Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# A Policy to Prevent Outsider Attacks on the Local Network

We used to be able to say, "If the laptop or computer is not owned by us, then it is not allowed to touch our network." However, over the last few years, business need has exceeded the desire to keep our network "pure" and many non-agency owned computers now have access to our local area network (LAN). Our Windows based agency owned computers run fully configured, heuristically enabled, daily updated virus protection. Our automated inventory system queries the status of this software and we remedy any below standard co...

Copyright SANS Institute
Author Retains Full Rights

AD

Clarissa L. Evans Brown
GSEC Practical Assignment Version 1.4b, Option 2
January 15, 2004

# A Policy to Prevent Outsider Attacks on the Local Network

## Abstract

This paper describes the research completed, the course of action taken and the decisions made in writing an issue specific security policy. My organization has systems and procedures in place to protect our agency owned computers from vulnerabilities and malware threats. We established these procedures because we had experienced attacks on our network and systems that had escalated in frequency and in negative effect. However, we did not have similar security procedures in place for contractor computers on our network. This made our network, and systems on our network, open to attack from within. I considered several options to control network access to these computers and minimize their threat potential. Although imperfect, the solution was to require, through a policy, the scanning of contractor computers for vulnerabilities and malware threats and ensure that these computers are free of these threats prior to connection to our network. To ensure compliance, all future Information Technology (IT) contracts will include this policy.

## The Threat Situation

We used to be able to say, "If the laptop or computer is not owned by us, then it is not allowed to touch our network." However, over the last few years, business need has exceeded the desire to keep our network "pure" and many non-agency owned computers now have access to our local area network (LAN).

Our Windows based agency owned computers run fully configured, heuristically enabled, daily updated virus protection. Our automated inventory system queries the status of this software and we remedy any below standard computers. Prior to the installation of our Software Update Services (SUS) server, these same Windows based computers had current operating system (OS) security patches and service packs installed via "sneaker net." These procedures create a fragile wall of protection, as the wall is only as strong as the most current software updates make it. This "fragile wall" is not unique to our systems. All organizations focused on security work to stay one-step ahead of the next malware threat. Most of the contractor computers are Windows based laptops that do not log on to our domain and are thus unaffected or unnoticed by our automated systems. Our network, and systems on our network, are vulnerable to attack by any new malicious code launched internally by these contractor computers.

As part of our Defense in Depth strategy, we also utilize a network based Intrusion Detection System (IDS). A computer identified as a potential threat, is flagged by this system and a "follow up" message is sent. A computer identified by this system as a serious threat, has the Internet Protocol (IP) address leased

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

to it blocked. Our IDS has blocked contractor computers in addition to flagging them. The IDS notification system crosses organizational boundaries and relies on human intervention. Notification is sometimes slow. Because a system has to be on the network in order for the IDS work, damage can occur prior to the issuance of any alert. It is therefore important to minimize alerts.

**Examples of the Threat**

The laptops of our largest contractor are not kept up to date with service packs, security patches and known malware signatures. They move frequently between the contractor's home office and our site and are thus vectors for threats to our network. Initially, the Computer Technician (CT) supporting these contractors was very busy responding to IDS alerts sent over by the Incident Response Team (IRT). He smartly began to take a proactive approach by asking the contractors to let him run vulnerability and malware signature scans of their laptops before they hooked them up to the network. In many cases, he installed OS service packs and security updates, updated the virus signatures and cleaned infections from the computers. This was effective in decreasing the alerts.

Relying on the eyes and ears of a diligent CT to protect the network from threat has its pitfalls. The CT cannot be everywhere at all times and can only act on known information. In one instance, a CT had cleared a laptop before the contractor connected it to the network. Unbeknownst to the CT, the contractor had a problem with his laptop when he subsequently traveled to his home office. His computer support swapped out the hard drive. The contractor checked to be sure that all of his data was present on the newly swapped drive but not that any service packs, security patches or virus protection had been reinstalled. His laptop was blocked by the IDS after being on our network for a short time. In another instance, a diligent CT intercepted and scanned a contractor's laptop before allowing it network access. The CT said that it was so full of worms that the log file "scrolled." The contractor thanked the CT for cleaning the system and updating the software because the computer ran better when he was done.

