Promoting Security from the Middle

By Siegfried Hill

The purpose of this document is to suggest some management approaches a small IT shop System Administrator can take to further his or her security initiatives.

The Haves and the Have Nots

A great amount of resources are being dedicated to improve information security in many corporate and governmental organizations [1]. These organizations usually have a well-equipped and well-staffed IT team with a high-placed executive to promote important IT issues. Conversely many other IT shops have a disproportionately small IT staff. These shops are the ones that rely heavily on the initiative of one or two individuals to develop and maintain the bulk of their security measures. Unfortunately for the better-equipped organizations, the vulnerabilities of these smaller shops are rapidly becoming an issue for the well-staffed IT team's own security in the form of such attacks as Windows Distributed Denial of Service [2].

Caught in the Middle

Consider a hypothetical shop that has 65 PCs, an NT domain controller with backup, a web server, and an FTP server. This shop has one System Administrator for the servers who also has the responsibility of maintaining the client PCs. The management (on one end of this business) is focused on selling widgets, and considers a computer in the same breath as all the other office equipment. The clients (the office staff on the other end) understand the computers better, but view them as tools to get their job done; they are therefore indifferent to any aspect of the computer that does not directly relate to the performance of their job. Stuck in the middle of these two groups is the System Administrator. The security tasks before this System Administrator are:

1) educate management about issues related to security and convince them to free up resources from widgets to implement security;
2) optimize the resources at her level to give her enough time to complete her tasks in a timely manner, and;
3) enlist the support of the clients to allow the necessary changes in client behavior and operations to implement security measures.

She must accomplish these tasks without alienating too many people, without compromising her career, and without negatively impacting her or her assistant's other duties. This may sound like an unrealistic expectation for this administrator, but I have found that there are management techniques for the part-time administrator to improve their security without having to sacrifice their career or sanity. With the right mindset and a healthy dose of patience, you can slowly affect change from the "middle".

Keep Expectations Realistic

If you are in a .GOV or .ORG that has tight funding, forget that "ideal shop" that SANS and CERT would love everyone to have (at least for the near future). The organization with a corporate culture imbued with a sense of urgency regarding security will accomplish this ideal quickly. The rest of us will have to settle for a more gradual embrace of IT security. Accept this. Remember the saying by Confucius: "A journey of a thousand miles begins with a single step." Keep focused on small victories and achievable goals. Every little step closer to total security is that much farther from system compromise. If you focus on getting everything locked down immediately, you will run out of enthusiasm and willpower before you achieve that goal. Do not lose sight of that "ideal shop" though; it is attainable. But be warned: it may take *years*.

Put It In Writing

Accept your risks and related potential losses. Whatever condition your security is currently in, you are implicitly accepting the risks and potential losses involved with your IT systems. If you have not already, formalize these risks and losses by documenting them. Get ahead of the game and create a risk analysis document. A risk analysis lists your major information resources, what bad things could happen to them, and what measures, if any you are taking to 1) eliminate the risk, and/or 2) reduce the potential impact of the risk. Many organizations have mandated formal risk analyses [3,4] but a concise document hashed over a long cup of

coffee is a fine start. A written risk analysis accomplishes two things: it gets your head together, so to speak, so you better understand the tasks facing you, and it provides you a concrete document to begin educating your management "end" of the business. Present the risk analysis written in laymen's terms to your immediate superiors and if possible, their superiors. Request that they sign the document indicating that they have read and understood the risks and potential losses facing the business. Odds are good that once you have detailed these risks in this way, you can expect more support. Don't expect miracles, though. At worst, the fact that your supervisors acknowledged the risks will provide a "cushion" for your career if the losses you outlined should become reality.

Choose Your Battles

After you have outlined your risks, you need to prioritize which risks must be addressed immediately, which risks can be addressed over time, and those risks which you are going to accept without taking any action. There may be risks you absolutely should address, but cannot because of reasons beyond your control. Some examples of reasons that would force you to leave a risk unresolved could be budgetary constraints, a lack of authority over associated resources, or bureaucratic mandates. Remain concerned about these risks; inform your supervisor about their unresolved status, and stay alert to a change in the inhibiting factors around these risks, but *accept* them. The time to address those risks will come and, when the opportunity is right, you should be ready to resolve the risk. Struggling to correct a risk at the wrong time is a waste of the precious few resources you do have. Picking a fight with clients or management over the removal of a risk at a time when the organization is not ready to change can result in a grassroots resistance against all your efforts to implement security (or any other policy for that matter!) Keep in mind that a risk in the system, by definition, is part of that system. What you consider a risk may exist because it is an asset for those with whom you are at odds. Get an understanding of the workflow involved with the risk. Consider working out a middle ground solution where the risk is managed, but the functionality is not completely removed. If such a compromise is unreachable, you may have to leave the risk as "understood and accepted" in order to gain support from clients and/or management to correct other risks. On occasion it takes the realization of actual loss related with a risk to galvanize support for correction of a risk. Don't view this as "closing the barn door after the horses have gotten out". Rather, seize the opportunity with your prior planning and newfound support to quickly and *tactfully* correct the problem. [5]

Use That Computer

All the statesmanship described above requires a valuable resource: your time. Free up your time a little by automating your administrative functions. Get a regularly scheduled tape backup running and have it automated so you only have to swap tapes. Get inexpensive tools available from the web for monitoring the status of your servers. If you have to, push to get a consultant to come in and set up the scripts so you can automate your event logs [6] and other reporting processes. Install on all your systems antivirus software that allows unattended, scheduled updates off of the internet. (Several of the major antivirus products provide this feature.) Visit your software vendor's update sites [5] and subscribe to the same vendor's security alert lists. Use a batch script (see appendix) and a simple database to keep track of the patches you get from those channels. Gain visibility of your systems by gathering relevant information and dropping that information into another simple database. Update your information as time permits. After you have it gathered in a searchable database, this information will allow you to quickly make informed decisions about the scope and magnitude of a risk to your systems should a new risk crop up.

