Global Information Assurance Certification Paper

Implementing a Security Program from the Beginning, for the Beginner

Thomas Paulger

GIAC Security Essentials Certification Practical Assignment Version 1.4b, option 1

July 9, 2003

Abstract

The beginner in Information Security will be overwhelmed by the daunting task in front of them, especially in a situation where Information Security was not accorded the importance it requires in today's connected world. This paper will help the new security administrator start a security program from scratch, and allow him/her to grow the security program to fit the business over time.

Introduction

"Oh, no, I was just appointed as the IT Security Manager!"

Here it is. You wanted new responsibilities and now you have them. However, that feeling in the pit of your stomach is making you wonder if you did the right thing. You are thinking, "What do I do now?" First of all, calm down, take a deep breath and congratulate yourself on your new position. Then, follow these steps and you will have a process for security and can start to impose some order upon the chaos for which you are now responsible.

Risk Assessment:

Whether you do a lengthy, formal risk assessment, or some shorter, informal brainstorming, you need to do a risk assessment. Why do you need to do this? You want to make sure you have a realistic idea of what you are facing. You need to respond to and mitigate risks appropriately, and to do this, you need to know what your risks are and what you are protecting. It doesn't make sense to spend a thousand dollars protecting something worth one hundred dollars, does it? Security is a process that you will be doing over and over again; recording what you do the first time will make risk assessment much easier to do the next time. During future assessments you just have to update your information, so it should go more quickly. This time, however, you need to start from scratch (somewhat) and understand the process as well as what needs to be done. The following steps will get you through the risk assessment.

- Threat Assessment and Analysis - This is a two-step process. First you identify all the threats against your organization. Depending on the nature of your business, you have to focus on different things. Commercial

business will primarily focus on threats to profit. Threats to the ability to provide services (especially essential services) will be the focus for government agencies. Many of the threats are the same, but you may end up prioritizing them differently based on your line of business. Identifying threats can be as simple as making a list. Remember, though, that you cannot protect yourself against all threats, so prioritizing and concentrating on the 'big' ones is necessary. That prioritization is the second step in the process. Once you have a prioritized list of threats, you can move on. Some threats you will see are common and highly visible, such as viruses, hackers, insider misuse, power loss, etc.

- Asset Identification and Valuation - Asset identification is something you certainly want to have help with. You can go out and inventory all your systems yourself, but you may be surprised by what your management thinks is valuable and what it is actually worth. Make up a short survey to be filled out by mid level management, and have them send it up through their supervisors for review. What you are looking for is a list of "systems" and how important they are to the organization. "Systems" can include servers, databases, email and the like. Use some sort of standardized rating scheme so that each manager can prioritize their systems. Use dollar values if available, otherwise use a number rating scheme, with 1= Most Important, and 5= Least Important. Since tangible assets are listed on corporate balance sheets, you may get some assistance with that portion of the inventory from your accounting department. Once you get a list together, you will have to merge all the priorities so that you have one comprehensive list. Of course, if you can get management to do this collection and summary for you, so much the better. However, this collection is probably going to take a while, so try to involve management more the second and subsequent time you identify and value assets. Start off by making and prioritizing a list. But remember, this is more than just a simple inventory of hardware. A database of names might be very valuable to your company's business model, but will not have a good dollar value in an inventory listing. There are several freely available sources to help with this; one of the best and simplest to start with is the Security Targeting and Analysis of Risks (STAR) Program from Virginia Tech. Take a look at their Business Impact Analysis/Risk Assessment for Information Assets documents, and you will be able to use that as a starting point. Of course, there are more comprehensive and complicated processes available, and depending on the complexity and scope of your network, you may need to explore those options. The National Institute of Standards and Technology (NIST) provides a free software-based questionnaire/survey called ASSET (Automated Security Self-Evaluation Tool) which is very comprehensive (and free) but of course, takes much more work. I suggest reviewing both and determining which might suit your needs best.

- Vulnerability Analysis - Now that you have some idea of what you are responsible for and how valuable it is, you should combine that knowledge with potential threats. Together, the asset list and possible threats will allow you to identify vulnerabilities and mitigate against them in a logical and cost effective way. There are many standard listings of common vulnerabilities. Some of the most comprehensive may be found at SANS or at Carnegie-Mellon University's CERT-CC (Computer Emergency Response Team-Coordination Center). There are many others, but I strongly recommend that the novice pick one or two and try to keep up with the flood of vulnerabilities. Take the list of systems you developed and go through and search for vulnerabilities to your particular systems, using the web sites listed above, or another that you prefer. Do not become complacent, however, since vulnerabilities are constantly being discovered, and exploited.