Our network was victimized and shut down by previous malicious code. We put controls in place to try to prevent any other "events" from happening again. Yet, we allow contractor computers to bypass these controls. It is apparent from my examples that our network, and systems on our network, are at risk regardless of the fact that a few diligent CTs have kept the past problems to a minimum.

**Options to Control the Threat**

I explored a range of options to minimize the threat that the contractor computers posed to our network. I focused on network access. If that was controlled, then the threat could be controlled.

I considered the option of creating hardware address access control lists (ACLs) on the routers in the areas where we have contractor computers. ACLs, would not let non-approved computers past the routers. Approved ACL list computers would be required to be free of vulnerabilities or malware threats. Unfortunately, the high turnover and mobility of the contractors would make

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

managing ACLs too laborious for our very small network team. In addition, this solution would not address the issue of contractor laptops or computers accessing the network in other areas that lacked the ACLs. Also, an ACL list might not have prevented the vulnerable contractor laptop that had the hard drive swapped out from accessing the network. If the hardware address had not changed as a result of the repair work that was done, such as replacing the network interface card (NIC), the laptop would have had access to the network through the router. The IDS would have blocked the IP address leased to it either way. All the work of setting up and maintaining the ACL would have been for naught. In addition, spoofing of hardware addresses can occur. This spoofing can allow an infected or vulnerable computer to sneak right past our defenses. In fact, since a computer has to be free of vulnerabilities or malware threats in order to be on the ACL list, the list would be a waste of time. Therefore, ACLs would not be effective in solving this issue.

I contemplated turning off Dynamic Host Configuration Protocol (DHCP) on the network and using static addressing instead. Static addressing is an arduous system that requires all IP addresses be set manually on each computer instead of automatically assigned as with DHCP. This would prevent any unknown, potentially threatening or vulnerable computers from automatically joining our network as the process of setting the IP address requires information that a contractor would not have. However, static addressing is very difficult to manage on a very large network, such as ours, and requires more IP address space than we have. Additionally, the computer would have to be “approved” before being given a static address. Therefore, the extra work of managing a statically addressed network would not be worth it.

I pondered the option of creating a virtual LAN (VLAN) for the contractor computers in order to isolate them from the rest of our network. This would not work, as many of the contractors need access to our network resources such as databases and file servers. However, I noted that a VLAN would be useful for isolating the computers from the rest of our network while accessing Internet resources and update sites. This is something that I will explore further when I have completed this project.

Another option would be to require that the contractor computers join our domain. We could create a container in active directory to group the contractor computers for identification and apply an auto update policy. This would allow us to push OS service packs and security updates through the SUS server. However, since our SUS server pushes software on a set schedule, there would be a window of time when the non-updated computer is on the network. If a computer leaves the domain prior to the time the SUS server is set to run, then reconnects later, the computer would not receive any updates. Perhaps this domain solution would require computers to be approved prior to accessing the network also. This makes the argument that contractor computers should not be laptops but instead less mobile desktop systems. Making the contractor computers join the domain would also allow us to use our automated inventory system to query the computers for virus software status. This would require them to run one of our brands of virus protection software to be effective. All of these

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

procedures would be the most time efficient for the longer-term contracts with stable staffing and not so for the "drive by" contractors, especially since it can take up to three days for domain account creation. This solution would be hard to implement and manage and less likely to satisfy the contractors simply because of their data mobility needs.

Finally, I considered simply requiring that the contractor computers be free of vulnerabilities and known signatures prior to their connection to our network. Two of my previously considered options required this prior to their implementation. This idea is similar to the procedures that those few diligent CTs were following except that we would shift most of the responsibility to the contractors. We have the scanning tools, such as the Security Auditor's Research Assistant (SARA), readily available and they could easily be provided to the contractors. If the contractors could not meet the condition, then the CTs could help. Consistent enforcement and awareness of this requirement would a challenge. However, a well-advertised written policy would combat these issues. Of course, this policy would have to be included in IT contracts to really be effective. Even so, I know that we would not achieve total compliance. We would however be aware of gross non-compliance if a contractor computer was flagged or blocked by the IDS and we could pass these non-compliance issues on to the contract officials to deal with. So, I chose this policy solution because it is proactive, the simplest to implement and it makes the most efficient use of my organizations resources.

