Global Information Assurance Certification Paper

Documentation: Essential to "Defense in Depth"

Michael Kirby

GSEC Practical Assignment Version 1.3

Introduction:

Several documents have caused the federal government to revisit the way they do business in regards to security. They include:

1. The ongoing lawsuit, "Cobell vs. Norton" – This case (http://www.indiantrust.com/clips.cfm?news_id=158) resulted in the shutdown of the Department of Interior's network to any outside resources.

2. The Office of Management and Budgets "FY2001 Report to Congress on Federal Government Information Security Reform" – This report http://www.whitehouse.gov/omb/pubpress/2002-05.html, found many agencies lacking in security concerns.

The fallout of Cobell vs. Norton opened some eyes to DOI's dependency on the Internet and email to conduct everyday business. Many problems developed because of this shutdown: no email caused us to rely on fax, snail mail and phone, no faxes could be sent or received via computers because all modems were unplugged, no research could be conducted via the internet. This resulted in the use of long distance and snail mail and caused long delays in correspondence.

With so many agencies showing poor results in the "FY2001 Report to Congress on Federal Government Information Security Reform" many at the grassroots level will be writing many reports or justifying networks, servers and resources.

Utilizing several Government documents as guides and other sites, preparation can begin now, without the last minute rush that results in the senior management wanting reports "yesterday". This document will show the different areas system administrators can catalog to prepare the agencies for the reports of tomorrow.

Why Document:

As system administrators are aware, documentation is a necessary part of the job. Unfortunately with all the talk of documentation, very little in the way of guidance on this matter is available. In everyday work, documentation sometimes falls by the wayside due to more pressing matters.

Documentation is part of "Defense in Depth". It's presence is invaluable when the network or systems are attacked and when the system administrator is under pressure to either stop an attack or remedy the problems in the wake of an attack.

As stated above with the law suit, “Cobell vs. Norton”, local system administrators must be able to justify the networks, servers, software and connections just to prove to the court that accessing outside resources will not cause damage to internal information. Because system administrators are a transient group, moving from one employment to another in order to advance, the need for documentation is very apparent. Moving into a new job, the need for documentation to review and learn the networks, servers, software and connections is a necessity.

What to Document?

The following list includes the basic areas necessary to be documented. There are many more areas that can be documented, but this list will be the start, and it can be expanded as necessary.

Areas to document:

Systems

Networks and connections

Server hardware

Operating systems

Software

Physical access

Intrusion detection

Security policies

Access

Internet connections

Intranet servers

Internet servers

Contingency planning

Basics of areas to document:

Systems

DOJ: "Systems Development Life Cycle Guidance Document." DOJ / IRM / Appendix C-9. March 2000.
URL: http://www.usdoj.gov/jmd/irm/lifecycle/apdxc9.htm

Systems themselves are the hardest to document. Fortunately at the level most system administrators are working (ie: at the Branch/Area level), this is not a necessary requirement. What is required is documentation of what systems used (financial, inventory, personnel etc.) and where they are located, including contact numbers to call. Most of these systems will either be developed at corporate HQ or be off-the-shelf software. If these are off-the-shelf software, keeping track of its security requirements is essential.

If you are required to document a system, NASA has a great report on documenting systems at:

NASA: CHAPTER 5: Information Technology Security Planning
URL: http://www.grc.nasa.gov/WWW/Directives/2810.1-Chap5.html

This report shows how to integrate security from inception of a software project to its retirement. Following these guidelines, you can keep your documentation correct and current.

Key Items to document:

1. Systems
2. Location (s)
3. Contact numbers
4. Security requirements

Networks and connections

NIST: SP 800-13 Telecommunications Security Guidelines for Telecommunications Management Network,
October 1995
URL: http://csrc.nist.gov/publications/nistpubs/index.html

Networks and connections require the most extensive documentation. The best way to document these is to create diagrams with connections. A picture is worth a thousand words.