- Risk Evaluation - Now that you have a good idea of your vulnerabilities and systems, you should figure out what to do about the threats. You basically have three choices: accept the risk, mitigate the risk or insure against the risk. You should have a decent idea what to do about the vulnerabilities and risks based on your previous work. For example, malicious code is a fairly high threat and most systems are vulnerable. Mitigate the risk by planning to implement some sort of virus protection. You can never eliminate risk but you can reduce it to an acceptable level. Don't just accept all risk because nothing bad has happened to you yet. With that attitude, it will. You also have to make sure you take reasonable (as opposed to unreasonable) actions to reduce or transfer your risk. For example, you don't buy expensive locks and lots of insurance to protect your $100 lawnmower from theft. So, for each threat and vulnerability, plan what you will do to reduce threats to an acceptable level, and insure against others if necessary. If that means literally getting an insurance policy, then do so.

- Report to Management - Now that you have gone through all this, you need to enlist management in your plan. Hopefully, you have a good relationship with management and have the goals of the organization at heart, since this is, in fact, the real reason to secure your systems. Start with a summary of what you have done, keeping your audience in mind. Then list all the systems you identified in your inventory and prioritize them. Values are important here, either in dollars or in value to the mission of the organization. Make sure that this value is presented in your report. Finish the report with your plan to management. You need to come in telling them what you propose to do to make things better. Do not come in telling them of all the problems, and ask them what they would like to do. You may get away with it, but you won't look good. I suggest briefing management with at least one plan. Two or three "courses of action" are even better, with a recommendation for one of these courses of action at the end of the presentation, with the reasons why. Solutions are what management wants

to see when they are presented problems, not just the problem itself. So, this done and with management approval, you can move on. Remember, this is an ongoing process, so keep records of what you have done, and be prepared to do it again later.

Policy Development

Policy Development can be a daunting task for anyone, let alone a systems person who might have much more technical expertise than writing experience. But, you have to face the fact that you need policies and that you are the one who knows what policies are needed. Follow the guidelines below and you will make it through this step.

- What are "Policies" and why have them? - Policies are really the formal communication of the organization's rules to everyone concerned. Unwritten policies are not useful to the security administrator when there is a conflict. You need to have something in writing, supported by those at higher levels in the management hierarchy than either you or the person with whom you are in conflict. Developing written policies that reinforce security is your job, if security policies are not in place already. Policies will tell everyone what is expected of them, and how they are supposed to act in certain situations. We all need this guidance; otherwise we tend to act in our own self-interest, which isn't always the best for the organization as a whole. Even though we all (well, most of us) know how to act in society, we still need to have written law and someone to enforce it for us to 'act right'. The same applies for computer system users, managers and administrators. Putting policies in writing is a requirement for good security administration, and should not be considered optional.

- Identify needed policies - There are many policies and types of policies to choose. What you need to think about, though, is matching policies to risks you have identified. While you are making a list of the policies you need to reduce your risk, think about who will be signing these policies. Certain risks might be acceptable for one part of the business, but not another. In that case, you will need to think about levels of policy. For example, the Research and Development section might require much higher security against hackers than your marketing division. In that case, separate policies may need to be written. Keep in mind that unnecessary policies will weaken the effectiveness of all policies, so limit your efforts to the ones you need.

- Templates - When you are developing policies, you have two choices. You can develop policies from scratch, or you can find pre-written templates to start. I would certainly recommend using the later to start.

There are many choices for policy templates, from expensive to free. Start simple and develop them over time. An extremely comprehensive (but moderately expensive) source is George Jenkins' Information Systems Policies & Procedures Manual. I would recommend this for a very large organization that needs many policies fast. This could also be a good resource further down the road, as your policies begin to grow and become more comprehensive. However, for most security administrators just starting out, I would recommend some simpler (and free) templates available on the World Wide Web. An excellent place to start is the SANS Model Security Policy Project. This is a very good resource for any security administrator, novice or experienced. You will find lists of common policies, and can download and customize them for your organization. Some of the basic policies you should consider are:

- Acceptable Use Policy
- Anti-Virus Policy
- Information Security Policy
- Audit Policy
- Dial In/Remote Access Policy
- Ethical Use Policy

From these policies you can fairly quickly draft up policies to move to the next step. Remember, it is VERY IMPORTANT that policies are simple to understand and simple to apply. You might not be able to get as concise as the "Thou shalt not kill" in the Ten Commandments, but let brevity and clarity be your guidelines. If you need a lawyer to explain what the policy means, then you will almost surely have problems later. If you are not the best wordsmith in the world, write your ideas down and have someone who is a good writer re-work them for you.