**Developing the Policy Solution**

I began the process of developing the policy by interviewing the people that it would affect. I started with the CTs that were working in departments with active contracts. Their biggest concern was that they could be liable for problems caused by any software installed by them. In addition, they were concerned whether they had the right to require the installation of any software on non-agency owned computers. Though they had done this in the past to protect the network and help their department get what they paid for, they were concerned about repercussions. Lastly, they did not want to be in the position of denying network access to a problem computer. They wanted to point to an official written policy.

I then brought the subject up with our organization's Information Systems Security Officer (ISSO). He was supportive of the idea in that it could potentially cut down on the number of incidents that he would have to handle from the IRT.

Next, I discussed the topic with the Project Officer for one of our largest contracts. He ran the idea past the Contract Officer for his project. The Contract Officer was supportive and stated that he would make amendments to the existing contracts if necessary. The key factor for both officers was time. The process to update software, clean, scan and request an unblock of a blocked IP address from the IRT takes time (a blocked IP can be released for another computer to pick up, but this defeats the security system). They both wanted to prevent the loss of productivity caused by the IDS blocking or even flagging a contractor computer. Additionally, the Project Officer wanted to make sure that

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the scanning software was readily available when any contractor computer needed access to the network.

Finally, I talked to our organization's Chief Information Officer (CIO) about my plan to write a formal policy addressing this issue. I had to prove my case with the CIO, which I did by identifying the contractor computers already on our network and stating that these non-agency controlled computers were vectors to threats of our network and systems. He recognized this risk and agreed to the policy. He then proceeded to suggest existing references on format including our policy on policies (policy on manual chapters). I pointed out that all the contractors I was aware of were using one of our brands of virus protection software. What should we do when faced with another brand? Should we require that all contractors use our brand and version of software? Ours had proven effective. Could we rely on other software to be effective? I had already completed research and knew that there were organizations that rated virus protection software. If we compiled a list of acceptable software, how could we know what fully configured meant for all of the products we encountered? How would we know if it was up to date? This was obviously very difficult to achieve. Therefore, we decided that if the computer passed our scans for known malware signatures, then network access would be granted. It would not matter if it were running software with which we were unfamiliar. However, if the scan of the computer revealed active malware, then we would install and configure our own licensed virus protection software. Of course, if the computer were running a current version of one of our brands, then this would not be necessary. We would then oversee the updating and configuring of the software or do it ourselves. I asked if we then would need to uninstall our licensed software when the computer no longer needed access to our network. We both agreed that the cost of licenses was minimal compared to the benefit that our network neighbors might reap as a result of another inoculated computer. Of course, since many software installations require administrative rights, a contractor would have to have this access for any problem computer.

So, I had buy in at all levels, a format to follow, and guidance on what the policy should say. However, I wanted to be sure that we that we had the legal ability to require software installations, and in some cases, our own virus protection software on contractor computers. I reviewed United States Code (USC), Office of Management and Budget (OMB) circulars, OMB memoranda, National Institute of Standards and Technology (NIST) guidelines, NIST Federal Information Processing Standards (FIPS) publications and Department of Health and Human Services (DHHS) policies to determine if the applicable laws, regulations and policies addressed this issue. I found that OMB policy supports the use of current software including OS patches and upgrades. I also found that my agency had a high-level policy specifically addressing the need for contractors to comply with our security procedures (specifically virus protection).

Now I had everything I needed to develop the policy. I utilized the SANS Policy Worksheet to derive the policy.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Policy Worksheet

