Manageable Network Plan

Comments or feedback? ***manageable@thematrix.ncsc.mil***

Manageable Network Plan

Have you discovered your network is insecure? Are your network admins always running around putting out fires? Does it seem to be impossible to get anything implemented or fixed on your network? If so, your network may be unmanageable.

The Manageable Network Plan is a series of milestones to take an insecure and unmanageable network from where it is to where it should be: manageable and minimally secure. The Plan is intended to be a long term solution; implementing the milestones may take a significant amount of resources and time (possibly months or even years). But consider this: **If your network is not manageable, or only barely manageable, it will be painfully difficult for you to fully implement *any* security measures. Once your network is manageable, then you will be able to consider and implement security measures—*and verify their implementation*—much more easily.**

Admins may start shouting, "We have no free time! How can we do all this???" Having a manageable network *increases* your free time; it allows you to be *proactive* instead of *reactive*. And if you do have a huge network, don't take on the whole network at once: consider starting with individual subnets.

The Plan milestones mainly address two very important areas: documentation and configuration management. Each milestone contains a To Do list, and may also contain Documentation requirements, things to Consider, and Ongoing tasks. Ideally, each milestone should be fully implemented before moving on to the next milestone, although some milestones can be implemented in parallel. If the earlier milestones are already implemented on your network, skip ahead to the first one that is not yet fully implemented. To determine this, each milestone has a Checklist. For each question in a milestone's Checklist, answer Yes or No; if No, provide an Explanation. If you consider the explanation acceptable from a risk management standpoint, check Accepts Risk. If all the questions can be answered Yes or Accepts Risk, the milestone is complete. Document your answers to these milestone checklists. If a future network evaluation finds problems on your network, that may indicate that you should no longer accept the risks that you did in some areas, and that changes are needed.

The Plan only occasionally offers specific guidance in the form of suggestions and references to additional material. This is because the Plan is meant to provide overall direction; the details are going to be network-specific. Use the Plan milestone To Do lists, Documentation requirements, and Ongoing tasks as a guide, and generate specific tasking for your network. The points to Consider under each milestone may suggest additional tasks for your network. Be sure each of the tasks include *what* is to be done, *who* is to do it, and *when* the task must be completed. Also be sure that your specific tasking does not water down or miss the point of the Plan milestones—that won't help your network become more manageable!

Note to Management

In order for this Plan to work, it will require—as with any strategic plan—a persistent organizational commitment. We understand that this may be difficult when balancing resources for your many mission priorities.

The risk of an unmanageable network is that, although it may be *available*, it is most likely not *secure*. This Plan helps your organization begin the long process of securing your network. We recommend that you do not execute this Plan before hiring the appropriate personnel. Familiarizing yourself with the Plan and consulting with your technical people may help you identify what resources and personnel skill sets will be needed. Keep in mind that hiring and retaining competent technical people is key to securing your network; turnover of personnel greatly contributes to making a network unmanageable.

With a strong organizational commitment, we're confident that this Plan will help you get your network manageable and more secure!

Milestone 1: Prepare to Document

Documentation will be a necessary part of every milestone.

To Do

- Set up a way to begin documenting information about your network. When a network change is made, be sure both the *what* and the *why* is documented.
  - Suggestion: Use a blog or bulletin board to notify admins of changes, and a wiki to document information. A common issue is when multiple admins administer the same devices: One of them goes on vacation and wants to know who picked up the slack (or not) while he was out. A blog of tasks the admins performed lets the admin who was on leave quickly catch up.

Consider

- **Doing documentation should be quick and painless, otherwise it will never get done. Make sure your documentation approach is easy to use.**
- The purposes of documentation are 1) to share information; and 2) to retain information. Does your documentation approach address these points?
  - Suggestion: If you do use a blog to document admin changes, consider using RSS feeds to keep other admins apprised of the changes.
- Having good documentation allows managers to track and reward progress. It may also allow users to understand and solve their own problems, instead of going to the admins for every little thing. Can management and users easily read your documentation?
- Having good documentation assists in disaster recovery. Is your documentation repository backed up on a regular basis?
- It's hard to read on-line docs when the power goes out! Is a hard copy version of relevant sections of your documentation readily available?
  - Suggestion: Hard copy documentation should at least include start-up information and sequence, and emergency procedures.
- If a network intruder obtains access to your documentation, they may discover additional information about your network. Is your documentation protected (e.g., password or PKI)?