- Management support - You must have management's full backing for all policies. This is very important. Remember, these are not your policies, but the organization's policies. You are just the 'expert' who drafts them for upper management. The more "upper" you can get to sign these, the better. Once you have the first draft of policies, try getting an informal review by the mid level management who would be most affected by the policy. Listen to their feedback and concerns and be prepared to explain, not argue, the intent and goals of each policy. It may go without saying, but getting buy-in at the middle management level is going to take some people skills. You are going to have to know your organization well enough to get the time and attention of the right people. Prepare to go to meetings, and present your case to them. If the final policies go forward to the head of the organization for signature, and the appropriate people have added "recommend approval" notes on it, you have a much higher chance of getting final approval. If at first you don't succeed, try, try again. Remember, this is a process and just getting one basic policy signed is a start, you can

(and should) grow from there. But, you do need something in writing from someone in authority in order to move forward.

- Publish and Enforce - Once you have a signed policy it will need to be published. Use the organization's established process for publishing policy, if such a process exists. Do not just let the policy sit in an archive where you can point to it later. Make sure the word gets out. You need to make a real effort to let everyone know that the policy exists, why it exists, and that it is supported by management. Enforcing some policies can be as simple as implementing firewall rule sets and password aging standards. Those are the easy ones to enforce. More difficult are the ones in which a user must be disciplined for a violation, or a new process must be inserted into an existing business practice. Enforcing these takes tact and some fortitude, and also a strict appearance of fairness. You must be seen to be abiding by the rules. A good security administrator must be viewed as looking out for the good of the organization and the policies you enforce should be viewed similarly.

Secure Systems

Now that you have done some of the less glamorous work, you have to take steps to secure your systems. Listed below are the technically challenging and necessary steps for security. These should end up as checklists so that you can keep up to date. I have included the following as general things you will have to do to secure your systems. Of course, your system may not include all of these, or may include some things not listed, but in general, the steps are the same.

- Basic Inventory and Priorities to Secure Systems - You can now start using your prioritized inventory of systems. Taking this information from the first steps in our process, you can identify which systems are the most important and where you need to concentrate your efforts. You secure the most important and vulnerable systems first and work your way down the list. Remember, time is also a resource, just like money, training, experience and personnel. Make sure your time is budgeted. As we proceed through the following steps, we will use some well accepted sources for our "step-by-step" process. Remember, 'step-by-step' means a checklist, a process that can be repeated over and over again. Developing it the first time is the hardest part.

- Virus Protection - Virus protection is probably the first and most important thing you can do to protect your systems. Of course, your priorities may vary, but typically virus protection is number one, and is a good place to start. There are many excellent virus protection vendors, such as Symantec, Sophos, McAfee, etc. These large vendors can provide an excellent product for desktops and servers as well as mail

content scanners. Before you buy, make sure to review your vulnerabilities. Viruses are typically introduced into systems through email, file sharing and floppies. By far the most common is via email, so you should protect any email coming into your system with a virus scanner. This will mean content scanning at your mail server. In addition, you cannot ignore the other methods of virus infection, so you should also have some kind of centrally managed virus protection on each desktop. Whichever product you chose, you will have to consider cost and methods of implementation, but if you are a beginner, something is better than nothing and simple is also a plus. Protect your system from viruses and you have reduced your risk considerably.

- Firewall/Router - I am lumping firewalls and routers together since they are choke points into your network, and need special attention. The devices themselves provide much of your network security, and there are many resources available to advise you how to secure them as well as vendor documentation. You need to remember that there are two forms of security for firewalls and routers. First, the device itself is providing security to the network, such as your firewall rule sets and router access-control lists. Second, there is the security of access to the device itself. A firewall or router that can be compromised is not trustworthy and should not be relied upon to provide the security to the network for which it is designed. Most firewalls and routers are provided with fairly secure operating systems, but you should ensure that the firewall or router is secure itself, before worrying about the rules it is applying to protect your network. It is beyond the scope of this paper to go into the intricacies of hardening operating systems and defining rule sets, but remember that defense in depth is a sound principle. Multiple layers of security help protect against configuration errors and new vulnerabilities, as well as giving the security administrator a little more time to react to threats as they become known.

