Global Information Assurance Certification Paper

The Life Cycle of Security Administration

Beau Spafford

17 April 2001

Version 1.2c

Outline

Introduction
Know Your Job Description
Get Some Education
Organize Your Sources
Get an Assessment
Implement Changes
Conclusion
Sources

Introduction

"Does anyone know how to close a port?" I still find myself asking this question rhetorically. About six months ago, I was brought on as a Data Security Administrator. I thought, "Boy, this is really cool!" I am going to secure data, and wear a badge, and carry a gun, and tell lots of people to be secure. The only part of that prophesy is I tell employees constantly, "DO NOT open e-mail from someone you don't know, telling you to open a naked picture of your wife!"

Most every position I have held has had a life cycle: beginning, middle, and end. This position, despite my misconceptions, is far more encompassing than I ever could have imagined and it's life cycle evolves back to the beginning instead of the end. This paper is for everyone who, like me, is about to take on a freight train with a hockey helmet. This job is tough, not glamorous, and the only time someone in your organization actually knows your name is when "Anna Kornikova" has aced his or her computer.

Don't be overwhelmed! Nobody is expecting you to perform miracles or become a scapegoat, however, it will be your job to reduce the probability your organization does not become the target and or victim of malicious activity. And when it does become a target, your job will be to reduce the risk of damage and liability. Let's begin.

Know Your Job Description

I made the mistake of thinking I was still in a position where I would actually work on computers and troubleshoot and all of that cool stuff. Wrong! I used to still perk-up when someone called with an IS request. "I know what is wrong!" I would tell my technicians. That got old for them and I found myself not having time to do what I had to do. Your job description will help you focus on what you have to do first.

Your job description should outline your responsibilities and duties. You should keep this posted on your desk somewhere for easy reference. Whenever that phone rings at the next cubicle and you hear a technician struggling, look at your job description! You have a ton to do! Turn your CD player up and get to work. Take each bullet from your job description and analyze it. Determine how you will do this and when should it happen. If you have no idea, ASK! I have never been in a position where I knew everything. Not yet, at least. Get your manager to help you with managing your own position. This will do at least two things.

Firstly, you will have first-hand knowledge of what your manager expects from you. You will know how they want things done, by when, and probably give you some references on how to do it better. Also, it could be that your manager used to occupy your desk. He/she could have old policies, procedures, vendors, white papers, etc. of how to do your job. Secondly, you will empower your own manager, and you are immediately getting the proverbial "brown nose". But the trust that your manager will in turn give to you will be worth it.

You should also become familiar with the rest of your department's job descriptions. It is not that you would want to say, "that is not my job, that is Debbie's!" The purpose of knowing your job description and your staff's is that you can delegate responsibility to other people on your staff. For example; while it is in your job description to "ensure virus software is up to date" you would not actually be installing this on all of your organization's PC's. You would let your technician apply these patches or have your Network Administrator add a batch file into the login script.

Since you know who can do the specific duties that you are responsible for, you can allocate your time to other important stuff like writing policies and procedures, hardening firewalls, auditing log files, responding to Intrusion Detection alerts, and assessing new technologies.

Get Some Education

There is really a bunch to learn about this occupation. As technology evolves, so do the requirements of this position. There are several ways to stay abreast of all of the changes. You can do this by subscribing to listservs, extending your formal education, or becoming certified.

I currently find several subscriptions very useful. Not only do they e-mail weekly newsletters, but they periodically send out warnings or alerts. They offer articles on new technologies, new vulnerabilities, and upcoming events. Above all, they can be trusted as sources and they bring all of this to your desk. Some examples are www.itsecurity.com, www.symantec.com, www.mcafee.com, www.sans.org and www.techrepublic.com. If you visit these sights, they offer free subscriptions.

Most universities now offer online education for degree-seeking students. As a full-time professional, this is a must for me. Some do a weekend class per month and some are

strictly online. Either way, by putting some more initials on your business card inevitably increases your awareness of the need for security.

To me, seeking my certification has been the most demanding and rewarding way to increase my technical expertise. Not only am I improving my organization's infrastructure with every new trick I learn, but also the knowledge shared by the INFOSEC community is truly awesome. I think the best way to transition into your new position is to become immersed in it. Certification has done that for me. Whether you do it with SANS or CISSP, do it. You will begin to feel more comfortable with your position immediately.

Organize Your Sources

This portion is simple. Take every security website you visit and bookmark it. You will be back. Read books and store them in a library near your desk. Place all of your organization's hardware and software reference material in one place. Make a space in your office just for your magazine subscriptions.

I have found that every website I go to has sites linked into it that are more valuable than the next. I now organize my favorites into folders. I have organized my folders into "Certification", "Policies/Procedures", "Security Patches", "Virus", "Disaster Recovery", "Backups", "Network", and then "vendors". This helps me keep my hundreds of website sources organized where I will be able to reference them in the future.

I have read six books since December, and four have been related to my job. This is awesome stuff and the more you read the better you will be prepared. Nevertheless, do not forget where you read that one important line about how a hacker sniffs your network. Hacking Exposed is an awesome book and everyone in this industry should read it. Another book that I reference frequently is Information Security Policies Made Easy. Keep that book close by and book marked. Buy a bookshelf and keep reading!

When you are scanned, fingerprinted, sniffed, or hacked, you will need to know how to fix it. By keeping your hardware and software references handy and book marked will help you immensely. Being prepared will save you a crucial amount of time and perhaps will even prevent a hacker from accomplishing their intent.

Subscribe to magazines and read them front to back. There is a lot of techniques, to do's, and do not's in magazines. They will keep you abreast of what is new and helping our industry and what is old and hurting it. Some examples are "INFO SECURITY NEWS", "INFORMATION SECURITY", and "Internal Auditor". Moreover, your organization will probably pay for them and you can get the free alarm clock!