| Step 1 Who does the procedure? | Why? |
|---|---|
| The computer owner/user or Computer Technician completes the procedure. | It does not matter who completes the procedure, as long as it is completed. |
| **Step 2 What is the procedure?** | **Why?** |
| To run the current recommended or licensed vulnerability and malware signature scans on the contractor computer. If the scans report problems with the computer, then all identified infections must be cleaned and all OS critical security patches and service packs must be installed. Additionally, fully configured and up to date <Agency> licensed virus protection must be installed. <Agency> licensed software does not need to be installed if a current version of <Agency> approved virus protection software exists on the computer and can be configured to <Agency> standards.<br>If installed, <Agency> licensed virus protection software does not have to be removed from non-agency owned computers once they no longer require access to the <Agency's> network. If Computer Technicians employed by the <Agency> perform the installations, then the owner or user of the laptop cannot hold the technician (s) liable for damages. The contractor must have or be able to provide, administrative rights on the computer to complete most installations. | Existing tools have proven reliable in detecting potential vulnerabilities and malware signatures. A computer that is not running fully configured and up to date virus protection and does not have the most current service packs and critical patches is vulnerable to attack by viruses, worms or Trojans. A breached system can become a vector for the attack to spread to the rest of the network and systems on that network. If a vulnerability or malware signature exists, it (or they) must be remedied through the installation of the above-mentioned software and any published fixes. The installation of <Agency> licensed software is allowed because Computer Technicians cannot be expected to be familiar with the details of all brands on the market.<br>The cost of providing licensed software to non- <Agency> computers is minimal compared to the benefit of our network "neighbors." There is some risk of software incompatibility with installation. This risk is most significant on computers not configured to our standards. CTs should not be liable for providing a service that in intended to meet the needs of the contractor. Many software installations require administrative rights. |
| **Step 3 When is the procedure done?** | **Why?** |
| The procedure must be completed prior to giving initial network access to any computer. It must be repeated each time a computer leaves then returns to the network. The procedure is not necessary for a returning computer if it does not connect to any wired or wireless network or if no | Any computer new to the network or returning to the network from another location that is not regularly queried for virus protection status or regularly receiving service packs and security patches, could act as a threat vector for viruses, worms or Trojans to enter our network. There is risk that a |

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

| | |
|---|---|
| hardware or software changes occur while the computer is away from the <Agency> network. | computer may be missing updates if it not scanned every time it leaves and returns to the network. However, scanning the computers every time they leave the network and return is time consuming. This way at least ensures that the computer will not introduce an active threat to the network. A computer that does not connect to another network while away is rare. Most will be scanned and thus updated. |
| Step 4 Where is the procedure done? | Why? |
| The procedure is completed at the location of the computer or Computer Technician. | No specific location is necessary. |
| Step 5 Policy Statement | |
| To ensure the protection of the <Agency's> network, and systems on that network, from malware threats, all non-<Agency> computers with demonstrated business need requiring access to the <Agency's> network must be free of vulnerabilities and known malware signatures prior to accessing the network for the first time and anytime thereafter when a threat may have been introduced. | |

I then used the information from the worksheet, input from the people I interviewed, my own insight and my organization's manual chapter format to write the policy.

**The Policy**

---

906 – Allowing Non-Agency Owned Computers Access to the <Agency's> LAN

---

A. PURPOSE: This policy specifies the requirements that non-agency owned computers must meet in order to gain access to the <Agency's> network. These requirements are in place to protect the <Agency's> network, and systems on that network, from malware threats. If these requirements are not met, then network access for the computer (s) is denied. This policy applies

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

to Windows based non-agency owned computers with a demonstrated need to access the <Agency's> network. The owners or users of these non-agency owned computers must comply with this policy.

B. BACKGROUND: An increasing number of contractor computers have a legitimate need for access to the <Agency's> network. All agency and contractor computers are required to have fully configured and up to date virus protection software installed. Agency and contractor computers must also have current OS service packs and security updates installed. The purpose of both of these requirements is to protect the <Agency's> network and systems on that network from malware threats. These malware threats exist in the form of worms, viruses and Trojans. All forms of threat put the network and systems on the network at risk for loss of confidential information (C), loss of integrity (I) of that information and loss of the availability (A) of information and resources. A computer that is not running fully configured and up to date virus protection and does not have the most current service packs and critical patches is vulnerable to attack. A breached system can become a vector for the attack to spread to the network and systems on the network resulting in the loss of one, or potentially all, CIA. Additionally, if a computer is flagged or blocked by the IDS because of a vulnerability or malware infection, updating software and removing infections causes loss of productivity. If the computer is blocked, even more productivity is lost, as a request, including the results of a clean scan, must be submitted to the IRT for response. Delays in productivity negatively affect the timeline of a project for the contractor, the contracting official and the <Agency>. Agency computers receive OS service packs and security updates from the <Agency's> SUS Server. The <Agency's> automated inventory system queries agency computers for anti virus software status and below standard computers are fixed. This intent of this policy is to provide a mechanism to bring contractor computers in compliance with agency requirements.