Ongoing

- From now on, whenever a change is made to your network, or to devices on your network, document it. Even if you have no current documentation, just documenting from this point forward will be beneficial.

Checklist

Check **Yes** or **No**. If No, provide an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 1: Prepare to Document
				Do you have a way to document information about your network?
				Are you currently documenting all changes to your network?
				Have you gone over the things to Consider for this Milestone?

Milestone 2: Map Your Network

In order to have any sort of control over your network, you first need to know where everything is.

To Do

- Create an accurate map of your current network (network topology). Be sure this network map is stored in a way that it can be easily updated, as network changes occur.
- Create an accurate list of ALL devices (computers, printers, routers, gateways, etc.) on your network. For each device, record host name, role (its purpose on your network), MAC address (and IP address if static), service tag, physical location, and operating system. This will probably require a room-to-room walkthrough of your organization, so that no devices are overlooked.
  - Suggestion: Store this information in a SQL database. Applications can be written to query this database and automate many tasks.
- Create a list of ALL protocols that are running your network.

Consider

- In the map of your network, have you also included any devices connected by wireless?
- Every asset on your network should have a specific person who is responsible for it; that way, if there is a problem, you know exactly whom you have to contact. Do you have that documentation and is it up to date?
- Any devices or protocols on your network that you have not approved should be removed.

Ongoing

- Update the network map and list of devices any time a device is added to or removed from the network.
- Update the list of protocols any time a new protocol is added to your network, or an old protocol is no longer used.

Checklist

Check **Yes** or **No**. If No, provide an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 2: Map Your Network
				Do you have a current, accurate network map?
				Do you have a current, accurate list of ALL devices (computers, printers, routers, gateways, etc.) on your network, including host name, MAC address, service tag, physical location, and operating system?
				Do you have a current, accurate list of ALL protocols that are running on your network?
				Have you gone over the things to Consider for this Milestone?

Milestone 3: Protect Your Network (Network Architecture)

A sound network architecture protects your high-value assets by limiting access to them, provides important functionality consistent with your business model, and ensures business continuity in the event of a disaster.

To Do

- Identify your current network enclaves: which groups of users on your network have access to what types of information. For example, the Engineering enclave has access to the CAD drawings, the Human Resources enclave has access to the personnel files, etc.
- Identify your current high-value network assets. Note that "high-value asset" does NOT mean "the machine cost a lot of money." Identify what you are trying to protect from a *business* standpoint: what *data* is most critical to you? The machines where this data resides are your "high-value assets."
- Identify the choke points on your network, especially those on the "edge."

Documentation

- Document which groups of users on your network have access to what types of data.
- Document the high-value assets and choke points on your network.
- Document which systems are dependent on which other systems in your network (system dependencies).

Consider

- Your network enclaves should be separated so that valuable data is only available to those who need it (segregation and isolation). For example, Engineering should have access to the CAD drawings, but not the personnel files; and Human Resources should have the opposite access. Are your enclaves sufficiently separated?
  - Suggestion: If your enclaves are not sufficiently separated, consider redesigning your network architecture and migrating to that new design.
    - For guidance on network architecture and design, see *Top-Down Network Design, Second Edition* by Priscilla Oppenheimer (Cisco Press, © 2004).
    - Above all, remember to keep your network architecture as simple as possible. Simpler networks are easier to manage.
  - Suggestion: Isolate your wired and your wireless networks. Isolate your VoIP and your data networks. Isolating these networks, either physically or logically, will limit the damage if one is compromised.
  - Suggestion: Separate network assets that contain different sensitivities of information. This might be done with VLANs.
  - Suggestion: Physically separate server functions onto different servers. For example, a domain controller should not also be running a customer database.
- Have you identified the trust boundaries of your network?
  - Suggestion: Draw these trust boundaries on your network map.
- Are the choke points on your network positioned correctly to most effectively protect your high-value assets?
- Are the choke points subject to increased monitoring and control? Are the logs generated by monitoring these choke points regularly reviewed? Is there a way to automate the process?

  - Suggestion: Place security gateways at these choke points. Consider allowing only the approved protocols documented in Milestone 2 to pass these gateways. For additional security, consider only allowing certain machines to send or receive specific protocols (port-based security).
  - Suggestion: Consider implementing a system so that network administrators are automatically informed when anomalous events occur.

- Do you have custom applications facing the Internet? If so, are they protected and/or are your developers trained in writing secure code?
  - For guidance on writing secure Web applications, see http://www.owasp.org/index.php/Category:OWASP_Guide_Project
  - For guidance on testing Web applications, see http://www.owasp.org/index.php/Category:OWASP_Testing_Project

- If you want to go more in-depth than just "what's a high-value asset and what's not" on your network, consider doing a complete Risk Assessment.
  - For an introduction to Risk Assessment, see "Risk Assessment" in Chapter 3 of *CISSP Exam Cram 2* by Michael Gregg (Exam Cram, © 2005) (http://www.informit.com/articles/article.aspx?p=418007&seqNum=4)

Ongoing

- Update the documentation whenever your network enclaves, high-value assets, choke points, or system dependencies change (added, removed, or relocated).

Checklist

Check **Yes** or **No**. If No, provide an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 3: Protect Your Network (Network Architecture)
				Have you identified your network enclaves?
				Have you identified the high-value assets and choke points on your network?
				Have you gone over the things to Consider for this Milestone?

Milestone 4: Reach Your Network (Device Accessibility)

Hard-to-administer devices on your network will be looked at less often and thus are more likely to have vulnerabilities.

To Do

- Make sure EVERY device (all computers, printers, routers, gateways, etc) on your network can be properly and easily accessed (either remotely or physically) and administered.
  - Suggestion: For Windows machines, implement Active Directory.
  - Suggestion: Do not use insecure protocols (telnet, ftp, etc.) to administer devices. If using SNMP, use SNMPv3 and its security features (versions 1 and 2 are insecure).
- For any devices that cannot be accessed on a regular basis, develop a plan to administer them.

Documentation

- Document your plan to administer ALL your devices, especially those that cannot be accessed on a regular basis.

Consider

- Are your admins able to administer your network from home or from outside your network? If so, make sure that that connection is extremely secure; once this Milestone is complete, if that connection is compromised, an intruder would gain access to your entire network!
- How are you going to administer laptops and other mobile machines?

Ongoing

- Update the documentation whenever your device administration plan changes.

Checklist

Check **Yes** or **No**. If No, provide an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 4: Reach Your Network (Device Accessibility)
				Can you properly and easily access (either remotely or physically) and administer EVERY device (all computers, printers, routers, gateways, etc.) on your network?
				Do you have a plan to administer devices that cannot be accessed on a regular basis, such as laptops and other mobile devices?
				Have you gone over the things to Consider for this Milestone?

Milestone 5: Control Your Network (User Access)

Users on your network should be limited to the least privilege that they require to perform their duties.

To Do

- Establish user accounts for all normal users: normal users should never have administrative privileges.
- Not everyone will be able to be a normal user, but limit the number of users with local admin privilege to an absolute minimum.
  - Suggestion: If a user does in fact require local admin privilege, consider only allowing that privilege for a limited time.
  - Suggestion: Network administrators should not be allowed to access the Internet or e-mail from their privileged accounts, as this is a security risk. Consider giving admins low-privilege user accounts to access the Internet and e-mail, and (as a reminder to the admins) setting the Internet proxy on their high-privilege accounts to go to 127.0.0.1. Or, consider using Software Restriction Policies to disallow Internet Explorer, Firefox, etc. within their high-privilege accounts.
  - Suggestion: Consider using Windows Delegation to give some domain admin privileges to those users that require it, without giving them full access. For operating systems other than Windows, use sudo or Role-Based Access Control (RBAC).

Documentation

- For those users that require local admin privilege, document the reasons for it.
  - Suggestion: When the reasons are no longer valid, remove the local admin privilege.

Consider

- Users with normal user accounts will not be able to install software. This is good from a security standpoint, but how will you handle those users who do need to install software? How will you handle your developers who write code and need to run arbitrary things?
- Having users with local admin privilege surf the Internet or read e-mail is a VERY serious security risk! Should you have a separate disconnected network where those users who require local admin privilege are located? Should they each have a separate machine on their desks for Internet access?
- Consider setting expiration dates (quarterly or yearly) on all user accounts, so that unused accounts will be automatically disabled.
- Anyone with administrative privileges on your network will have access to all its data. Are those individuals properly vetted in your hiring process?
- When an employee leaves your organization, is his or her account(s) disabled?

Checklist

Check **Yes** or **No**. If No, provide an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 5: Control Your Network (User Access)
				Have you restricted as many users as possible on your network to the least privilege that they require to perform their duties?
				For all users not restricted to least privilege, have you documented their reasons for having elevated privileges, and are those reasons regularly reviewed?
				Have you gone over the things to Consider for this Milestone?

Milestone 6: Manage Your Network, Part I (Patch Management)

Actively managing your network in a few areas can dramatically improve your security; this milestone and the next are focused on setting up these management areas. Note that the specific implementations will differ for different devices roles and operating systems.

To Do

- Establish a patch management regime for ALL the operating system and application software on all the devices (workstations, servers, routers, etc.) on your network.
  - Suggestion: As far as possible, this should be automatic. Be careful patching your servers, so they don't all reboot at once and affect your network availability.
  - Suggestion: For the Windows operating system and Microsoft applications, use Windows Server Update Services (WSUS). Windows workstations should be set to automatically apply patches distributed by WSUS. For operating systems other than Windows, consider using Puppet and/or Spacewalk, or writing custom scripts. *[Note that these tools have not been evaluated by the NSA and might not be approved for use in your organization.]*
    - For more information on WSUS, see http://technet.microsoft.com/en-us/wsus
    - For more information on Puppet, see http://reductivelabs.com/trac/puppet
    - For more information on Spacewalk, see http://redhat.com/spacewalk
  - Suggestion: Any software (or hardware) that you are using that is End-Of-Life (EOL)—and thus no longer able to be patched—should be removed from your network as soon as possible. It is a serious security risk.

Documentation

- Document your patch management regime: include how each device is patched (automatically or manually), and the procedures for patching those devices that need patches applied manually.

Consider

- Automating administrative tasks frees up network administrator time. Is as much administration as possible done in an automated way?
- How the devices on your network are administered should be standardized. Do all your network administrators use the same tools?
- How will you know when new releases become available for non-Microsoft applications?
  - Suggestion: Have a generic admin alias that maps to all the admins, and subscribe to release announcements for your approved applications.
- How will you update non-Microsoft applications? Device drivers? Web browser plug-ins?

Ongoing

- Update the documentation whenever your patch management regime changes.

Checklist

Check **Yes** or **No**. If No, provide an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 6: Manage Your Network, Part I (Patch Management)
				Have you established and documented a patch management regime for ALL the operating system and application software on your **workstations** (including laptops and other mobile devices)?
				Have you established and documented a patch management regime for ALL the operating system and application software on your **servers**?
				Have you established and documented a patch management regime for ALL the operating system and application software on your **routers** and other network devices?
				Have you gone over the things to Consider for this Milestone?

Milestone 7: Manage Your Network, Part II (Baseline Management)

To Do

- Create an approved application list for each class of device on your network (client workstations, servers, etc.). For each application, specify its name and specific version, the reason it was approved, and the network ports and protocols it uses (if applicable).
- Establish the criteria and process for getting an application on the approved list.
  - Suggestion: The reason for having an application on the approved list should never be just "Because so-and-so wants it." The application should always be justified by a business case, like "We need Adobe Flash on our Internet-connected boxes because our clients' websites use it."
  - Suggestion: Before an application is added to the approved list, it should be researched for any security issues. In addition, consider whether it conflicts with any of your existing security policies, and whether it can be easily updated.
  - Suggestion: Before an application is added to the approved list, it should be tested to make sure it works with the other applications in the baseline and that it won't interfere with your network. Consider setting up a small, isolated subnet for this testing.
  - Suggestion: Once an application is added to the approved list, your patch management regime from Milestone 6 will need to be updated appropriately.
- Create device (especially workstation) baselines. All software applications in a device baseline should be from the approved list for that device.
  - Suggestion: When creating your device baselines, be sure to implement the recommended security guidance for those devices. Be sure that all software included in the baselines is fully patched and correctly and securely configured. Remove unneeded components from default installs, disable unnecessary services, remove default passwords, implement screen lock timeouts, etc. Also be sure that your patch management regime from Milestone 6 covers all the software in your baselines.
    - For guidance on securing Microsoft products, see http://www.microsoft.com/technet/security/guidance/
    - For additional configuration and security guidance, see http://www.nsa.gov/snac/
  - Suggestion: When a device is replaced on your network, the new device should conform to the appropriate baseline.
  - Suggestion: Reimage your devices on a regular basis (e.g., every 6 months) to get rid of any resident malware, ensure compliance, etc. As an added benefit, this will encourage your admins to document system changes and fixes, so they don't have to "rediscover" them after the devices have been reimaged.
  - Suggestion: Set your workstations to automatically reboot on a regular basis (e.g., every night) to keep any small problems from accumulating, clear up any memory issues, etc. Consider scheduling a server task to reboot all your workstations remotely; having this task on the server allows it to be easily adjusted for special situations, instead of having to modify a script on each individual machine.
  - Consider: If you use an application such as Norton Ghost to baseline your machines, remember that every machine baselined this way will have the same local administrator account *and password*. This is probably okay for your workstations, but your servers should all have individual local administrator credentials.

Documentation

- Document the approved application list and the criteria and process for getting an application on the approved list.
- Document the device baselines.

Consider

- Backup your baselines and store them offline. An adversary who gains access to network copies of your baselines may modify them.
- Besides software baselines for your devices, do you also have hardware baselines? Some things to consider in that area might be disabling wireless cards, setting the boot order in the BIOS to hard drive only, and creating BIOS passwords.

Ongoing

- Update approved application lists, criteria and process for getting an application on the approved list, and baselines documentation whenever they change.
- As time permits, already installed applications that are not approved should be removed from the network.
- As time permits, reimage current devices with the appropriate baseline.

Checklist

Check **Yes** or **No**. If No, provide an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 7: Manage Your Network, Part II (Baseline Management)
				Have you created and documented an approved application list for each class of device on your network?
				Have you established and documented the criteria and process for getting an application on the approved list?
				Have you created and documented device (especially workstation) baselines?
				Have you gone over the things to Consider for this Milestone?

Milestone 8: Document Your Network

As time permits, your processes and procedures for your network should be documented. This helps keep your network manageable. Even if you only have time to document one process per week, that's still better than nothing!

Documentation

- Document full procedures to rebuild servers and other important devices on the network, in case of catastrophic failure.
- Document all administrative processes and procedures used on your network. Obviously, an exhaustive list of what to document cannot be provided because each network will be different. However, for ANY network, two very important procedures to document are:
  - How to add a new user
  - How (and when) to remove a user

Consider

- The documented procedures should always be followed. Are they?
- Are new network admins required to become familiar with and use this documentation?
- Consider the following scenario to determine if your documentation is complete and up-to-date: suppose one of your most knowledgeable admins cannot be contacted for an extended period of time. Will your network grind to a halt? Will it explode in chaos? What does that admin know that is not written down?
- Consider occasionally engaging the services of a technical writer to gather, clarify, and maintain your documentation.
- Keep hard copies of your processes and procedures on hand, in case of emergency.

Ongoing

- As time permits, continue to document your administrative processes and procedures.
- All documentation must be reviewed and updated as necessary.

Checklist

Check **Yes** or **No**. If No, provide an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 8: Document Your Network
				Are the procedures to rebuild servers and other important devices on your network fully documented and kept up to date?
				Do you have documented procedures for adding and removing users from your network?
				As time permits, are you documenting all other administrative processes and procedures, and keeping them up to date?
				Have you gone over the things to Consider for this Milestone?

And Now....

Congratulations! You now have a manageable network!

Ongoing

To recap, here are the ongoing things you should now be doing on your network:

- Documenting whenever a change is made to your network, or to the devices on your network
- Updating the network map and list of devices any time a device is added to or removed from the network
- Updating the list of protocols any time a new protocol is added to your network, or an old protocol is no longer used
- Updating the documentation whenever your network enclaves, high-value assets, choke points, or system dependencies change
- Updating the documentation whenever your device administration plan changes
- Updating the documentation whenever your patch management regime changes
- Updating approved application lists, criteria and process for getting an application on the approved list, and baselines documentation whenever they change
- As time permits, removing any already installed applications that are not approved
- As time permits, reimaging current devices with the appropriate baseline
- As time permits, documenting all administrative processes and procedures
- Reviewing and updating all documentation as necessary

Consider

At this point, you can begin to consider adding additional features and security to your network. See Network Security Tasks below.

Network Security Tasks

Once your network is manageable, you can begin to consider adding additional features and security to it. If your network is not manageable, or only barely manageable, it will be painfully difficult for you to fully implement *any* security measures. Once your network is manageable, then you will be able to consider and implement security measures—*and verify their implementation*—much more easily.

The following tasks are security-related things to consider implementing on your network. Obviously, which of these you implement and what order you implement them will be specific to your network. Be sure to document everything you do. Remember that each of these tasks requires man-hours both to implement and to maintain; if a task is not properly staffed, it won't be beneficial—and may even be detrimental—to your network. Make sure you include the cost of this additional manpower in any cost-benefit analysis you do.

These tasks present things to consider; they only occasionally offer specific guidance, in the form of suggestions and references to additional material. The implementation details are going to be network specific and can be handled far better by the individual network's CIO and administrators. **The best thing to do is to give the admins some research time to find the best solution for your specific network, and then give them time to implement and configure it correctly.**

Business Functionality Tasks

Backup Strategy

A comprehensive backup strategy for your network is needed to ensure business continuity in the event of unexpected failure or data loss. Your strategy should address *what* gets backed up, *when* it gets backed up, *where* the backup media are stored, and *how* to restore from backup media. Your strategy should be documented and kept updated. Be sure to regularly test the restore part of your strategy!

- Consider: If you backup your data off-site, consider encrypting it to prevent any compromise of your data.

Incident Response and Disaster Recovery

Sooner or later, something bad will happen on your network. Without a plan for incident response and disaster recovery, you will lose valuable information and possibly business. Your plan should be documented, regularly tested, and kept updated.

- Suggestion: Read *Incident Response & Computer Forensics, Second Edition* by Mandia, Prosise, and Pepe (McGraw-Hill/Osborne, © 2003), especially Chapter 2 ("Introduction to the Incident Response Process") and Chapter 3 ("Preparing for Incident Response").

Security Policy

According to RFC 2196, "A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide." In other words, your security policy specifies how your network is to be used. Your security policy should be reviewed at least yearly to check that it matches what you are currently doing.

- Consider: In and of itself, a security policy provides *no protection* for your network (other than giving you a legal basis to fire an employee who does not comply with your security directives). Your security policy must be technically and automatically enforced to have benefit. Is security enforced automatically on your network, so you don't have to just rely on users to remember your policies?

- Suggestion: Your security policy should contain the following sections (taken from *Top-Down Network Design, Second Edition* by Priscilla Oppenheimer [Cisco Press, © 2004], p. 271):
  - Access policy: Specify access rights and privileges, allowed connections to external networks and devices, and whether installing software is allowed
  - Accountability policy: Specify responsibilities of employees, including how this will be audited and how incidents will be handled
  - Authentication policy: Specify password policy and guidelines for remote authentication
  - Privacy policy: Specify employee expectations of privacy regarding monitoring of email, keystrokes, and access to their files
  - Computer-technology purchasing guidelines: Specify requirements for acquiring, configuring, and auditing systems and networks for compliance with the security policy
  - User agreement: Employees must sign a document stating that they agree to comply with the security policy
- Suggestion: Make sure your security policy is not so restrictive that it annoys your users, or they will find ways to get around it.

Training

People need training. Training allows your admins to learn from the pros and meet people they can contact (possibly for free) if they have a problem. Users need regular training so they are aware of how your network should and should not be used. Managers need training to learn how they can better enable and support the admins trying to manage and secure the organization's network. Training should be interactive, hands-on, and useful.

- Consider: Are your admins certified? Certification ensures a baseline level of understanding of IT functions and lends credibility to the IT staff.
- Consider: Do you have management buy-in for needed network security changes? If not, management may require better presentation of the reasons why the changes are needed, and what the results of *not* implementing the changes could be.
- Consider: Do your users know what's in your security policy?

Host-Based Security Tasks

Executable Content Restrictions

The only applications and code that should run on your operational network should be applications and code that you have approved. Unapproved—and possibly malicious—code should not be allowed to run.

- Suggestion: Various techniques can be used to enforce this, first and foremost by having your users not run as administrator. Other techniques include Windows Software Restriction Policies (SRP), Data Execution Prevention (DEP), and Address Space Layout Randomization (ASLR). Host Intrusion Prevention Systems (HIPS) can also be used to enforce execution restrictions.
  - For more information on implementing SRP, see http://technet.microsoft.com/en-us/library/bb457006.aspx
  - For more information on enabling DEP on Windows, Linux, Solaris, and Macintosh, go to http://www.nsa.gov/ia/ and search for "DEP"
- Suggestion: Microsoft Office documents are often used to deliver malicious code. The Microsoft Office Isolated Conversion Environment (MOICE) can be used to sanitize these Office documents when they are opened, but before the malicious code can execute.
  - For more information on implementing MOICE preprocessing of Office documents, go to http://www.nsa.gov/ia/ and search for "MOICE"

Virus Scanners and Host Intrusion Prevention Systems (HIPS)

A host-based virus scanner detects and removes known threats; a Host Intrusion Prevention System (HIPS) detects suspicious host behavior to protect against not-yet-known threats. Your hosts need protection from both kinds of threats. All of your hosts should employ a HIPS and should regularly run virus scans. Also, the virus scanners and HIPSes must be kept up to date.

Personal Electronic Device (PED) Management

Without proper management of Personal Electronic Devices (e.g., USB drives), unauthorized devices will be connected to your operational systems. Data could be stolen, or viruses unknowingly transferred.

- Suggestion: Your security policy should specify what can and cannot be connected to workstations by users. However, this must be enforced so you don't have to just rely on users to remember your policy. Consider using an application to do this enforcement automatically.

Data-at-Rest Protection

If a mobile device, such as a laptop or Blackberry, is lost or stolen, sensitive data on that device could be compromised. To prevent this, files on the device should be protected.

- Suggestion: Use either a software or hardware encryption solution to encrypt the data on the device. Be sure to *not* then store the decryption key on the device. If you use Windows Vista Enterprise or Ultimate, or Windows Server 2008, BitLocker Drive Encryption is included with those operating systems.
- Consider: Some mobile devices offer "self-destruct" (data wipe) capabilities if someone fails logging on to them too many times.

Network Monitoring and Control Tasks

Network Access Protection/Control (NAP/NAC)

When someone plugs a device into your network, the device should not automatically be connected to your operational network. The device should only be allowed on the operational network after a verification procedure (authenticate, verify patch level, etc.).

- Suggestion: Consider using an application like NetReg (http://netreg.sourceforge.net; Carnegie Mellon's version: http://www.net.cmu.edu/netreg). *[Note that this tool has not been evaluated by the NSA and might not be approved for use in your organization.]*

Security Gateways and Firewalls

Security gateways and firewalls examine traffic and provide a way to allow, deny, or modify the traffic between nodes. Security gateways should be placed at the choke points on your network, so that sensitive information is adequately segregated from the rest of the network by means of the infrastructure.

- Suggestion: Direct all your e-mail traffic through a gateway. Consider doing filtering, virus scanning, or blocking of attachments there. Also consider doing spam blocking and domain enforcement (e.g., e-mails from outside that appear to originate from inside are blocked).
- Suggestion: Direct all your web traffic through a gateway. Consider restricting downloading binary content there.
- Consider: For your firewalls, consider whether they should be stateful, whether they should do both ingress and egress filtering, and if they should do any rate-limiting.

Remote Access Security

Remote access (wireless access, people accessing your network from home, etc.) can be difficult to secure. First consider: Should users be allowed remote access to your network? Should administrators be able to access and control your network from home? If so, make sure that unauthorized people cannot access your network because of insecure protocols or security mechanisms.

- Suggestion: Limit the access that remote devices have to your network, place them in a quarantine, or subject them to increased monitoring.
- Suggestion: Require users accessing your network remotely to use a VPN and to only VPN from company-owned machines. Require ALL traffic to go through the VPN; do not allow split-tunnels.
- Suggestion: Use secure wireless protocols. Authenticate your wireless users by using a RADIUS server or VPN solution.
- Suggestion: Use NAP/NAC to enforce some security requirements on remote users.
- Suggestion: Regularly audit your remote access. Make sure that you know in general who is accessing your network when, so you can spot any anomalous activity.

Network Security Monitoring

Without knowing what is happening on your network, you will be unable to detect problems early. By knowing what traffic normally flows through your network, you will be able to detect anomalies. Your network security monitoring solution should be configurable and precise enough that you can quickly adjust it to monitor select things more in depth if you suspect a problem or infection.

- Suggestion: Read *The Tao of Network Security Monitoring* by Richard Bejtlich (Addison Wesley, © 2005).
- Suggestion: Consider implementing a system so that network administrators are automatically informed when anomalous events occur.
- Suggestion: Consider using Snort (http://www.snort.org) or Nessus (http://www.nessus.org/nessus). *[Note that these tools have not been evaluated by the NSA and might not be approved for use in your organization.]*
- Consider: Is your monitoring solution effective to monitor not only at the edge of your network (external threats), but also *inside* your network, such as at choke points and trust boundaries (insider threats)?

Log Management

Your logs (gateway and firewall logs, router logs, IDS logs, host OS logs, virus scan and HIPS alerts, etc.) contain information that can help with troubleshooting, compliance, incidence response, and statistics. However, these logs can rapidly become completely unmanageable and hence, completely ignored. Having a way to manage these log files will ensure that you will be able to retrieve information when you need it. Configure your logging to provide sufficient useful information, but not too much: for example, only record events at warning level and above. Your logs should be reviewed regularly—more often, if you suspect a problem or infection.

