Global Information Assurance Certification Paper

The New Government Information Assurance Officer
Hank N. Williams
GSEC 1.4b, Option 2
May 28, 2003

Abstract

Taking over as the new Information Assurance Officer at a Department of Defense (DoD) organization proved to be quite a challenge. The position had not been effectively filled for over two years. The organization was small but full of warfighters who were only interested in getting the job done. Information Assurance was considered a force detractor, not a force multiplier.

Policies and systems documentation were out of date and inadequate. The training program was virtually none existent. It was up to me to bring the command back into compliance with numerous government regulations and prove that Information Assurance could be accomplished without detracting from the mission. This is the story of the situation I found, the challenges I faced, and how I overcame them.

In the Beginning

When I arrived at my new job I received a short brief from my boss in which I was told that he depended on me to determine where the command stood in its security posture and he wanted to know how I planned to "put things right". I was also informed that one of my first priorities would be to prepare the necessary system accreditation documentation for our proposed migration to Windows 2000. I was then shown my desk and to all the files of my predecessor, who had departed over two years earlier.

I did not do much the first month or so except for some small, urgent items. Mostly, I walked around the facility and talked to different individuals and observed how people went about doing their jobs. Although I had not worked here before, I did know some of the current employees. One of the senior system administrators was a good friend and another friend worked in a different area. I talked to both of them extensively to get a feel for the security posture from both a system administrator's point of view and that of a general user. I also talked with others whom I had not known previously. I talked to both managers and lower level employees. I talked with our military staff and with the civilians, of which we had about a 50/50 split.

The command maintained three separate LANs, each one a different security domain: Top Secret, Secret and Unclassified. Each domain was physically separated from each other and the classified domains had their own hardware encryption devices. The three networks had no physical or logical interconnection. Although a domain might be classified Top Secret, the data

stored on the domain could be classified anywhere from Unclassified to Top Secret. The same held true for the Secret domain. Of course, the Unclassified domain held only unclassified data.

At the end of my first month I came up with a list of 5 major items that most needed attention: The Major System Upgrade, Security Policy, Security Awareness, Security Compliance, and Configuration management.

For readability's sake, I will discuss the before, during, and after sections item by item.

Major System Upgrade

When I arrived at the command, Windows NT was the current operating system in use. For multiple reasons, the command had decided to upgrade to Windows 2000 on both workstations and servers. The upgrade to the production systems, however, could not be performed until the Certification and Accreditation process had been performed.

The Department of Defense, being the large government agency that it is, has a very large, complex, and cumbersome process for accrediting information networks. This process is called the Defense Information Technology Security Certification and Accreditation Process, more commonly known by its acronym, DITSCAP.

DITSCAP comprises four phases: Definition, Verification, Validation, and Post-accreditation. The final result of the DITSCAP process is the System Security Authorization Agreement (SSAA).

In phase one, the SSAA is developed and security requirements are identified. First, I talked to the senior system administrators to determine our system architecture. Once I had a full understanding of how our network was designed and the necessary user requirements, I began researching the security requirements. I researched the applicable Security Requirements Traceability Matrix (another voluminous DoD manual) to begin my security risk assessment. This is a formalized DoD procedure to determine the necessary security measures based upon the sensitivity of the information and the existing threat. The results of the risk assessment guided me in determining the proper security measures to apply to the network.

Phase two began on the test LAN. First, we took the results of phase one and along with the recommendations in the NSA Windows 2000 guides configured the Windows 2000 workstations and servers in the test LAN. We then used a set of testing procedures developed by the Navy Information Security Office to test that the systems behaved as expected. Any deviations we noted were annotated in a Test Evaluation Report and corrective actions were determined and applied.

In Phase 3 the Navy Information Security Office visited our location and performed their own set of testing procedures to validate everything we had done on our test LAN. Once that had been completed to their satisfaction, we performed the migration on the production LAN. The Navy Information Security Office then re-validated everything on the production LAN and issued our three-year accreditation.

Phase 4 is ongoing during the three-year period of the accreditation. Changes to the baseline are documented and periodic testing of the LAN is performed to ensure that it continues to meet the required security posture.

Security Policy

The command's security policy was last updated over 4 years ago. All in all it was not a bad policy, but it had not kept up with the times and left several areas uncovered.

One of the problems was the fact that individuals had access to the 3.5" floppy drive on their computer. Disks were basically uncontrolled coming into the command and several viruses had been introduced in recent months. To bring this under control, the command policy instruction was changed in the following manner.

First, floppy drives at the user's workstation were disabled using a domain policy. Secondly, anyone who desired to bring in any type of removable media was required to bring it to the Information Assurance office for virus scanning and transfer to the appropriate LAN. The IA staff then conducted a virus scan on a stand-alone workstation and transferred the data as needed.

The other major concern was the uncontrolled transfer of information between security domains, also known as cross-domain transfers.

On an almost daily basis there was a need to transfer data files from one security domain to another. For obvious reasons there was no real concern when transferring from a lower domain to a higher domain. Our concern was a possible compromise of classified data in a transfer from higher domains to lower domains.