C. ISSUING OFFICE: Department of <Name, Location, Phone>. Prepared by: <Name, Office, Title, Location, Phone, Date>

D. REFERENCES:

1. Computer Security Act of 1987, http://www.ciao.gov/resource/computer_security_act_of_1987printer.html

2. DHHS Automated Information Systems Security Program Handbook, http://wwwoirm.nih.gov/policy/aissp.html

3. OMB Memorandum M-99-20, http://www.whitehouse.gov/omb/memoranda/m99-20.html

4. Anti Virus Software, <internal web site link>

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

5. Virus Removal Tools, <internal web site link>

6. Scanning Tools, <internal web site link>

E. DEFINITIONS:
[Also see APM Chapter 107 for a glossary of abbreviations and acronyms]

1. IDS: Intrusion Detection System
2. IRT: Incident Response Team
3. LAN: Local Area Network, computer network
4. Malware: Generic term used to refer to all types of malicious computer code
5. OS: Operating System
6. SUS: Software Update Services Server
7. Threat: Circumstance or event with potential to intentionally or unintentionally exploit a vulnerability in a system
8. Vulnerability: Flaw or weakness in a system that could be exploited with malicious intent

F. RESPONSIBILITIES:

CIO: Is responsible for approving or denying all written requests for exception to this policy.

ISSO: Must make known and available the current recommended and /or licensed scanning software to the Computer Technician (s) and the contractor (s). Serve as liaison to IRT for requests to unblock computers.

Contracting Official: Must be aware of and make this policy known to contractors. Must ensure inclusion of this policy in contract documents.

Computer Technician: Must either scan contractor computers or make scanning tools available to contractors. Must either install or make available to contractors any necessary OS service packs, security patches or virus protection software as identified by scanning software. Must also clean or aid the contractor in cleaning any identified infections. The Computer Technician must respond in a timely manner to contractor requests for any of the above services.

Contractor: Before being granted <Agency> network access, must perform scans on computer or make computer available to Computer Technician for scanning. Must install or allow Computer Technician to install any necessary OS service packs, security patches or virus protection software as identified by scanning software. Additionally the contractor must clean or allow the Computer Technician to clean any identified infections. The contractor must

© SANS Institute 2004, Author retains full rights.

have or be able to provide, administrative rights on the computer to complete software installations. The Contractor must communicate the need for Computer Technician services to the Computer Technician in a timely manner.

G. POLICY: To ensure that the <Agency's> network and systems on that network are protected from malware threats, all non- <Agency> computers with demonstrated business need requiring access to the <Agency's> network must be free of vulnerabilities and known malware signatures prior to being given network access for the first time and anytime thereafter when a threat may have been introduced.

H. PROCEDURES:
   a. Before accessing the <Agency> network, contractor computers must be scanned for vulnerabilities and known signatures. See referenced web site links for the current recommended or licensed scanning tools and instructions on the use of these tools.
   b. If the scans report vulnerabilities and or active malware on the computer, then all OS security patches and service packs must be installed and any identified infections must be cleaned. Additionally, fully configured and up to date <Agency> licensed virus protection software will be installed. <Agency> licensed software does not need to be installed if a current version of <Agency> approved virus protection software exists on the computer and can be configured to <Agency> standards.
   c. If Computer Technician(s) employed by the <Agency> perform the scanning and software installations, then the owner or user of the laptop cannot hold the agency or technician(s) liable for damages.
   d. These procedures must be followed each time the computer leaves and then returns to the network. This does not have to be done if a computer does not connect to any wired or wireless network while away from the <Agency> network or if no modifications of hardware or software have been made.
   e. If a successful malware attack occurs on the non-agency owned computer while it is on the <Agency's> network, <Agency> Computer Technicians will aid in the remediation.
   f. <Agency> licensed virus protection software does not have to be removed from non-agency owned computers once they no longer require access to the <Agency's> network.

I. DATE LAST UPDATED: 14 January 2004

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

**Analysis and Outcome**

After the policy was complete, I went back to the SANS textbook to make sure that it passed all the tests. I asked myself the following questions:

Q1. Does it contain the most common elements?
A1. Yes. The common elements are; who must comply, who is responsible and what they must do. The scope section of a policy describes who must comply. Though my organization does not use a scope section, I added scope statements to the Purpose section and described compliance to this policy in the Responsibilities section. The other elements, who is responsible and what they must do; are covered in the Responsibilities and Procedures sections respectively.