In creating the diagram, utilize lines to show your connections, connection speeds, media and any redundancy. Be sure to show all hardware including routers, switches, bridges and hubs, etc. All hardware should show location, model and serial numbers. In tables to go along with the diagram, you should show IP addresses, TFTP file locations, and types of connections. You should document all configurations as well as any SNMP points.

You should also document the topology types as well as all network operating systems in use. Document locations of wire closets as well as what kind of physical access restrictions exist.

Key Items to document:

Diagram with:

1. Connections
2. Connection speeds
3. Media
4. Hardware
5. Locations
6. Model
7. Serial numbers
8. IP addresses
9. TFTP file locations
10. Configurations
11. SNMP
12. Network operating systems
13. Topology
14. Wire closets
15. Physical security

Server Hardware

NIST: SP 800-12 An Introduction to Computer Security: The NIST Handbook, October 1995
URL: http://csrc.nist.gov/publications/nistpubs/index.html

As any good system administrator/security specialist should know, becoming intimate with your servers is a necessity. Some basic things to document regarding servers are the models, serial number and configurations, as well as the location and physical access to the servers. Knowing your backups and their schedule as well as off site storage can become handy in the event of a human or natural disaster or an attack. The location of audit files (as well as their authenticity) is an ace in the hole when you are trying to stop or audit an attack. Don't forget the OS, NOS or such things as what services are running.

Knowing some of these items such as model and serial number, can also come in handy if a physical theft occurs.

Key Items to document:

1. Model
2. Serial number
3. Configuration
4. Location
5. Physical access
6. Backups
7. Operating systems
8. Network operating systems
9. Services running on server
10. Audit file locations

Operating Systems

NIST: System Administration Guidance for Windows 2000 professional
URL: http://csrc.nist.gov/itsec/guidance_W2Kpro.html

NIST: Operating System Security: Adding To The Arsenal Of Security Techniques
URL: http://www.itl.nist.gov/lab/bulletns/dec99.htm

The operating systems that are utilized for your workstations, servers etc. are the basis from which almost all attacks are sprung. Knowing what operating systems are in use, what revision they are, how security is configured on them and what services are running on them is imperative. Knowing your operating systems is almost as good as

knowing your enemy (hackers). Since it is hard to know your hackers, knowing your operating systems is the next best thing.

Key Items to document:

1. Operating systems in use
2. Revision
3. Security configuration
4. Services running

Software

NIST: SP 800-23 Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products,
August 2000
URL: http://csrc.nist.gov/publications/nistpubs/index.html

NIST: SP 800-4 Computer Considerations in Federal Procurements: A Guide for Procurement initiators, Contracting Officers and Computer Security Officials
March 1992
URL: http://csrc.nist.gov/publications/nistpubs/index.html

DOJ: "Systems Development Life Cycle Guidance Document." DOJ / IRM / Appendix C-9. March 2000.
URL: http://www.usdoj.gov/jmd/irm/lifecycle/apdxc9.htm

NASA: CHAPTER 5: Information Technology Security Planning
URL: http://www.grc.nasa.gov/WWW/Directives/2810.1-Chap5.html

What software are users running? What standard office software are they using? Viruses attack different software with varying results. If you are using Microsoft Outlook for an email client you are prone to many viruses, whereas someone using Lotus Notes has less attention from the virus programmers.

Do you know what services are being used? A service such as gnutella, opens tunnels hackers can exploit and should be monitored more closely.

You have to be a system analyst during this part of your investigation. Interview your users, know their habits, needs and limitations. Many companies have policies relating to the use of gnutella, streaming video and audio, etc. These activities alone during a time of national interest (ie: Super Bowl) can cause major network bottlenecks that can appear as an attack.

In my small hometown, recently the High School Girl's volleyball team was in the state finals. Of course an internet radio station was broadcasting the game, and the local radio station wasn't. We noticed a network slowdown. In analyzing the traffic we figured out that several people were streaming the audio over the network to their workstations.