Get an Assessment

How would you determine your strengths and weaknesses, unbiased? Whom would you trust to give you an honest assessment of how bad or good your organization looks?

What would you ask them to assess? These questions should be answered prior to having someone scan, probe, or infiltrate your network.

No one, not even you should ever place an assessment tool on your network without approval. Despite your intent, you might be looking for a job if something bad happens and no one knows why. This is the first step in assessing your network and or security posture; get permission! The second step is determining who you would like to assess your organization. Many different companies and software solutions offer this. One idea is to have an industry-wide regulatory group or organization to conduct a review. They know your industry and they can compare you against your direct competition. They, hopefully, are impartial and can offer your organization a dedicated individual who assesses organizations in your industry as a full-time job. This brings experienced auditing to your organization, which is always beneficial.

If you do not receive approval for an external assessment, you probably already have one that you could use. Unix, NT 4.0 Server and Novell 5.x come with audit capabilities. Enable this. Once you enable auditing, configure it to log user logons, security changes, file access, and file deletions. Use netstat to determine services running on machines and look for ports that are listening. Use sysdiff and other default programs versus a commercial product like Tripwire. There are default tools within most platforms, which will enable you to perform simple tasks. These tools will allow you to create a baseline, backup your system files, and assess any inconsistent activities. At minimum, you can take this evidence to your manager to influence him to have a formal audit or to use a commercial product.

There are certain vulnerabilities that you need to protect your organization from. Edit policies and procedures to be current and applicable to your current architecture. Dedicate management to hire train and certified employees and keep them. Make sure your servers, programs, and virus signature software are all updated with the latest versions and patches. Ensure your network does not allow user's PCs to have modems running in conjunction with your LAN connection. Ensure third party vendors comply with policies regarding logging into your network.

A great place to start for a free tool that will assess your current hardware is The Center for Internet Security (www.cisecurity.org). They have a free tool called PatchWork. Run it and it will give you generic errors and fixes. Another way to assess your system is your vendor. They should have a page dedicated to patches, service packs, or even free upgrades. In addition, you can go to sites, which devote their services to determining and or reporting vendor weaknesses. One example is www.securitytracker.com.

Implement Changes

I walked into an office with a single report on the desk. This was an audit. The audit highlighted one hundred and thirty-seven recommendations that we should consider. This was an excellent introduction to what I would need to concentrate on for the next twelve months.

Everything needed to be changed, or so it seemed. We started with our policies. We could not really begin until we addressed what we expected of our employees. We changed our policies from being specific and narrow to being general and broad. We addressed WHAT needed to be done, instead of HOW to do it. We consolidated familiar policies and created committees of people who would complete the policy before going to lunch. We consulted with compliance officers, internal auditors, and federal regulatory documents. Above all we wanted to move set are employees up for success and not failure. Once we did all of the above, we submitted our policies to the Board of Directors, got their signatures, and employed them into policy by the

This assessment gave me another insight I had not considered much before hand: physical security. As broad as the potential breaches of security are, I was concentrating more on internal or Internet attacks. Physical security was so easy to fix, however, and really enhanced our overall strength. Access Control Devices have been implemented and are centrally controlled in a restricted data center. Doors are automatically locked and vendors are now processed through a reception area where they sign in. All employees are routed through specific doors now to access their work areas and any door that shuts, does. Before these changes, you simply needed to walk in a door, ride the elevator to the data center floor, knock on the door, and BAM, you are in. Not any more!

Next, we worked on our servers. The first thing I did was to establish what hardware we had. I created a network diagram both for our main office and for our remote locations. With this diagram I was able to visually place all servers and in turn note their configurations and specifications. Once I had everything on paper, I began to highlight the audit's recommendations on our map. Next to the highlighted recommendation I placed the fix to the problem. This visualization helped me tremendously. It gave me an opportunity not only to assess the weaknesses of our organization, but to improve upon the strengths as well.

Once we had our map detailed, we determined potential weaknesses and pinpointed plans on addressing them. We learned our firewall was not on the latest version and fixed it. We determined there were ports open on our servers that were not necessary and closed them. We discovered modems attached to servers 24/7 for no reason and we disconnected them. We enabled NAT to protect our public IP addresses. We revised our disaster recovery plan and then tested it. We implemented daily incremental backups and weekly full backups. We outlined separation of duties for the IS Department and encouraged cross training. We scheduled classes for the staff and supported certifications. We audited our vendors and mandated from them certain criteria, which we hold to be critical for data security. We enforce policies and test periodically to ensure compliance. We initiated a C-SIRT and are shooting for 100% certification on that team. We believe in defense in depth and are implementing a VPN and learning more about honey-pots. We created a library for our software and licenses and keep them under lock and key.

Conclusion

All of these specific actions supported not only the audit recommendations but our policies as well, which brings us full circle to our job description. Re-evaluate your job description and your organization. Once you have assessed your organization, see what can be done to improve the work cycle. Implement changes you feel would benefit the organization as a whole. Streamline the workflow of your staff and upper management. Automate functions that you have done manually in the past. Investigate what other organizations are doing and determine if what they are doing is better. If not, share with them what you are doing.

This job has no end. It is kind of like being a lawn maintenance guy in the tropics. There is no break! Keep improving and keep testing.

Sources

1. Hacking Exposed, Network Security Secrets & Solutions, McClure, Scambray, Kurtz, Osborne/McGraw-Hill, Berkeley, CA, 1999.
2. Information Security Policies Made Easy, Charles Cresson Wood, Version 7, licensed.
3. "INFO SECURITY NEWS", Volume 12, No. 4, pp 36-38.
4. www.securitytracker.com
5. www.microsoft.com
6. www.cert.org
7. www.cisecurity.org