When I arrived cross-domain transfers were not covered in the security policy instruction. After researching the issue and looking for regulatory guidance, a written policy was added to the security policy instruction. The policy fell into three main sections: avoidance, verification, and procedure.

In avoidance, I outlined different techniques individuals could use to try to avoid having a cross-domain transfer. The easiest of course was to create or find the data on the target domain.

Verification included requiring that documents to be transferred be created as new documents. Sanitizing a Top Secret document to bring it to Secret creates the risk that something will be missed. The primary tenet of verification is that at least two individuals, ***who are cognizant of the data***, are required to certify that the data does not exceed the classification of the target domain.

Once the data has been verified, it is passed to my assitant or myself for the actual procedure. We use a set of tools developed by the Air Force to perform the actual transfer. These tools first search the data and compare it with a dirty word list for possible indications that the data was not properly sanitized. Then a special file copy routine ensures that only the data in the actual file are copied and that any excess bits between the EOF marker and the end of the sector are not copied. The last tool ensures that the transfer medium is clear of any data other than that which is desired for the transferred. The data is then transferred via sneaker net.

Security Awareness

When I arrived at the command, the Security Awareness program was rudimentary at best. It consisted of a few slides during the command's yearly physical security training given each December.

In November I began researching items for the new information security briefing. First, I looked at the relevant DoD regulations. Unfortunately, they were rather vague as to the required content of the training, stating only that annual training was required. I also did some Internet searches at different sites such as www.sans.org and infosec.navy.mil. While I did find some good info at these sites, I did not find the all-inclusive, ready to go, user-training presentation that I had hoped for. This meant that I was going to actually have to knuckle down and develop my own training program.

After some research into past problems at the command and talks with some of the other IT department heads, I developed a three-part training program: Initial user training, annual refresher training and a monthly IA newsletter e-mail.

The initial training is for newly assigned personnel. The information Assurance office is one of the checks on the inprocessing checklists given to each person when they arrive. New arrivals are required to view a PowerPoint presentation that briefs them on all of the command IA policies. Once they have viewed the brief they are asked to sign a user agreement whereby they formally acknowledge and agree that they have been properly trained in the policies and agree to abide by them. Our legal counsel approved this agreement and it gives

us grounds for legal enforcement, if necessary. Once all of this is done we process their new computer account request form. Having the form originate in our office ensures that all new users receive the brief and do not skip us during their inprocessing.

The main focus of our IA awareness program is during the yearly training given the month of December. The training is usually given in about four different sessions to ensure that everyone has an opportunity to attend. We also take attendance to verify that all members of the command have received the mandatory training.

The training focuses on four areas: Security Practices, Malicious Code, Software, and Cross-Domain Transfers.

In the Security Practices section I discuss passwords, reminding everyone that passwords must be a minimum of eight characters in length and consist of both upper and lower case letters and at least one number and special character. I also remind them that they must screen lock their system whenever they are away from their desk. This helps to prevent unauthorized access to system resources. Users are also reminded that they must power their systems down at the end of the day.

The malicious code section gives users a basic understanding of what is malicious code and the various forms in which it appears. We discuss various symptoms that may be an indication that a computer is infected with a virus. They are also trained on the proper procedures to follow should they suspect that they have received a virus.

In the software section, we discuss the proper procedures for acquiring new software. It is emphasized to them that they must never download executables or other program type software without approval from the IA office.

In the cross-domain transfer section I explain the proper procedures for requesting and performing cross-domain transfers.

In addition to these formal training requirements, about once a month I send out an e-mail on current IA issues. I use the www.sans.org web site and some of the different DoD IA web sites for content and pertinent information. I did not list these web sites as most of them are on the classified LAN and not publicly accessible.

Security Compliance

Security compliance within the DoD is divided into two parts; initial configuration and patching newly discovered vulnerabilities.

The Defense Information Systems Agency (DISA) in conjunction with the National Security Agency (NSA) publishes Security Technical Information Guides (STIGs) on how to securely set up hardware devices from individual computer workstations to servers to network devices such as routers and firewalls. In addition, DISA also publishes Security Readiness Review (SRR) checklists for each of these systems. Automated scripts are available for Windows NT and 2000 workstations and servers. Theses checklists and scripts are updated once a quarter to ensure that they are current with the latest patches.

Combating newly discovered vulnerabilities is the responsibility of the Joint Task Force-Computer Network Operations (JTF-CNO), a division of DISA. JTF-CNO closely monitors private industry and liaises with major software producers such as Microsoft and Sun Microsystems. As new vulnerabilities are discovered, they are evaluated by JTF-CNO. If the vulnerability is deemed a threat, JTF-CNO uses a process called Information Assurance Vulnerability Management to publish the vulnerability to the DoD. Vulnerabilities are classified as Information Assurance Vulnerability Alerts (IAVA), Information Assurance Vulnerability Bulletins (IAVB) or Information Assurance Vulnerability Technical Advisories (IAVT). IAVAs are for severe risk vulnerabilities, IAVBs are for medium risk vulnerabilities and IAVTs are for low risk vulnerabilities.