- Suggestion: Deploy a centralized logging solution. Consider using an application like Splunk (http://www.splunk.com) or Snare (http://www.intersectalliance.com). *[Note that these tools have not been evaluated by the NSA and might not be approved for use in your organization.]*
- Suggestion: Time synchronization in your logs is very important, so that events can be properly correlated. Use Network Time Protocol (NTP).

- Suggestion: Consider implementing a system so that administrators are automatically informed when anomalous events occur.

Audit Strategy

To verify that your administrative actions are having the desired effect on your devices and users, you need an audit strategy. You can also use an audit to make sure you have approved all the protocols and applications currently running on your network, and gather metrics about your network. Your audit strategy should address *what* gets audited, *when* it gets audited, and *what* you're looking for.

- Suggestion: Consider using Nessus (http://www.nessus.org/nessus) and/or a Security Content Automation Protocol (SCAP) validated tool. *[Note that these tools have not been evaluated by the NSA and might not be approved for use in your organization.]*
- Suggestion: Consider gathering the following information:
  - How many total devices/hosts are currently on your network
  - How many devices/hosts currently cannot be contacted by the administrator
  - How many devices/hosts currently do not comply with your documented baselines
  - How many devices/hosts currently are running unapproved applications
  - How many devices/hosts currently aren't fully patched
  - How many total user accounts currently exist on your network
  - How many old, unused, or disabled (and perhaps unauthorized) accounts currently exist on your network
  - How many weak passwords exist on your network
  - Do you have any rogue, unauthorized wireless access points (Check by warwalking / wardriving)
- Suggestion: Read *Security Metrics* by Andrew Jaquith (Addison Wesley, © 2007).

Quick Reference

Readings Mentioned

Network Architecture (Milestone 3)

- *Top-Down Network Design, Second Edition* by Priscilla Oppenheimer (Cisco Press, © 2004)
- "Risk Assessment" in Chapter 3 of *CISSP Exam Cram 2* by Michael Gregg (Exam Cram, © 2005) (http://www.informit.com/articles/article.aspx?p=418007&seqNum=4)
- Writing secure Web applications (http://www.owasp.org/index.php/Category:OWASP_Guide_Project)
- Testing Web applications (http://www.owasp.org/index.php/Category:OWASP_Testing_Project)

Baseline Management (Milestone 7)

- Securing Microsoft products (http://www.microsoft.com/technet/security/guidance/)
- Additional configuration and security guidance (http://www.nsa.gov/snac/)

Incident Response and Disaster Recovery (Business Functionality Network Security Task)

- *Incident Response & Computer Forensics, Second Edition* by Mandia, Prosise, and Pepe (McGraw-Hill/Osborne, © 2003)

Executable Content Restrictions (Host-Based Network Security Task)

- Implementing Windows Software Restriction Policies (SRP) (http://technet.microsoft.com/en-us/library/bb457006.aspx)
- Enabling Data Execution Prevention (DEP) on Windows, Linux, Solaris, and Macintosh (go to http://www.nsa.gov/ia/ and search for "DEP")
- Implementing Microsoft Office Isolated Conversion Environment (MOICE) preprocessing of Office documents (go to http://www.nsa.gov/ia/ and search for "MOICE")

Network Security Monitoring (Network Monitoring and Control Network Security Task)

- *The Tao of Network Security Monitoring* by Richard Bejtlich (Addison Wesley, © 2005)

Audit Strategy (Network Monitoring and Control Network Security Task)

- *Security Metrics* by Andrew Jaquith (Addison Wesley, © 2007)

Tools Mentioned

Note that these tools have not been evaluated by the NSA and might not be approved for use in your organization.

Patch Management (Milestone 6)

- Windows Server Update Services (WSUS) (http://technet.microsoft.com/en-us/wsus)
- Puppet (http://reductivelabs.com/trac/puppet)
- Spacewalk (http://redhat.com/spacewalk)

Network Access Protection/Control (NAP/NAC) (Network Monitoring and Control Network Security Task)

- NetReg (http://netreg.sourceforge.net; Carnegie Mellon's version: http://www.net.cmu.edu/netreg)

Network Security Monitoring (Network Monitoring and Control Network Security Task)

- Snort (http://www.snort.org)
- Nessus (http://www.nessus.org/nessus)

Log Management (Network Monitoring and Control Network Security Task)

- Splunk (http://www.splunk.com)
- Snare (http://www.intersectalliance.com)

Audit Strategy (Network Monitoring and Control Network Security Task)

- Nessus (http://www.nessus.org/nessus)