Q2. Is it clear?
A2. Yes, It was reviewed be several levels of staff and each understood the specifics of the policy.

Q3. It is concise?
A3. Well, it exceeds the two page recommended limit but I based it on my organizations format of what had to be included. At least the policy statement meets the recommended length of one (long) sentence.

Q4. Is it realistic?
A4. Yes, it sets the same standards for contractor computers that are in force for agency owned computers.

Q5. Does it provide sufficient guidance for the development of procedures?
A5. Yes, the policy spells out the required actions in the procedures section. However, the policy does not describe the procedures in enough detail to preclude a separate procedures document.

Q6. Is it consistent with higher-level policy and guidance?
Q6. Yes, my agency wrote an Automated Information Systems Security Program (AISSP) handbook based on the Computer Security Act of 1987 that specifically requires contractor computers to meet the same security standards set forth in the document. The AISSP specifically requires virus protection. Additionally, OMB policy supports the use of current software including OS patches and upgrades.

Q7. Is the policy forward thinking?
A7. Yes, the policy specifies roles for responsibility not individual people and does not specify which scanning processes to use but instead includes a link to an internal web site where the current scanning software and instructions exist.

Q8. Are there provisions to keep it current?

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

A8. Yes, per my organization's Administrative Policy Manual, each policy is set for annual review by the manual coordinator. This is especially important with impending changes in Federal Law.

Q9. Is the policy readily available?
A9. The policy will be posted on the web site of the Administrative Policy Manual. The procedure for approval of posting of a policy includes the review of Senior Administrative Officers (AOs). All AOs are involved in departmental contracts. To be sure that existing and future contracts include this policy; all AOs will receive a copy of the policy. Upon approval of the policy, it will be included in the orientation documentation that CTs receive. Each current CT will receive a copy of the policy. The policy will be a topic at a weekly meeting of the technicians.

Next, I sent a copy of the policy to the CIO, ISSO, the Project Officer I interviewed and a few selected Computer Technicians. I made a few changes as suggested by the CIO, but overall the policy met approval. I will now send a copy to the Manual Coordinator who in turn will forward the policy to the Senior AOs. The Senior AOs have up to a month to respond. While I am waiting for a response, I plan to gather IDS alert statistics so that I have some measurable baseline from which to measure changes in the number of IDS alerts as a result of the policy being in effect. I also plan to draft detailed procedures and a checklist.

**Conclusion**

I identified a problem within my organization and developed a solution for it in the form of an incident specific security policy. Now that I am somewhat familiar with the laws and regulations affecting Information Technology for my agency and know the format and procedure for writing a policy, I could easily do it again. In fact, the process of writing this one policy has made me aware of many others that we are lacking. I hope that the security awareness that our organization has fostered over the last few years will help me get acceptance at all levels on others as I had on this one.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## References


Castelli, Jacqueline. "Choosing your anti-virus software." 12 April 2002. http://www.sans.org/rr/papers/index.php?id=784 (15 January 2004)

Cisco. "Action Steps for Improving Information Security." *Network Security Investment-The Executive ROI Briefcase.* 26 November 2003. http://www.cisco.com/warp/public/cc/so/neso/sqso/roi5_wp.htm (15 January 2004)

Cole, Eric etal. SANS Security Essentials with CISSP CBK, Volume 1. SANS Institute, 2003

Danchev, Dancho. "Building and Implementing a Successful Information Security Policy." *Network Security Library.* 25 June 2003. http://www.secinf.net/policy_and_standards/Building_Implementing_Security_Policy1228.html (15 January 2004)

Department of Health and Human Services. "Automated Information Systems Security Program Handbook." http://wwwoirm.nih.gov/policy/aissp.html (15 January 2004)

Fraser, B. (Editor). "RFC 2196: Site Security Handbook." September 1997. http://www.faqs.org/rfcs/rfc2196.html (15 January 2004)

Lindley, J. Patrick. "Technical Writing for IT Security Policies in Five Easy Steps." 20 September 2001. http://www.sans.org/rr/papers/index.php? id=492 (15 January 2004)

Moleshead, Zoe. "Internal Insecurities." *The Information and Technology Publishing Co. Ltd*. 20 July 2002. http://www.itp.net/features/details.php?id=564&srh=Internal%20Insecurities&tbl=itp_features (15 January 2004)