When I arrived at the command I talked to the system administrators to find out if the systems had been set up originally as required by DISA and if patches had been applied as necessary under the IAVM process. I was told that when the systems were installed a couple of years ago, they had used the guidance currently in effect to set the security setting on the computers. They were not aware of the router guidance and the individual responsible for the router had set it according to how he felt is was best secured.

The first thing I did was to run the SRR automated scripts on the Windows NT computers and perform the manual checklists in those cases where automated scripts were not available. The results on the computers were not as bad as I had feared. Most of the security settings had been done. What were lacking were the patches for newly found vulnerabilities. These patches had been applied haphazardly. Some computers had some patches and other computers had different patches. There was no documentation as to which patches had been applied to which computer.

The router, however, was another story. The network administrator had basically set up the router as allow by default and deny by exception. This is exactly opposite to DoD policy, which is deny by default and allow by exception.

To fix the current problems, I had the network administrator redo the settings on the routers in accordance with the STIG published by DISA. I also researched the different patches required on the computers that had not been applied and ensured that our system administrators got all of these fixed.

I worked with our database administrators to build a simple Microsoft Access database that I could use to track IAVM items. This database tracked the different items by their type, gave a short description of the vulnerability, whether or not they were applicable to us, the due date and if we had complied. In addition the database tracked by device, which patch was installed on which device, who had installed it and the date it was installed.

This entire process took us about six months to complete, but I am now confident that our systems are in compliance with DoD guidelines and directives regarding information security. We also now do a much better job of fixing new vulnerabilities as quickly as possible.

Configuration Management

For the last several years, configuration management basically did not exist. If a section of the command wanted a new piece of software or hardware, they would submit a purchase request and the computer systems department head would either approve or disapprove it. Of course this is a very simplistic view of the process, but my point is that security was very rarely, if ever, a consideration in the acquisition process.

DoD regulations required that all changes to the information systems baseline be approved through the auspices of a documented configuration change process. The regulations gave us a lot of leeway on exactly how we instituted this configuration management process.

In going through the files of my predecessor I found an instruction on configuration management that was about ten years old. Apparently, the command had had a configuration management process at one time, but it had gone by the wayside before my arrival.

I took this plan, blew off the dust, and used it as a starting point for our new configuration management plan. What we created was a Configuration Control Board (CCB) that would meet and approve or disapprove of all requested changes to our baseline. Members of the board included the Board President, Computer Systems Department Head, Senior System Administrator of each network, the Database Division head, myself, and any other pertinent individual from the command. The chief of our Systems Architecture Division served as the board president.

Requests for changes to the baseline were submitted to the board president on a Configuration Change Request Form. This form asked for the requested change, the name and department of the requestor, the justification for the change, the affected system(s), and the estimated cost.

Upon receipt of the form the board president classified the change as either a Major or a Minor change. Major changes consisted of software application purchases, OS purchases or new network hardware. Minor changes could be installation of previously evaluated and approved software on a new user terminal or purchase of new monitors.

Minor changes were approved directly by the board president. Copies of the approved form were given back to the requestor and to myself for filing in the appropriate system accreditation package.

Major changes were brought before the monthly Configuration Change Board. If the request was time sensitive, then an ad hoc board was held. The board could either approve the change as submitted, disapprove the change, request further testing in the test network or request further justification or information from the requestor.

This new process is now in place and assures that all changes to the different systems are well documented and well thought out. We now know what we have, where we have it and why we have it.

Conclusion:

It has now been about one year since I took over as the information Assurance Officer and I am glad to say that our security posture is much better now than before I started. While we have come a long way, the job is far from over.

Now that we have completed the migration of the Top Secret domain to Windows 2000, it is time to do it all over again for the other two domains. Fortunately, much of the work previously done will apply to the new accreditation packages.

I recently attended the annual IA conference for our region and came away from it with various impressions. One was that, over all, I truly feel that my command is one of the better ones with respect to Information Assurance. Our people now realize that Information Assurance is important and must be a factor in our daily operations. Fortunately, they have also learned that Information Assurance is not the big, bad dragon they feared it was. Through cooperation, proper planning, and coordination solutions to IT problems can be implemented that provide for proper information security and do not interfere with the mission.

The other was that there is still so much to learn about information assurance. One of the future initiatives is towards securing information on an individual object basis rather than a network centric basis. This will allow us to move away from separated security domains and create a multi-level security domain, thereby minimizing the need for multiple computers per user. User identification will be accomplished through the use of PKI tokens, Common Access Cards with

card readers or possibly by Biometrics. Information Assurance is guaranteed to keep me busy.

References

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

National Security Agency, Security Recommendation Guides
http://www.nsa.gov/snac/win2k/index.html

Navy Information Assurance
https://infosec.navy.mil/ps/?t=main/main.tag&bc=main/bc_main.html

Department of Defense Directive 8500.1, Oct. 24, 2002, Information Assurance

Department of Defense Directive 8500.1, Feb. 6, 2003, Information Assurance (IA) Implementation