Key Items to document:

1. Software used
2. Office software used
3. Revision
4. Email
5. Services (Gnutella)
6. Interview your users

Virus Protection

NIST: SP 800-5 A Guide to the Selection of Anti-Virus Tools and Techniques December 1982
URL: http://csrc.nist.gov/publications/nistpubs/index.html

Virus protection is one of the main lines of defense. It should be installed on every desktop and on servers too. Though documentation is minimal here, it should not be forgotten. Keep track of which vendor(s) you are using, whether it is individual or an enterprise edition, how updates are obtained and how often as well as contract renewal dates. Keeping track of which computers do not have current virus protection due to any reason is imperative.

Key Items to document:

1. Vendors
2. Individual or enterprise
3. Updates
4. Contract renewal
5. Computers unprotected

Physical Access

NIST: Guidelines for ADP Physical Security and Risk Management
URL: http://csrc.nist.gov/publications/fips/fips31/fips31.pdf

Physical access is sometimes overlooked as a means of egress. Whether it be the actual physical theft of a server, or access to wiring closets with routers, switches, hubs etc. not in the primary corporate HQ, knowing your physical access can be a great help in deterring hackers, inside vandalism and access.

Knowing what locks are installed, whether alarms are installed, and who has access to this space is knowledge that can be used to determine intruders.
It has been stated that up to 70% of network problems and data theft are caused by insiders in the company.

Key Items to document:

1. Access limitations
2. Locks
3. Alarms
4. Who has access

Intrusion Detection

NIST: Acquiring And Deploying Intrusion Detection Systems
URL: http://www.itl.nist.gov/lab/bulletns/nov99.htm

NIST: Guidelines on Firewalls and Firewall Policy
URL: http://www.itl.nist.gov/lab/bulletns/bltnjan02.pdf

NIST: SP 800-31 Intrusion Detection Systems (IDS)
November 2001
URL: http://csrc.nist.gov/publications/nistpubs/index.html

There are many types of Intrusion Detection systems. They can be host-based, network-based, audit files, firewalls, as well as honeypots, etc.

If your intrusion detection system installed is host-based, document what servers they are located on and what kind of intrusion detection is installed. Does it monitor audit files? If so which files? Does it monitor key files? Again which ones?

Network-based intrusion detection requires knowing which segment of the network the device is on. Where are you monitoring? What kind of traffic are you monitoring?

With audit files, where are they located? What are you monitoring with your audit files? Do you have a third party software that monitors your audit files?

Firewalls are key components. Where they are located on your network is very important. What are your access lists? What services are you passing? Keeping the configuration documented is imperative.

Do you have any honeypots? Where are they located on your network? What is the IP addresses and how are you monitoring them?

Key Items to document:

1. Host, network based or both
2. Location
3. Which files does it monitor (audit or key files)
4. Which segment is network based detection located
5. Where are you monitoring
6. What kind of traffic
7. Audit file locations
8. Third party software
9. Firewall location (physical and network location)
10. Access lists
11. Services being passed
12. Configuration
13. Honeypots location (physical and network location)
14. IP addresses
15. Monitoring

Security Plans and Policies

NIST: SP 800-18 Guide for Developing Security Plans for Information Technology Systems
December 1998
URL: http://csrc.nist.gov/publications/nistpubs/index.html

NIST: Information Security Policies For Changing Information Technology Environments
June 1996
URL: http://www.itl.nist.gov/lab/bulletns/archives/liz

Setting security plans, policies and enforcement of same is one of the primary items that will have an impact on your network and servers. Though security plans and policies are usually done at the corporate level, you can also shore up any holes at your area. This involves local management, but will pay off if the holes are tightened.

The documentation of security plans and policies should include all upper management guidance, what access is available, the type of training needed for a user to access the network and what level of password strength is required.

Another item of documentation needed is the penalties involved for infractions against the policies set forth.

You will need to make sure all policies include documentation regarding yourself and your auditing of the network, your ability to run security auditing, etc. This will cover you and your activities and should be signed by upper management.

Key Items to document:

1. All upper management guidance
2. Access available
3. Training needed
4. Level of password strength
5. Penalties
6. Policies regarding yourself and auditing of the network

Access

NIST: SP 800-12 An Introduction to Computer Security: The NIST Handbook, October 1995
URL: http://csrc.nist.gov/publications/nistpubs/index.html

Documentation of who may have access to the network is imperative. This includes not only those who currently have access, but also those who in the past have had access.

Also document who may have physical access to equipment, servers, network devices etc. An ounce of prevention is worth a pound of cure!

Remote access to WAN/LAN should also be documented especially in the area of VPNs and access to network devices via telnet. What services are you running on your routers, servers, and firewalls that will allow access to your network from outside?

Key Items to document:

1. Remote access to devices
2. Physical access to devices
3. VPN's
4. Remote access to network
5. Services running on routers, servers that allow access to outside sources

IP Addresses

NIST: SP 800-12 An Introduction to Computer Security: The NIST Handbook, October 1995
URL: http://csrc.nist.gov/publications/nistpubs/index.html

Within the IP realm, IP addresses range must be known, which ones are static and which are dynamic, which ones pertain to servers, and networking devices.

Also document all the subnetting done with the individual LANs deployed, as well as what the DHCP servers are if utilizing DHCP.

Another item worthy of note in the IP world is knowing the IPs of the gateways, DNS servers, and major network points. These can be very useful in testing networks.

Key Items to document:

1. Range of IP addresses
2. Static and dynamic
3. IP of servers and networking devices
4. Subnetting
5. DHCP and proxy servers
6. IP of the gateways, DNS servers, and major network points

Internet and outside Connections

NIST: SP 800-12 An Introduction to Computer Security: The NIST Handbook, October 1995
URL: http://csrc.nist.gov/publications/nistpubs/index.html

What are the connections to the outside world? What are the settings for browsers? Encryption levels for browsers? Within Internet Connections, what is allowed in and out? What ports are open? Who has access? Is there a firewall present? What is its access list?

Documentation is necessary whenever there is a modem setup to answer, whether it be on a server as a RAS connection, hooked to a Cisco router, or even on a desktop PC for a person dialing in to access their computer remotely. All these act as security holes and should be documented and setup correctly.

Key Items to document:
1. Connections
2. Browser settings
3. Encryption settings
4. Ports open
5. Access
6. Firewall
7. Access list
8. Modems setup to answer

Intranet Servers

NIST: SP 800-44, Guidelines on Securing Public Web Servers
URL: http://csrc.nist.gov/publications/drafts/PP-SecuringWebServers-RFC.pdf

Many companies today have intranet servers. These are usually served by IIS or Apache software. It has been stated "Having IIS setup is like having a screen door on a submarine"

Documentation of the setups of the intranet servers is necessary. Documentation of the revision levels and patches applied is also necessary.

Key Items to document:

1. Web server software
2. Setup
3. Revision
4. Patches

Internet Servers

NIST: SP 800-44, Guidelines on Securing Public Web Servers
URL: http://csrc.nist.gov/publications/drafts/PP-SecuringWebServers-RFC.pdf

Internet servers are a lot like intranet servers, except they are on the front lines and very vulnerable to attack from outside forces. In addition to the documentation stated above for intranet servers, also heavily document their location in regards to the network.

Key Items to document:

1. Web server software
2. Setup
3. Revision
4. Patches
5. Location in regards to network

Contingency Planning

NIST: Contingency Planning Guide for Information Technology Systems
URL: http://csrc.nist.gov/publications/drafts/ITcontingency-planning-guideline.pdf

FIPS 87 Guidelines for ADP Contingency Planning
March 1981
URL: http://csrc.nist.gov/publications/fips/fips87/fips87.pdf

Enough can not be said about documenting your contingency plans! When everything has broken, the creek is rising and lightening storms are shutting down power is not the time to be figuring out what you should be doing to keep your network or internet server running.

If you have documented correctly, you should be able to just follow the directions you have set down in more peaceful times and restore the network online.

Of course a lot of contingency planning is based on documentation of the above in all areas. In addition to this, you have to look at alternative ways to keep your Servers/networks running.