- Unix Servers - There are some very basic steps you can take to secure a UNIX server, with variations depending on the flavor of UNIX involved. Again, it is beyond the scope of this paper to go into details, so I will discuss some good sources for documentation and “how-to” as well as review the basics. There are several (at least) good sources for UNIX checklists available on the web, such as Yale University’s Network Security Checklist for UNIX Workstations or, for Solaris, the YASSP ("Yet Another Solaris Security Package"). In addition, the Center for Internet Security has more detailed benchmarking tools for Solaris and Linux (as well as Windows 2000) available. These will detail the basic steps to secure a UNIX machine and enable you to keep track of progress as you improve security and how your vulnerability level will change as new threats and vulnerabilities emerge. Some of the basics for UNIX are keeping software patched, minimizing system services to

those absolutely needed, robust and secure logging, strict user access controls, maintaining regular backups and auditing the file system and file permissions. In addition, for both UNIX and Windows servers, consider a system integrity checker such as Tripwire to make sure your system has the integrity with which it was installed. This can be important at a later date when you suspect (or know) you have been compromised. Tripwire is available in both commercial and open source versions.

- Windows Servers - If you have Windows server products, such as NT, 2000, or 2003, you need to have the same sort of checklist that you have for UNIX systems. A very good first step for this are the Center for Internet Security benchmarking tools cited above. There are many other sources available to help secure Windows servers, not the least of which is Microsoft, which has gotten much better over the years at providing methods, tools and information to assist you in protecting their operating systems. The basics for securing Windows servers are essentially the same as UNIX servers, i.e. patching, logging, auditing, backups, user and user access management, etc. Do not forget, you need to document what you do and prepare a checklist in order to repeat the process at a later date. For both Windows and UNIX servers, a handy source to keep bookmarked is the SANS/FBI Top Twenty List of Vulnerabilities. This list is up to date and authoritative; it will give you a very good head start on eliminating the vulnerabilities with the highest risks.

- Desktop - Securing your network access points and servers is important, but so is securing the users' desktops. Users are probably also using the desktop to do things they shouldn't. How much do you secure the desktop? Since the insider threat is commonly accepted to be high, try to make sure your control of the desktop is appropriate to the threat. Making the desktop secure is a matter of keeping the vendor updates and patches under control (generally Microsoft). Think seriously about some way to standardize the desktop that the users see. Generally, group security policies for Windows are a very good option. However, if you have chaos on the desktop, and by that I mean users are allowed to control their own desktop, be prepared to work on this a lot. In the ongoing competition between 'operations' and 'security', you will find that this is the most difficult to deal with at the level of the individual user.

User Education

Now that you have done much preliminary work studying your systems, developing policies and securing your systems, you should have a good idea of

what you would like to do to educate users and management. Following are some guidelines you should use in your education plan.

- Education Plan - You need a plan to educate users and management as well as IT system personnel. Your plan should be in writing and have the approval of management. It should be presented very basically with some of the following steps.

- Security Awareness - For the users (which essentially means everyone) you should make sure that each user reads the policies and acknowledges understanding them. Require a signed form before any access is given and keep those signed forms on file. Keep them simple and make sure users are allowed to ask for clarification from their supervisors on the meaning of policy. Insert the user agreement and policy acknowledgement into the Human Resources Department's 'new-hire' orientation. If there is not a formal process for new-hires, try to insert the user agreement into the informal process. Make use of login banners wherever you can. Each and every time a user is reminded of security, it helps to ingrain security as part of your company's culture. Simple is better, and you can find sample login banners on the web. A good sample can be found at the University of Chicago, Network Security Center. You must also try to give periodic updates or reminders on security. Think about how your organization works, and try to find ways where you can personally make short presentations to captive audiences about security, for example, regular staff meetings. If you cannot do them in person, use email (sparingly) to send short notices on different topics of interest.