Inspect the Troops

While you are performing the routine work on your clients' machines, do some forensics. Pay attention to who has the perfectly clean desktops and who has so many files out on top that 'My Computer' is buried. Look for telltale signs of 'promiscuous' clients who may be installing every screensaver they get by email. Make notes (if only mental ones) of who has installed MP3 grabbers and who opens twelve applications at startup. Keep an eye out for undeleted installers and those 'Recycling Bins' that never get emptied. From this you can develop a

feel for those who might be at higher risk for system violations. In addition to identifying high risk clients, you can single out those savvy clients who may be able to help you by being 'front-line' troops in the fight to keep the client systems secure. I like to affectionately call these folk "Junior Tech Support". "Junior Tech Support" are those non-IT staff who love computers enough to understand them beyond mere literacy. Frequently you will find they have already initiated troubleshooting procedures before you get wind of any problem. These are the clients you want to educate, encourage, and support as much as possible in the course of your work. They can detect intrusions and compromises much faster by virtue of the fact that they are there when it happens and are much quicker to notice anomalies than your average client.

Network, Network, Network!

Just as your "Junior Tech Support" can sharpen their skills from you, don't underestimate your ability to learn and grow from your peers. Get on those listservs and User Group newsthreads! Communicate! Usually you can find answers to a security question you may have just by reading existing posts. Otherwise, you can post a question and other professionals are usually quick to post a reply with their experiences. Every major operating system has a listserv dedicated to informing users about security updates and issues with the software [7]. The web is a cozy place. Don't be afraid to send an email requesting help or information from someone who is an expert in their area of knowledge. More than likely they would be glad to assist and, at worst, you may get ignored. As has been demonstrated by the Motion Picture Industry [8] attempting to go it alone in cyberspace can be disastrous.

Persistence Pays Off

As you probably noticed, the above suggestions can be time consuming to follow. If you don't have a budget for a lot of people to spread the tasks out, then you have to spread the tasks out over time. Be patient. The investment in bringing management to understand the bottom line of the risks, getting yourself better organized, and training your clients will, over time, allow you to more efficiently identify and resolve security issues.

[1] "Supporting the World's Strongest Military Force." Budget of the United States Government Fiscal Year 2001. 9. 7 FEB 2000. URL: http://w3.access.gpo.gov/usbudget/fy2001/pdf/budget.pdf (11 SEP 2000).

[2] Pickel, Jed. "CERT® Incident Note IN-2000-01 Windows Based DDOS Agents." 28 FEB 2000. URL: http://www.cert.org/incident_notes/IN-2000-01.html (11 SEP 2000)

[3] Commonwealth of Virginia Council on Information Management.
"Risk Analysis: Identifying Potential Threats." ITRM Standard 95-1 Information Technology Security. 31 JAN 1995. URL: http://www.dtp.state.va.us/pubs/standards/s-95-1.htm#sec3
(11 SEP 2000)

[4] "Risk Analysis." Florida State University AIS Data Management/Computer Security.
URL: http://www.aus.fsu.edu/dm_sc.html#ra (11 SEP 2000)

[5] Northcutt, Stephen. "Computer Security Incident Handling Step-by-Step." Version 1.35. 5 SEP 2000. URL: http://fbox.vt.edu/cc/security/i.pdf (11 SEP 2000)

[6] "Dumpel.exe: Dump Event Log."
URL: http://www.microsoft.com/windows2000/library/resources/reskit/tools/existing/dumpel-o.asp
(12 SEP 2000)

[7] "Vendor Tools and Information." SECURITY.VT.EDU. 3 APR 2000.
URL: http://security.vt.edu/lockitdown/index.phtml#VendorToolsInformation
(11 SEP 2000)

[8] “Cease and DeCSS: DVD's Encryption Code Cracked.” Emedia Industry News. 4 NOV 1999.
URL: http://www.emediapro.net/news99/news111.html (12 SEP 2000)

Appendix:
Using a DOS batch file and a database program to keep track of your downloaded patches:

1) When downloading your patches, store them in a flat directory structure with a directory for each common group of patches, directly under the root, and named appropriately. For example, you would create a directory under ‘C:\’ called ‘PATCHES’. Under ‘PATCHES’ you would create several directories labeled ‘WIN95’, ‘IE5.0’,’OFFICE2K’, etc. No directories would be stored under this layer of directories. This flat structure facilitates the database import process.

2) Run the following from the command prompt at the ‘C:\PATCHES’ directory level:
dir *.exe /s /b >dirlist.txt
Note: this assumes your patches are self-extracting. If they are zip files or other extension, use the appropriate extension to replace “.exe”.

3) Import the resulting text file “dirlist.txt” into a blank database, using the backslash “\” as a delimiter.

4) Create a quick and dirty report grouped by the third column and you will have a current list of your patches as a checklist. You may choose to add a field in your table that resolves to true or false that helps you keep track of those patches you have applied to your systems.

Last Updated: May 27th, 2017

Upcoming Training

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