Being involved in the Y2K efforts of 1999, I find that a lot of the same contingency plans put into place for natural and Y2K disasters relate to the same for security planning.

Contingency planning is very specialized to your area and any attempt to show you how to document it would be a folly. Leaving you with….document document document.

Conclusion

In conclusion, if the above documentation is done, any time that you have security breaches, incidents or even court cases, you can answer questions quickly and efficiently. This type of documentation comes in handy when all heck is breaking loose and you are torn a million ways as your network is down and under attack or even when your email is not being transferred and the Head Honcho is hoping for an email from the President of United States.

This kind of documentation will also help those who follow in your footsteps to learn the network, servers, connections etc. They will be eternally grateful (well at least thankful). Though this kind of documentation needs to be secured in a good location, accessible to those who need it, but out of the hands of John Q. Public. Giving a hacker this kind of documentation is like letting a kid loose in a candy store.

Bibliography

Indian Trust: lawsuit, “Cobell vs. Norton”
URL: http://www.indiantrust.com/clips.cfm?news_id=158

The Office of Management and Budgets “FY2001 Report to Congress on Federal Government Information Security Reform”
URL: http://www.whitehouse.gov/omb/pubpress/2002-05.html

NASA: CHAPTER 5: Information Technology Security Planning
URL: http://www.grc.nasa.gov/WWW/Directives/2810.1-Chap5.html

DOJ. "Systems Development Life Cycle Guidance Document." DOJ / IRM / Appendix C-9. March 2000.
URL: http://www.usdoj.gov/jmd/irm/lifecycle/apdxc9.htm

NASA: CHAPTER 5: Information Technology Security Planning
URL: http://www.grc.nasa.gov/WWW/Directives/2810.1-Chap5.html

NIST: SP 800-13 Telecommunications Security Guidelines for Telecommunications Management Network,
October 1995
URL: http://csrc.nist.gov/publications/nistpubs/index.html

NIST: SP 800-12 An Introduction to Computer Security: The NIST Handbook,
October 1995
URL: http://csrc.nist.gov/publications/nistpubs/index.html

NIST: Operating System Security: Adding To The Arsenal Of Security Techniques
URL: http://www.itl.nist.gov/lab/bulletns/dec99.htm

NIST: SP 800-23 Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products,
August 2000
URL: http://csrc.nist.gov/publications/nistpubs/index.html

NIST: SP 800-4 Computer Considerations in Federal Procurements: A Guide for Procurement initiators, Contracting Officers and Computer Security Officials
March 1992
URL: http://csrc.nist.gov/publications/nistpubs/index.html

NIST: SP 800-5 A Guide to the Selection of Anti-Virus Tools and Techniques
December 1982

URL: http://csrc.nist.gov/publications/nistpubs/index.html

NIST: Guidelines for ADP Physical Security and Risk Management
URL: http://csrc.nist.gov/publications/fips/fips31/fips31.pdf

NIST: Acquiring And Deploying Intrusion Detection Systems
URL: http://www.itl.nist.gov/lab/bulletns/nov99.htm

NIST: Guidelines on Firewalls and Firewall Policy
URL: http://www.itl.nist.gov/lab/bulletns/bltnjan02.pdf

NIST: SP 800-31 Intrusion Detection Systems (IDS)
November 2001
URL: http://csrc.nist.gov/publications/nistpubs/index.html

NIST: SP 800-18 Guide for Developing Security Plans for Information Technology Systems
December 1998
URL: http://csrc.nist.gov/publications/nistpubs/index.html

NIST: Information Security Policies For Changing Information Technology Environments
June 1996
URL: http://www.itl.nist.gov/lab/bulletns/archives/liz

NIST: Contingency Planning Guide for Information Technology Systems
URL: http://csrc.nist.gov/publications/drafts/ITcontingency-planning-guideline.pdf

FIPS 87 Guidelines for ADP Contingency Planning
March 1981
URL: http://csrc.nist.gov/publications/fips/fips87/fips87.pdf

Last Updated: May 23rd, 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
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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 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 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
SANS Munich Summer 2017	Munich, Germany	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