- Management threat briefings - In addition to educating users, you also need to make sure management receives periodic threat briefings. Try to make the briefings short and to the point, and do not be an alarmist. You have to tread the fine line between crying wolf and ignoring threats. Remember, your duty is to make sure management is aware of the risk they are taking in the realm of IT security.

- System Administrator Training - System or Network administrators, and IT personnel need more detailed briefings and training. Take the next step and look for training to attend, hands on, on-line or whatever you can get. There are many such courses available, such as the SANS courses. These might start with "Security Essentials", and moving on to the more advanced "Securing UNIX" or "Securing Windows". These courses cost time and money, but would be well worth putting on your budget and agenda, even if you do have to do them after you have gone through this process on your own. If you have a large IT staff then you should implement security briefings and training for them.

Many times IT personnel make decisions in order to 'make things work,' which isn't always what you wanted from a security point of view. Keeping them aware of security issues is critical.

Do it all again

Now you think you are all done. You can not rest on your laurels, but must get ready to do this on a regular basis**.** This means developing standard procedures that you (or someone else) can follow from now on.

- Checklist - Develop a checklist based on the process you just went through. If you can summarize what you did the first time, and keep a record of it, it is much easier to duplicate the next time around, when you get a new server, router, or system. Maintain your checklist and build on it over time.

- Build on work done - Build on your experience and dig deeper as needed. Remember that in the initial stages you had to budget your time and prioritize. You keep doing that, but now you should have some time to go back to those things you had to put lower on the priority list the first time around. Examining risk and lowering it is your goal.

- Schedule reviews - Plan a schedule (annually, quarterly, monthly, weekly) for reviewing your security posture. Different threats require different review schedules. For example, you may review your virus protection status weekly, but review your Audit Policy every two years. Depending on your resources, make sure that you do review and redo everything you did above with some regularity.

Conclusion

Security is a never ending process. If you thought you could reduce all your risk to nothing, and then sit back and enjoy it, you were wrong. The world is always changing and the threat is always changing. It is your job to keep up with the threats your company faces.

There are subjects not touched on in this paper that you may discover to be important. These might include intrusion detection, both network and host-based; vulnerability scanners such as Nessus, which can maintain a baseline for you; or incident response handling. Your job is also to keep management informed of the risk they are assuming in their business world. That is what makes you the Information Security Manager and it is your job to enjoy.

Resources

SANS Institute. SANS GIAC "Security Essentials Course." http://www.giac.org

Chapman, D Brent and Zwicky, Elizabeth D. Building Internet Firewalls. Sebastopol: O'Reilly, 1995.

Jenkins, George H. Information Systems Policies & Procedures Manual. Paramus, NJ. Prentice Hall. 2001.

Cheswick, William and Bellovin, Steven. Repelling the Wily Hacker. Reading, MA. Addison-Welsley.1994.

Editors: Linda Garrison and Martin Grand. "Cyberterrorism: An Evolving Concept". National Infrastructure Protection Center Highlights. 15 June 2001. http://www.nipc.gov/publications/highlights/2001/highlight-01-06.htm

SANS/FBI. "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus". 29 May 2003. http://www.sans.org/top20/

National Institutes of Standards and Technology-Computer Security Resource Center. "Automated Security Self-Evaluation Tool". http://csrc.nist.gov/asset

The Security Targeting and Analysis of Risks (STAR) Program. Virginia Technical Institute. http://security.vt.edu/playitsafe

Blank Business Impact Analysis/Risk Assessment. Virginia Technical Institute. http://security.vt.edu/playitsafe/riskanalysis/RA-Dept01-MST-Blk.doc

SANS Critical Vulnerability Analysis Archive. http://www.sans.org/newsletters/cva/index.php

Carnegie-Mellon Software Engineering Institute. CERT Coordination Center. http://www.cert.org/nav/index_red.html

SANS Security Policy Project. http://www.sans.org/resources/policies.

"Yet Another Solaris Security package". http://www.yassp.org

NESSUS. http://www.nessus.org

"Network Security Checklist for Unix Workstations". Yale University. http://www.yale.edu/its/security/new-index.html?http://www.yale.edu/its/security/Procedures/Securing/Unix

Tripwire. http://www.tripwire.com or http://www.tripwire.org

Center for Internet Security. http://www.cisecurity.org

Microsoft. How to Maintain Windows Security.
http://www.microsoft.com/windows/security/default.mspx

University of Chicago. Network Security Center.
http://security.uchicago.edu/docs/login_banners.shtml