National Institute of Standards and Technology. "Security Self-Assessment Guide for Information Technology Systems." November 2001. http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf (15 January 2004)

National Institute of Standards and Technology. "Guideline for the Analysis of Local Network Security." 9 November 1994. http://csrc.nist.gov/publications/fips/fips191/fips191.pdf (15 January 2004)

U.S. Office of Management and Budget. "Circular No. A-130." 8 February 1996. http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html (15 January 2004)


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

U.S. Office of Management and Budget. "Memorandum M-99-20." 23 June 1999. http://www.whitehouse.gov/omb/memoranda/m99-20.html (15 January 2004)

U.S. Public Law. "Computer Security Act of 1987." 11 June 1987. http://www.ciao.gov/resource/computer_security_act_of_1987printer.html (15 January 2004)

U.S. Public Law. "Federal Information Security Management Act of 2002." http://csrc.nist.gov/policies/FISMA-final.pdf (15 January 2004)

Wan, Chris. "Developing a Security Policy-Overcoming Those Hurdles." 16 January 2003. http://www.sans.org/rr/papers/index.php?id=915 (15 January 2004)

Wills, Laura. "Security Policies: Where to Begin." 8 February 2003. http://www.sans.org/rr/papers/index.php?id=919 (15 January 2004).

© SANS Institute 2004, Author retains full rights.

Last Updated: September 5th, 2015

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Crystal City 2015 | Crystal City, VAUS | Sep 08, 2015 - Sep 13, 2015 | Live Event |
| SANS Network Security 2015 | Las Vegas, NVUS | Sep 12, 2015 - Sep 21, 2015 | Live Event |
| SANS Seoul 2015 | Seoul, KR | Sep 14, 2015 - Sep 19, 2015 | Live Event |
| SANS Tallinn 2015 | Tallinn, EE | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Baltimore 2015 | Baltimore, MDUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| Data Breach Investigation Summit & Training | Dallas, TXUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Perth 2015 | Perth, AU | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS ICS Amsterdam 2015 | Amsterdam, NL | Sep 22, 2015 - Sep 28, 2015 | Live Event |
| SANS Bangalore 2015 | Bangalore, IN | Sep 28, 2015 - Oct 17, 2015 | Live Event |
| SANS Seattle 2015 | Seattle, WAUS | Oct 05, 2015 - Oct 10, 2015 | Live Event |
| SANS DFIR Prague 2015 | Prague, CZ | Oct 05, 2015 - Oct 17, 2015 | Live Event |
| SOS: SANS October Singapore 2015 | Singapore, SG | Oct 12, 2015 - Oct 24, 2015 | Live Event |
| SANS Tysons Corner 2015 | Tysons Corner, VAUS | Oct 12, 2015 - Oct 17, 2015 | Live Event |
| SANS Gulf Region 2015 | Dubai, AE | Oct 17, 2015 - Oct 29, 2015 | Live Event |
| SANS Tokyo Autumn 2015 | Tokyo, JP | Oct 19, 2015 - Oct 31, 2015 | Live Event |
| SANS Cyber Defense San Diego 2015 | San Diego, CAUS | Oct 19, 2015 - Oct 24, 2015 | Live Event |
| SANS Sydney 2015 | Sydney, AU | Nov 09, 2015 - Nov 21, 2015 | Live Event |
| SANS South Florida 2015 | Fort Lauderdale, FLUS | Nov 09, 2015 - Nov 14, 2015 | Live Event |
| SANS London 2015 | London, GB | Nov 14, 2015 - Nov 23, 2015 | Live Event |
| Pen Test Hackfest Summit & Training | Alexandria, VAUS | Nov 16, 2015 - Nov 23, 2015 | Live Event |
| SANS Hyderabad 2015 | Hyderabad, IN | Nov 24, 2015 - Dec 04, 2015 | Live Event |
| SANS Cape Town 2015 | Cape Town, ZA | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS San Francisco 2015 | San Francisco, CAUS | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| Security Leadership Summit & Training | Dallas, TXUS | Dec 03, 2015 - Dec 10, 2015 | Live Event |
| SANS Milan 2015 | OnlineIT | Sep 07, 2015 - Sep 12, 2015 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |