Manageable Network Plan

Networks often become unmanageable and rapidly get out of control. An unmanageable network is insecure. The Manageable Network Plan is a series of milestones to take an unmanageable and insecure network and make it manageable, more defensible, and more secure. It provides overall direction, offers suggestions, calls out crucial security tips, and gives references to books, Web resources, and tools.

Comments or feedback? **manageable@nsa.gov**

The Manageable Network Plan

Have you discovered that your network is insecure? Are your network administrators 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.

An unmanageable network is insecure!

The Manageable Network Plan is a series of milestones to take an unmanageable and insecure network and make it manageable, more defensible, and more 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: If your network is not manageable, or only barely manageable, it will be very difficult for you to fully implement *any* security measures. Once your network is manageable, you will be able to consider and implement security measures—and verify their implementation—much more efficiently and effectively.

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.

Each of the Plan's milestones contains a "To Do" list, and may also contain documentation requirements, points to consider, and ongoing tasks. Ideally, each milestone should be fully implemented before moving on to the next one, 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.[1] If all the questions can be answered Yes or Accepts Risk, the milestone is complete. Document and date your answers to these milestone checklists. If a future network evaluation finds problems on your network, it may indicate that you should no longer accept the risks that you did in some areas, and that changes are needed.

The Plan provides overall direction, offers suggestions, calls out crucial security tips,[2] and gives references to books, Web resources, and tools.[3] Every network is different, so 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. When developing these tasks, be mindful of any security assessment and authorization authorities that you must comply with. Use relevant standards and community-vetted data models (such as SCAP standards,[4] Department of Defense data models, etc.), so that you can benefit from others' work, both immediately and in the long term. Be sure each task states *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*. It may be available to those who *shouldn't* have access! This Plan helps your organization begin the long process of securing your network. The Plan is consistent with the Consensus Audit Guidelines (CAG) (www.sans.org/cag) and will enable you to more easily implement any regulatory requirements you may have. 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.

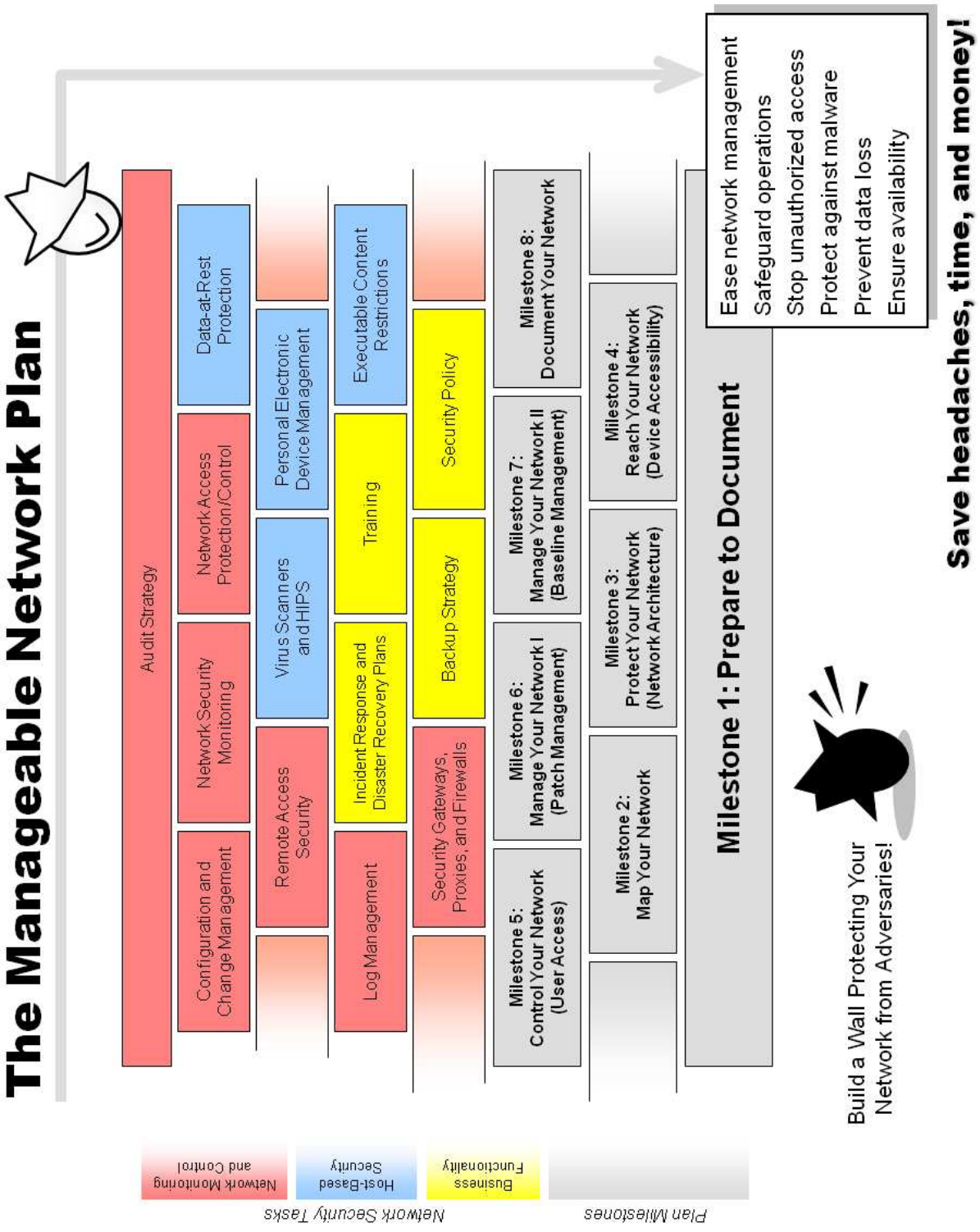
With a strong organizational commitment, we're confident that this Plan will help you make your network manageable and more secure!

[1] For information on risk management, see NIST Special Publication 800-39: "Managing Information Security Risk: Organization, Mission, and Information System View" (Available at http://csrc.nist.gov/publications/PubsSPs.html).

[2] These crucial security tips are consistent with the top mitigations noted in the Australian Defence Signals Directorate's "Top 35 Mitigation Strategies" (www.dsd.gov.au/infosec/top35mitigationstrategies.htm).

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

[4] For information on using SCAP, see NIST Special Publication 800-117: "Guide to Adopting and Using the Security Content Automation Protocol (SCAP)" (Available at http://csrc.nist.gov/publications/PubsSPs.html).


The Manageable Network Plan
Audit Strategy
Configuration and Change Management
Network Security Monitoring
Remote Access Security
Log Management
Virus Scanners and HIPS
Incident Response and Disaster Recovery Plans
Security Gateways, Proxies, and Firewalls
Network Access Protection/Control
Data-at-Rest Protection
Personal Electronic Device Management
Executable Content Restrictions
Training
Backup Strategy
Security Policy
Milestone 5: Control Your Network (User Access)
Milestone 6: Manage Your Network I (Patch Management)
Milestone 7: Manage Your Network II (Baseline Management)
Milestone 8: Document Your Network
Milestone 2: Map Your Network
Milestone 3: Protect Your Network (Network Architecture)
Milestone 4: Reach Your Network (Device Accessibility)
Milestone 1: Prepare to Document
Ease network management
Safeguard operations
Stop unauthorized access
Protect against malware
Prevent data loss
Ensure availability
Save headaches, time, and money!
Build a Wall Protecting Your Network from Adversaries!
Network Monitoring and Control
Host-Based Security
Business Functionality
Network Security Tasks
Plan Milestones

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. (This does not mean *do* all the documentation here—just set up a way to do it.)
  - Suggestion: Use a blog or bulletin board to notify admins of changes, and a wiki to document information. A common issue occurs 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

- **Ease of use.** Doing documentation should be quick and painless, otherwise it will never get done. Make sure your documentation approach is easy to use.
- **Purpose.** 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.
  - Consider: 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?
- **Sufficient level of detail.** Someday you will need to consult your documentation to rollback an unwanted change to a device, or to rebuild a device that had a catastrophic failure. Does your documentation approach support recording information at this level of detail? Do your admins realize that they need to document to this level of detail, and include not only the *what* but also the *why* of changes?
  - Suggestion: Before making changes to a device's configuration, save off the current configuration file. Then if the changes don't work properly, it's easier to rollback to a working version.
  - Consider: It's not the mundane, day-to-day things that are so important to document; it's the trouble spots, weird fixes, chain reactions due to unexpected dependencies, command line parameters, installation procedures, etc.
- **Timestamps.** Does your documentation approach ensure that everything has a timestamp, so you know when it was last valid? (Yes, this includes even the sticky notes!)
- **Backing up.** Having good documentation assists in disaster recovery. Is your documentation repository backed up on a regular basis?
- **Protection.** 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) and encrypted?
  - Suggestion: Never store non-temporary passwords on the network or send them in an e-mail. A network intruder can find them and use them to further compromise your network.
- **Hard copy.** 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.
  - Consider: Besides protecting your on-line documentation, it is also important to protect the hard copy version (limit number of copies, keep in secure area, shred old versions, etc.).

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 (or provide reference to) 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 points to consider for this Milestone?

Checklist date:

Milestone 2: Map Your Network

In order to have any sort of control over your network, you first need to know where everything is. This milestone and the next focus primarily on gathering information about your network (although the points to consider may prompt you to investigate making network changes). Note that, depending on your network, it may be easier to implement Milestones 2 through 5 first for the infrastructure and then for the endpoint devices, instead of trying to do everything at once.

CAG[5] Critical Control:
1

To Do

- Create an accurate map of your current network (network topology). Be sure this network map is stored in a way that is secure, but yet still allows easy updates as network changes occur.
  - Suggestion: If you have any devices connected by wireless, they should be included on the map. Connections to any clouds, external networks, and the Internet should also be included on the map.
- 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 or firmware. (Your organization may require recording additional information.)
  - Suggestion: Store this information in a database. Applications can be written to query this database and automate many tasks. Be sure to properly secure this database!
  - Suggestion: Make use of tools (such as Nmap and/or arpwatch) to discover your network devices, but do not rely on them to discover ALL your devices. A room-to-room walkthrough of your organization will probably be required, so that no devices are overlooked.
    - For more information on the network security scanner Nmap, see http://nmap.org.
    - For more information on arpwatch, for tracking MAC-IP address pairings, see http://ee.lbl.gov.
  - Consider: An alternate way to gather this information is to require users to register their devices in order to obtain an IP address on your network. Consider using an application like NetReg (http://netreg.sourceforge.net; Carnegie Mellon's version: www.net.cmu.edu/netreg) or a commercial IP Address Management (IPAM) solution.
- Create a list of ALL protocols that are running your network.
  - Suggestion: Three possible ways to do this are: 1) Use Wireshark, tcpdump, and/or WinDump to figure out what is currently running on your network (you may also be able to get this information directly from your routers); 2) Allow traffic with only specific protocols and ports through your firewalls and see what breaks; or 3) Read the documentation on all your network applications to determine what *should* be running on your network.
    - For more information on the network protocol analyzer Wireshark, see www.wireshark.org.
    - For more information on the network packet analyzer tcpdump, see www.tcpdump.org.
    - For more information on the Windows port of tcpdump, WinDump, see www.winpcap.org/windump.

Consider

- **Physical routes.** If you are using a Virtual Local Area Network (VLAN), have you recorded the possible *physical* routes that your VLAN traffic traverses? This is important to know so that if, for example, you take a router down for maintenance, you can be sure that it won't accidentally bring down your virtual network.
- **Asset responsibility.** 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 and stored securely? Consider recording it in the device list created in this Milestone.
- **No unapproved devices and protocols.** Any devices or protocols on your network that you have not approved should be removed.

[5] For more information on the SANS Consensus Audit Guidelines (CAG), see www.sans.org/cag.

- **Asset management.** The ideal way to keep track of all the devices on your network is to implement a formal IT inventory (or asset) management process. Such a process can help you keep track of devices all the way from request and procurement to disposal.

Ongoing

- Update the network map and list of devices any time a device is added to or removed from your network.
- Update the list of protocols any time a new protocol is added to your network, or an old protocol is no longer used.
- Periodically use the tools mentioned above to check your network map and your lists of devices and protocols for accuracy. Remember, the tools won't find everything, but they may find things that were added to the network without your knowledge.

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) 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, role, MAC address, service tag, physical location, and OS/firmware?
				Do you have a current, accurate list of ALL protocols that are running on your network?
				Are you currently updating your network map and lists of devices and protocols whenever a change is made to your network?
				Have you gone over the points to consider for this Milestone?

Checklist date:

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.

CAG Critical Controls:
19; 1, 6, 11, 13, 15, 20

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 HR 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? What *functionality* is absolutely required? The machines where this data resides (for example, your servers) and where this functionality is implemented (for example, your domain controllers) are your high-value assets—your "crown jewels".
- Identify the choke points on your network. A choke point is a location which allows access between different "sections" of your network, such as sections with different trust levels, or your different enclaves. Ideally, all traffic between these sections should flow over a relatively small number of choke points. Especially be sure to identify the choke points on the "edge," i.e., the points of access into your network.

How to Identify Your High-Value Network Assets

1. Identify the products your organization produces.
2. Understand your production process.
3. Identify your high-value network assets:
   - **Any machine** involved in your production process that cannot be easily replaced in a timely manner.
   - **Any machine** that holds data important to your production process, where that data cannot be easily restored in a timely manner from a *recent* backup.
   - **Any machine** that EVER comes in contact with sensitive data, i.e., data that would cause your organization (or other people or organizations that rely on you) grave damage if a competitor or someone with malicious intent got access to it.

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

- **Damage containment.** Your network should be designed to keep any damage to it contained. A potential intruder should not have open access to everything on your network once he gets past the boundary defenses: loss of one network asset should not be loss of all. Users on your network may not need open access to all the information and assets on your network: only allowing access to sensitive information by those with a genuine need-to-know reduces the insider threat.
  - Suggestion: Your network enclaves should be separated so that valuable data is only available to those who need it. For example, Engineering should have access to the CAD drawings, but not the personnel files; and HR should have the opposite access. 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).
    - For guidance on isolating assets based on security dependencies (specific to a Windows network, but the general principles apply to any network), see *Microsoft Windows Server 2008 Security Resource Kit* by Jesper Johansson (Microsoft Press, © 2008), Chapter 13 ("Securing the Network").
    - Keep your network architecture as simple as possible. Simpler networks are easier to manage.
  - Suggestion: Consider the following separations to help limit damage in case of compromise:
    - Isolate your wired and your wireless networks, either physically or logically.
    - Isolate your VoIP and your data networks, either physically or logically.

    - Separate network assets that contain different sensitivities of information. If this can't be done physically, consider using VLANs and/or IPsec Encapsulating Security Payload (ESP).
    - Keep internal administrative functions, internal user functions, and external user functions separate: Physically separate server functions onto different servers—for example, a domain controller should not also be running a customer database. In addition, your servers should never be used as workstations.
  - Suggestion: Your network will have trust boundaries between machines whose data you trust more and those whose data you trust less. The amount of control you have over the machines may determine these boundaries. At a minimum, there should be trust boundaries between your organization's internal network, the extended enterprise, and the Internet. This is the idea behind, for example, putting all your publicly-accessible assets into DMZs (demilitarized zones). There should also be a trust boundary between your internal network and your remote access users, and there may be trust boundaries between your enclaves. Consider drawing these trust boundaries on your network map from Milestone 2.
  - Suggestion: Be sure the choke points on your network are positioned to most effectively protect your high-value assets. Place security gateways, proxies, or firewalls at your network choke points so that traffic over them can be monitored and controlled (see the *Security Gateways, Proxies, and Firewalls* and *Network Security Monitoring* Network Security Tasks). Consider placing choke points at your other trust boundaries as well, and allowing only the approved protocols documented in Milestone 2 to go through. To decrease your attack surface, limit the number of Internet gateways/access points into your network.

Crucial Security Tip

  - Suggestion: Examine your network trust relationships—those within your internal network and also those you have with external networks—to determine whether they are really necessary for your organization's mission. Eliminate all those that are not needed. Trust relationships can be exploited by malicious intruders to gain access to your network. Traditional network defenses (e.g., firewalls, malware scanners, etc.) *cannot defend* your network against an exploited trust relationship!
  - Suggestion: Use penetration tests and Red Team exercises to test your damage containment.

- **Cloud computing.** If all or part of your network is integrated with "the cloud"—or you are considering such integration—be sure that you understand the benefits and risks involved.
  - Suggestion: For more information on the benefits and risks of cloud computing, see the following:
    - NIST Special Publication 800-146: "Cloud Computing Synopsis and Recommendations" (Available at http://csrc.nist.gov/publications/PubsSPs.html)
    - The Cloud Security Alliance's "Security Guidance for Critical Areas of Focus in Cloud Computing" (Available at https://cloudsecurityalliance.org/research/security-guidance)
- **Virtualization security.** If your network includes virtual servers and/or desktops—or you are considering using these—be sure that you understand the security implications. For more information, see NIST Special Publication 800-125: "Guide to Security for Full Virtualization Technologies" (Available at http://csrc.nist.gov/publications/PubsSPs.html).
  - Suggestion: Be sure to follow the configuration and hardening guidance from the vendor of your virtualization solution.
- **Physical security.** Physical security of your network assets is extremely important! If an adversary can *physically* touch your boxes, it won't matter how well you secure your data.
  - Suggestion: At the very least, implement some kind of monitored physical access control so that unauthorized individuals are not allowed near your high-value assets.
- **No single points of failure.** Are there any single points of failure for critical systems on your network? These should be eliminated. Think end-to-end when considering this. For example, is all your critical outgoing network traffic routed through only one physical cable? Even if you have multiple cables out, do they ever run together, such as through a single conduit under a river? Are both the main and backup power supplies on a critical server plugged into the same UPS? Etc.
  - Suggestion: Regularly test your failover equipment and scenarios.

- **Custom Web applications.** Do you have custom Web applications facing the Internet? If so, are they protected and/or are your developers trained in writing secure, robust, and fault-tolerant code?
  - Suggestion: Use the Open Web Application Security Project (OWASP) resources for secure Web application development:
    - Secure Web application development guide (www.owasp.org/index.php/Category:OWASP_Guide_Project)
    - Web application testing guide (www.owasp.org/index.php/Category:OWASP_Testing_Project)
    - Developing your own security controls can lead to wasted time and security holes. Use the OWASP Enterprise Security API (ESAPI) toolkits (www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API).
    - The best place to defend a Web application from malicious activity may be within the application itself. Consider using the OWASP AppSensor framework (www.owasp.org/index.php/Category:OWASP_AppSensor_Project).
- **Legacy systems.** Do you have legacy systems and software that your organization depends on? If so, are they protected from more modern attacks and other misuse? If they ever get compromised, is the rest of your network protected from *them?*
  - Suggestion: Put your legacy systems on a separate network and access them through a custom Web service that appropriately sanitizes all input and output.
  - Suggestion: For guidance on migrating legacy systems, see "DoD Legacy System Migration Guidelines" (www.sei.cmu.edu/library/abstracts/reports/99tn013.cfm).
- **Risk assessment.** 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.
  - Suggestion: For more information on risk assessment and risk management, see the following:
    - NIST Special Publication 800-30: "Guide for Conducting Risk Assessments" (Available at http://csrc.nist.gov/publications/PubsSPs.html)
    - ISO 31000:2009 - "Risk Management – Principles and Guidelines" (Available at www.iso.org)

Ongoing

- Update the documentation whenever your network enclaves, high-value assets, choke points, or system dependencies change (added, removed, or relocated).
- Re-evaluate your network architecture periodically. Your security and manageability requirements may change, especially as your organization grows.

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) 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?
				Are you periodically re-evaluating your network architecture to make sure it most effectively protects your high-value assets, limits access to sensitive information, and keeps damage contained?
				Have you gone over the points to consider for this Milestone?

Checklist date:

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 in a secure manner.
  - Suggestion: For Windows machines, implement Active Directory.
  - Suggestion: Windows Group Policy is a powerful way to securely configure and administer the machines in a Windows network domain. For more information on Windows Group Policy, see *Group Policy: Fundamentals, Security, and Troubleshooting* by Jeremy Moskowitz (Addison-Wesley, © 2008).
  - Suggestion: To configure and administer non-Windows machines on your network, consider using Puppet. For more information on Puppet, see www.puppetlabs.com.
- For any devices that cannot be accessed on a regular basis, such as laptops and other mobile devices, develop a plan to administer them. Consider using a network access control solution (see the *Network Access Protection/Control* Network Security Task).
  - Suggestion: If a user is allowed full administrative control of such a device, the device should be wiped and reimaged before it is allowed back on the network.

Documentation

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

Consider

- **No insecure administration protocols.** Do not use insecure, clear-text protocols (telnet, rsh, ftp, tftp, etc.) to administer devices. Use SSH instead of telnet or rsh. Use SCP or SFTP instead of ftp. If using SNMP, use SNMPv3 and its security features (versions 1 and 2 are insecure).
  - Suggestion: On Windows machines, use the PuTTY SSH client and the WinSCP SFTP client. SSH and SFTP capabilities are included natively on Linux/Unix.
    - For more information on PuTTY, see www.chiark.greenend.org.uk/~sgtatham/putty.
    - For more information on WinSCP, see http://winscp.net.
  - Suggestion: Block the insecure protocols mentioned above on your network, in order to prevent malware from misusing them.
- **No unacceptable security dependencies.** A critical device should never be administered from a less critical device, because this makes the security of the critical device dependant on the security of the less critical device. For example, a domain controller should never be administered from an Internet-connected workstation. Consider using dedicated management stations for administering critical devices.
- **Remote administration.** 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! (See the *Remote Access Security* Network Security Task.)
- **Physical security.** Not just anyone should be able to walk up and access your network devices in an administrative mode. Do you have some sort of physical access control in place to prevent this? Do your admins know to close a device's administrative interface when they walk away from it?
- **Automating administration.** Automating administrative tasks frees up network administrator time. Is as much administration as possible done in an automated way?
- **Same administrative tools.** The way the devices on your network are administered should be standardized. Do all your network administrators use the same tools?

Ongoing

- Update the documentation whenever your device administration plan changes.

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) 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 points to consider for this Milestone?

Checklist date:

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.

CAG Critical Controls: **12, 16**

To Do

- Establish non-privileged user accounts for all normal users: normal users should never have administrative privileges.
  - Consider: Not everyone will be able to be a normal user, but limit the number of users with administrative privileges to an absolute minimum.
    - If a user only requires privileged access to certain directories or applications, use Windows Group Policy to grant that access instead of giving the user local admin privilege. If a user does require full local admin privilege, consider only allowing that privilege for a limited time or isolating any system on which that privilege is given.
    - 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). Alternatively, consider using an application to granularly elevate user privileges.

Documentation

- For any user that does require local admin privilege, document the machine(s) it is given on (perhaps in the device list from Milestone 2) and the reasons for it.

Consider

Crucial Security Tip

- **No Internet or e-mail from privileged accounts.** Letting users with local admin, root, or other elevated privileges surf the Internet or read e-mail is a VERY serious security risk! Malicious websites and e-mail attachments can make use of those elevated privileges to install malware on the network. Network administrators and other high-privileged users should not be allowed to access the Internet or e-mail from their privileged accounts. For suggestions on how to enforce this, see the "Enforcing No Internet or E-mail from Privileged Accounts" NSA Fact Sheet (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).
- **Segregate admin roles.** Administrative accounts at any level should only be used to administer computers at that level. For example, a domain admin account should only be used for administering the domain; it should not also be used for administering servers and workstations—separate admin accounts should be used for that (and these separate admin accounts need to have different passwords!). Segregating admin privileges in this way makes it much more difficult for an attacker who takes over one machine to then compromise the whole domain.
- **Users installing software.** Users with non-privileged accounts will not be able to install software. This is good from a security standpoint, but how will you handle those users who do actually *need* to install software? How will you handle your developers who write code and run arbitrary things?
- **No "entitlement."** Employees may need to be reminded that they are not "entitled" to have unfiltered Internet access and install whatever software they want on their workstations. After all, they do not own "their" workstations; the company does. Enforcing these restrictions will go far in making your network more manageable!
- **Expiration dates on accounts.** Consider setting expiration dates (quarterly or yearly) on all user accounts, so that unused accounts will be automatically disabled.
- **Hiring consideration.** Anyone with full administrative privileges on your network will have access to all its data. Are those individuals properly vetted in your hiring process? Are they periodically reinvestigated?
- **Disable account when employee leaves.** When an employee leaves your organization, is his or her account(s) disabled?

Ongoing

- For each of your users that has elevated privileges, regularly review the reasons for this. When the reasons are no longer valid or no longer justifiable, remove the privileges.

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) 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 points to consider for this Milestone?

Checklist date:

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 specific implementations will differ for different device roles and operating systems.

CAG Critical Control: **4**

To Do

- Establish a patch management process for ALL the operating system and application software on all the workstations, servers, and network infrastructure devices (e.g., routers, firewalls, etc.) on your network.
  - Suggestion: Prioritize your patch management. All of your systems should be patched regularly, but those systems and applications that handle data from untrusted sources (such as the Internet) must be patched more often. In addition, critical patches must be applied whenever they are released. The sensitivity and criticality of certain systems may warrant exceptions, however. If you make exceptions, be sure that those systems are isolated as much as possible and monitored closely for signs of known attacks.
  - Consider: Patching your laptops and other mobile devices may be difficult, because they may not be regularly connected to your network. The plan to administer these devices (developed in Milestone 4) should include regular patching. Alternatively, consider using a network access control solution, to make sure that these devices are up to date before being allowed access to your network resources (see the *Network Access Protection/Control* Network Security Task).
  - Suggestion: As much as possible, patching should be automatic. Remember that a reboot may be required for a patch to be properly applied. Be careful patching your servers, however, 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) or an automated commercial solution. Windows workstations should be set to automatically apply patches. For operating systems other than Windows, consider using Puppet, Spacewalk, or custom scripts.
    - For more information on WSUS, see http://technet.microsoft.com/en-us/wsus/default.
    - For more information on Puppet, see www.puppetlabs.com.
    - For more information on Spacewalk, see http://spacewalk.redhat.com.
    - For patch management solution suggestions from actual users, see the SANS WhatWorks website (www.sans.org/whatworks), section 4.4 Patch and Security Configuration Management and Compliance.[6]
  - Suggestion: Review after patching your systems, to verify that the patches were applied correctly. As a sanity check, use different tools than those used for pushing out the patches.
  - Suggestion: For additional recommendations on patch management, see NIST Special Publication 800-40: "Creating a Patch and Vulnerability Management Program" (Available at http://csrc.nist.gov/publications/PubsSPs.html).

Documentation

- Document your patch management process. Consider documenting it in the device list from Milestone 2. For each device (or group of identical devices), include:
  - How often (on what schedule) patches should be applied
  - How patches are downloaded, verified, and tested
  - How the patches are applied (automatically or manually)
  - The procedures if any patches need to be applied manually
  - How the patch application is verified
  - Each specific system that warrants an exception from the patch management process, the reasons for the exception, and how this vulnerability of an unpatched system is being mitigated.

[6] Note that the products mentioned have not been evaluated by the NSA and might not be approved for use in your organization.

Consider

Crucial Security Tip

- **Non-Microsoft updates.** How will you update and patch non-Microsoft applications, such as Adobe Acrobat? What about device drivers and Web browser plug-ins? These unpatched third-party applications, etc. are a huge attack vector for malware.
  - Suggestion: In order to know when new releases become available for your approved non-Microsoft applications, have a generic e-mail alias that maps to all the admins and subscribe to release announcements for those applications.
  - Suggestion: WSUS can also be used to patch third-party applications. See www.windowsitpro.com/article/patch-management/Secure-non-Microsoft-applications-by-publishing-3rd-party-updates-to-WSUS.aspx.
- **No end-of-life software/hardware.** 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.

Ongoing

- Continue to execute the patch management process that you established in this Milestone.
- As necessary, update your patch management process and documentation.

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) 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 process for ALL the OS and application software on your **workstations** (including laptops and other mobile devices)?
				Have you established and documented a patch management process for ALL the OS and application software on your **servers**?
				Have you established and documented a patch management process for ALL the OS and application software on your **network infrastructure devices**?
				Have you gone over the points to consider for this Milestone?

Checklist date:

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

To Do

CAG Critical Controls:
2, 3, 6, 10; 12

- 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. Consider how much you trust the application's developer to deliver a product with a minimum of vulnerabilities. In addition, consider whether the application conflicts with any of your existing security policies, and how easily it can be 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 process from Milestone 6 will need to be updated appropriately.
  - Suggestion: Implement restrictions so that only those applications that have been approved are allowed to execute on your network. Consider using application whitelisting (see the *Executable Content Restrictions* Network Security Task).
- Create device (workstation, server, router, etc.) baselines. All software applications in a device baseline should be from the approved list for that device. Note that virtual machines and thin clients need baselines as well.
  - Suggestion: If similar devices are used in environments that require different capabilities or pose different threats, the devices should have different baselines. For example, the workstations used by developers should have a different baseline than those used by managers, because the managers will most likely not require all the applications and privileges that the developers will. Having more "special purpose" machines and less "general" machines will limit the damage that can be done if a machine is compromised.
  - Suggestion: When creating your device baselines, be sure to implement the recommended security guidance for those devices. All software included in the baselines should be fully patched and correctly and securely configured. Remove unneeded components from default installs, disable unnecessary services, remove default passwords, limit the number of cached credentials, implement screen lock timeouts, disable Windows auto-run, etc. Be sure that your patch management process from Milestone 6 covers all the software in your baselines.
    - **Securing Web browsers.** Properly securing the Web browsers in your workstation baselines is extremely important: the Internet can be a dangerous place! For suggestions on securing Web browsers, see www.us-cert.gov/reading_room/securing_browser. For Internet Explorer, especially note the guidance on Security Zones. For Firefox, strongly consider using the NoScript add-on that is mentioned. In addition, consider minimizing the number of plug-ins in the browser, as these might contain security vulnerabilities.
    - The Microsoft Baseline Security Analyzer (MBSA) can be used to scan for security misconfigurations in your Microsoft baselines before deploying them. For more information on MBSA, see http://technet.microsoft.com/en-us/security/cc184924.aspx.
    - The Center for Internet Security (http://cisecurity.org) provides benchmarks and tools for checking that your operating systems, applications, and devices (including Windows, Linux, Solaris, Apple, Oracle, Cisco, etc.) are configured securely.
    - For additional configuration guidance, see the following:
      - NSA configuration guides (www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml)
      - NIST National Checklist Program (http://web.nvd.nist.gov/view/ncp/information)
      - DISA Security Technical Implementation Guides (STIGs) (http://iase.disa.mil/stigs/index.html)

Documentation

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

Consider

- **Backing up offline.** Backup your baselines and store them offline. An adversary who gains access to network copies of your baselines may modify them.
- **Same password problem.** If you use an application such as Norton Ghost to baseline your machines, keep in mind that every machine baselined this way will have the same local administrator/root account *and password*. Without ever having to crack the password, an attacker using a pass-the-hash technique could use the same password *hash* to compromise all your machines. If you consider this risk of compromise to be greater than the administrative overhead, either disable the local admin accounts or manually change all the passwords.
  - If you manually change all the passwords, *do not* store them in a file or e-mail on the network! Instead, use a simple algorithm to generate each password. For example, append the last few characters of the machine name to the original common password. This way your admins know all the passwords, but the password hashes are different across all your machines. This makes the pass-the-hash attack ineffective. It is not a foolproof solution, but it is better than all of your machines having the same password!
  - For more information and a tool to help with this on a Windows network, see *Protect Your Windows Network* by Johansson and Riley (Addison-Wesley, © 2005), p. 226-228 and Appendix D. This book is also a good general reference for securing a Windows network.
- **Hardware configurations.** Do the baselines for your devices also include their hardware configurations? Some things to consider in this area might be disabling wireless cards, setting the boot order in the BIOS to hard drive only, and creating BIOS passwords. In addition, make sure that your systems support signed BIOS updates (check with your vendor), to help prevent unauthorized BIOS modifications.
  - Suggestion: Limit your hardware based on the capabilities needed and the threats posed. For example, not all of your workstations may need USB ports, wireless capability, huge hard drives, powerful graphics cards, CD/DVD writers, etc. (As a bonus, this may reduce your power and cooling requirements!)
- **Reimaging devices.** Consider reimaging your devices on a regular basis (for example, 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. Be sure that any host-based security still performs properly on the reimaged devices.
- **Automatic reboots.** Consider setting your workstations to automatically reboot on a regular basis (for example, 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.

Ongoing

- Update the device baselines on a regular basis. As far as possible, baselines should contain the latest versions of operating system and application software. Baselines should never contain software or hardware that is end-of-life and no longer supported.
- Update approved application lists, criteria and process for getting an application on the approved list, and baselines documentation whenever they change.
- From now on, whenever a device is added or replaced on your network, the new device should conform to the appropriate baseline. If the device cannot be wiped and re-baselined, consider a network access control solution (see the *Network Access Protection/Control* Network Security Task), or quarantining the device.
- As time permits, any installed applications and services 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 (or provide reference to) 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 baselines (workstation, server, router, etc.)?
				Are you currently, whenever a device is added or replaced on your network, making sure the new device conforms to the appropriate baseline?
				Have you gone over the points to consider for this Milestone?

Checklist date:

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! Be sure to give priority to documenting those things that are most important to keeping your organization doing business.

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, four very important procedures to document are:
  - How to add a new user
  - How (and when) to remove a user
  - How to add a new system
  - How to remove a system

Consider

- **Completeness.** 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? To test if you've thought of everything, have that admin go on vacation…
- **Hard copy.** Keep hard copies of your processes and procedures on hand, in case of emergencies. Keep duplicate copies at your continuity of operations site, in case of more serious emergencies.
- **Always followed.** The documented procedures should always be followed. Are they? Are new network admins required to become familiar with and use this documentation?

Ongoing

- As time permits, continue to document your administrative processes and procedures.
- All documentation must be reviewed periodically (for example, annually) and updated as necessary. Consider occasionally hiring a technical writer to gather, clarify, and maintain your documentation.

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) 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 and systems 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 points to consider for this Milestone?

Checklist date:

And Now…

Congratulations! You now have a manageable network!

Ongoing

To recap, here are the ongoing tasks you should now be doing on your network. Look for cost-effective ways to automate these!

- 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
- For each of your users that has elevated privileges, regularly reviewing the reasons for this and removing the privileges when the reasons are no longer valid or no longer justifiable
- Continuing to execute your patch management process
- As necessary, updating your patch management process and documentation
- Updating device baselines on a regular basis
- Updating approved application lists, criteria and process for getting an application on the approved list, and baselines documentation whenever they change
- Whenever a device is added or replaced on your network, making sure the new device conforms to the appropriate baseline
- As time permits, removing any installed applications and services that are not approved
- As time permits, reimaging current devices with the appropriate baseline.
- As time permits, documenting all administrative processes and procedures
- Periodically using discovery tools to check your network map and your lists of devices and protocols for accuracy.
- Re-evaluating your network architecture periodically, to determine if it still meets your security and manageability requirements.
- Reviewing all documentation periodically and updating it as necessary

Documentation

Develop checklists (e.g., daily, monthly, yearly, etc.) to remind admins of activities that need to be carried out on a regular basis.

Consider

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

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, you will be able to consider and implement security measures—and verify their implementation—much more efficiently and effectively.

The following are security-related tasks to consider implementing on your network once it is manageable. 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 in sufficient detail. 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 your 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

CAG Critical Control: **8**

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!

- Suggestion: Encrypt your backups to prevent compromise of your data.

Incident Response and Disaster Recovery Plans

CAG Critical Control: **18**

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

- Consider: If your organization does not have the skills, resources, or time to do a good job of cleaning up your network after a security incident, call in the professionals! Doing a poor job of eradicating an intrusion and then having to spend more money to fix the mess is much worse than spending the little extra to get it done right the first time. An important part of your incident response plan should be to define which types of incidents you can handle yourself and which types you cannot.
- 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").
- Suggestion: For some considerations on remediation, see http://blog.mandiant.com/archives/1525.[7]
- Suggestion: For additional recommendations on incident response, see the following NIST Special Publications (Available at http://csrc.nist.gov/publications/PubsSPs.html):
  - SP 800-61: "Computer Security Incident Handling Guide"
  - SP 800-83: "Guide to Malware Incident Prevention and Handling"
- Suggestion: For additional recommendations on contingency planning, see NIST Special Publication 800-34: "Contingency Planning Guide for Federal Information Systems" (Available at http://csrc.nist.gov/publications/PubsSPs.html).
- Consider: If your network is integrated with "the cloud", be sure you and your cloud provider(s) have agreements codified in contracts and SLAs on how to recognize and handle incidents and disasters.

[7] The NSA makes no endorsement of the services offered by this company.

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. 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 include the following sections:
  - *Acceptable Use Policy,* defining how the organization's computer equipment and network resources are to be used
  - *Privacy Policy,* specifying employee expectations of privacy regarding monitoring of email, keystrokes, and access to their files
  - Depending on your organization's security posture, other policy sections that may be important for your network include an Access Policy that specifies allowed access to network resources and allowed connections to other networks and devices; an Accountability Policy that specifies responsibilities of employees and how incidents will be handled; a Password Policy; Purchasing and Disposal Guidelines; etc.
  - *User Agreement,* which employees must sign, stating that they agree to comply with the security policy
- Suggestion: For more information on security policy development and implementation, see the SANS Security Policy Project website (www.sans.org/security-resources/policies).
- 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

CAG Critical Controls: **9**; 18

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 *current* security policy?
- Consider: If there is a security breach, your users may notice odd things happening on their computers and the network long before the admins do. Do your users know to report these things? Do they know *how* (where and to whom) to report these things?
- Suggestion: The Defense Information Systems Agency (DISA) has many training courses available for free on a variety of Information Assurance topics. These courses are available on CD and/or online. For more information, see http://iase.disa.mil/eta/online-catalog.html.
- Suggestion: For additional recommendations on training, see NIST ITL Bulletin October 2003: "Information Technology Security Awareness, Training, Education, and Certification" (Available at http://csrc.nist.gov/publications/PubsITLSB.html). As appropriate, also see the following NIST Special Publications (Available at http://csrc.nist.gov/publications/PubsSPs.html):
  - SP 800-16: "Information Technology Security Training Requirements: A Role- and Performance-Based Model"
  - SP 800-50: "Building an Information Technology Security Awareness and Training Program"

Host-Based Security Tasks

Executable Content Restrictions

CAG Critical Control: 2

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, as this may compromise your network.

Crucial Security Tip

- Suggestion: Unapproved applications (those not in your baselines from Milestone 7) should not be allowed to run. This can be enforced through application whitelisting, using Windows Software Restriction Policies (SRP), Windows AppLocker, or a commercial solution.
  - For more information on using SRP for application whitelisting, see the "Application Whitelisting Using Software Restriction Policies" guide (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml).
  - Windows AppLocker is the new version of SRP for Windows 7 and Windows Server 2008 R2, with a better implementation, new features, and more flexibility. SRP is still supported for backwards compatibility; for example, if you have a mixed network of XP, Vista, and Windows 7, then you can set up SRP rules and all three OS versions will enforce them. For more information on AppLocker, see http://technet.microsoft.com/en-us/library/dd548340(WS.10).aspx.
  - On Linux/Unix, execution restrictions can be enforced by mounting world-writable directories (e.g., /tmp) as separate partitions with the noexec option enabled. On Mac OS X, the Parental Controls can be used to prevent unapproved applications from launching.
- Suggestion: If an application becomes infected by malware, it must be prevented from doing things it should not be doing. Various techniques can be used to enforce this, first and foremost by having your users not run as administrator. Other techniques include Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), Linux mandatory access control technology (such as SELinux), and Unix chroot "jails". Host Intrusion Prevention Systems (HIPS) can also be used to enforce execution restrictions.
  - For more information on enabling DEP on Windows, Linux, Solaris, and Mac OS X, see the "Data Execution Prevention (DEP)" NSA Fact Sheet (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).
- Suggestion: Microsoft Office documents are often used to deliver malicious code. If you use Office, upgrade to Office 2007 or later, which uses the newer Open XML file formats. Office 2010 offers additional protection by opening documents from untrusted sources in a read-only isolated sandbox known as "Protected View".
  - If you cannot immediately upgrade to Office 2007 or later, use the Microsoft Office Isolated Conversion Environment (MOICE) to sanitize your Office documents when they are opened, before any malicious code can execute. For more information on implementing MOICE preprocessing of Office documents, see "The Microsoft Office Isolated Conversion Environment (MOICE) and File Block Functionality with Office 2003" NSA Fact Sheet (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).
- Suggestion: The Enhanced Mitigation Experience Toolkit (EMET) is a free Windows utility that helps prevent vulnerabilities in software from being exploited. EMET can be configured to protect *any* software running on Windows, no matter when or by whom it was written. For more information on EMET, see www.microsoft.com/download/en/details.aspx?id=1677. Note that EMET might prevent legitimate programs from working, so be sure to test before deploying.
- Suggestion: Consider accessing high-risk applications and files (Web browsers, e-mail clients, files downloaded from the Internet, etc.) in a virtual machine (VM). This can keep malware contained. If the VM becomes compromised, it can be reverted to a known good state and the host computer remains unaffected. However, note that if transferring files out of the VM is allowed, or the VM has network connectivity to unprotected hosts, then your network could still be compromised.

Virus Scanners and Host Intrusion Prevention Systems (HIPS)

*CAG Critical Control: **5***

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 HIPS must be kept up to date.

- Suggestion: A HIPS usually has an adaptive or "learning" mode to help ease its integration into your network defenses. This mode "learns" what network traffic normally flows to and from your hosts and automatically creates rules to allow that traffic. DO NOT leave the HIPS in this mode indefinitely! Otherwise, when a network attack happens, the HIPS will just automatically create a rule to allow it.
- Consider: A HIPS provides admins with great flexibility in securing their networks, but it is expensive, and time-consuming to configure and monitor. Roughly equivalent protection can be obtained by using the following four technologies on each host: 1) Host firewall; 2) Buffer overflow protection, such as DEP, mentioned above; 3) Program execution blocking, such as AppLocker or SRP, mentioned above; and 4) Virus scanner with real time protection ("guard") functionality enabled.

Personal Electronic Device (PED) Management

CAG Critical Controls: 5, 17

Without proper management of Personal Electronic Devices (USB drives, BlackBerry devices, iPhones, etc.), unauthorized devices will be connected to your operational systems. Data could be stolen, or malicious software 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 endpoint device control or endpoint data loss prevention (DLP) security application to do this enforcement automatically.
  - In Windows Vista and later, Group Policy can be used to do this enforcement. For more information, see http://msdn.microsoft.com/en-us/library/bb530324.aspx.
- Suggestion: Unless it is required, disable support for USB storage devices on your machines.
  - For more information on disabling support for USB drives in Windows, Linux, Solaris, and Mac OS X, see the "Disabling USB Storage Drives" NSA Fact Sheet (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).
- Suggestion: For iPhone and iPad security tips, see the "Security Tips for Personally-Managed Apple iPhones and iPads" NSA Fact Sheet (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml). For information on managing iOS devices in an enterprise, see www.apple.com/support/iphone/enterprise.
- Suggestion: Use a mobile device integrity solution to ensure that the mobile devices on your network are properly configured and secured, and that they have remained in a secure state without being compromised. For U.S. Government organizations, free tools are available at www.iad.gov, under Mitigations - Tools.
- Suggestion: For additional recommendations on Personal Electronic Device security, see NIST Special Publication 800-124: "Guidelines on Cell Phone and PDA Security" (Available at http://csrc.nist.gov/publications/PubsSPs.html).

Data-at-Rest Protection

CAG Critical Control: **17**

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.

- Consider: The best data-at-rest protection is to *not store* sensitive data in insecure places, or places where it will persist for a long time. Is it really necessary to send your sensitive information via e-mail? Is it really necessary to store your sensitive data on mobile devices?
- 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.
  - BitLocker Drive Encryption is included with Windows Vista Enterprise and Ultimate, and Windows Server 2008. For more information on configuring BitLocker, see the "How to Securely Configure Microsoft Windows Vista BitLocker" NSA Fact Sheet (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).
  - The U.S. Government has selected several companies to provide them with products to encrypt data-at-rest. For more information, see www.gsa.gov/portal/content/102647.
- Consider: Some mobile devices offer "self-destruct" (data wipe) capability if someone fails logging on to them too many times.
- Suggestion: For additional recommendations on data-at-rest protection, see NIST Special Publication 800-111: "Guide to Storage Encryption Technologies for End User Devices" (Available at http://csrc.nist.gov/publications/PubsSPs.html). Appendix A contains some alternatives to encryption.

Network Monitoring and Control Tasks

Network Access Protection/Control (NAP/NAC)

CAG Critical Control:
1, 5

When someone plugs a device into your network, that device should not automatically have access to everything. The device (and any users of the device) should only be allowed to access your network resources after a verification and authentication procedure.

- Suggestion: "Rogue" devices such as unauthorized wireless access points, laptops, or additional switches should be prevented from connecting to your network. Configure your network switches to only allow certain MAC addresses to connect to their physical ports (port-based authentication, or port security). For a more robust solution, consider implementing IEEE 802.1X, where client machines must authenticate at the network layer using certificates (which, unlike MAC addresses, generally cannot be spoofed).
  - For more information on implementing port security, see the "Port Security on Cisco Access Switches" NSA Fact Sheet (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).
- Suggestion: Devices that are misconfigured, behind in patches or malware scans, etc. should be prevented from accessing your network resources, because they may open up vulnerabilities on your internal network. Use a solution that assigns machines connected to your network to separate VLANs, based on initial (and even ongoing) health and configuration checks and policies that you set. On Windows, consider using Network Access Protection.
  - Network Access Protection is included with Windows Vista, Windows Server 2008, and Windows 7, and is also supported on Windows XP with Service Pack 3. For more information, see http://technet.microsoft.com/en-us/library/cc730902(WS.10).aspx.
  - For network access control solution suggestions from actual users, see the SANS WhatWorks website (www.sans.org/whatworks), section 3.2 Network Access Control.[8]
- Consider: If you have machines that have not been connected to the network for a period of time (such as laptops taken on business trips) and so have fallen behind with patches and configuration, you can use Windows Active Directory to prevent those machines from connecting to your internal network. Place each such machine into a "disabled" OU that has no access to internal network resources. The user of the machine will then have to call in and get his machine properly updated, after which the machine can be placed back into its proper OU.
- **User authentication.** Users must also be authenticated before they are allowed access to your network resources. Your network likely has an authentication mechanism in place already; however, your authentication process may not be as robust as it should be, or your authentication mechanism itself may be vulnerable to attack. For some suggestions on hardening this critical piece of your infrastructure, see the "Hardening Authentication" NSA Fact Sheet (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).

Security Gateways, Proxies, and Firewalls

CAG Critical Controls:
11, 13; 5, 6

Security gateways, proxies, and firewalls can examine traffic and provide a way to allow, deny, or modify the traffic between nodes. These devices 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.

- **White-listing vs. black-listing.** When generating rule sets for your gateways, proxies, firewalls, or any other type of access control, keep in mind that white-listing (specify trusted and deny everything else) is generally more effective than black-listing (specify untrusted and allow everything else). This is because it is impossible to list *everything* that's untrusted in your black list.
- 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 (for example, e-mails from outside that appear to originate from inside are blocked).
- Suggestion: Direct all your web traffic through a proxy or secure Web gateway; your workstations should never directly connect outside of your network. Consider blocking or restricting downloads there.

[8] Note that the products mentioned have not been evaluated by the NSA and might not be approved for use in your organization.

- Consider: For your firewalls, consider whether they should be simple packet-filtering, stateful inspection, or application-proxy firewalls. Besides doing ingress filtering, also do egress filtering: do not allow any traffic to leave from a workstation or server on your network that is not absolutely essential for that machine to fulfill its role. This can help contain attacks, as it will likely prevent any malware from "phoning home". Rate-limiting (throttling) can also be used to protect your network from (and keep it from contributing to) denial of service attacks.
  - For recommendations on configuring firewalls, see NIST Special Publication 800-41: "Guidelines on Firewalls and Firewall Policy" (Available at http://csrc.nist.gov/publications/PubsSPs.html).

Remote Access Security

CAG Critical Controls: **7**; 13, 14

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 quarantine, or subject them to increased monitoring. Remote access clients should never be allowed to connect directly to your internal network; they should connect to a DMZ (demilitarized zone) so they at least have to go through a firewall to get to the internal network. In addition, strong authentication should be enforced for remote access users. Consider using a network access control solution.
- Suggestion: Require users accessing your network remotely to use a Virtual Private Network (VPN) and to only access the network from company-owned machines. Require ALL traffic to go through the VPN; do not allow split-tunnels. All VPN traffic should be inspected (*after* it is decrypted) before it is allowed to interact with any of your network resources.
- Suggestion: Use secure wireless protocols. If you are using legacy wireless technology (IEEE 802.11a/b/g), move to IEEE 802.11i/WPA2: the legacy technology has serious security flaws. Authenticate your wireless users by using a TACACS+ or RADIUS server, or VPN solution.
  - For additional recommendations on wireless security, see the following NIST Special Publications (Available at http://csrc.nist.gov/publications/PubsSPs.html):
    - SP 800-48: "Guide to Securing Legacy IEEE 802.11 Wireless Networks"
    - SP 800-97: "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i"
    - SP 800-121: "Guide to Bluetooth Security".
- Suggestion: Regularly audit your remote access. Make sure that you know in general *who* is accessing your network *when* doing *what*, so you can spot any anomalous activity.
- Suggestion: For additional recommendations on remote access security, see the following NIST Special Publications (Available at http://csrc.nist.gov/publications/PubsSPs.html):
  - SP 800-46: "Guide to Enterprise Telework and Remote Access Security"
  - SP 800-114: "User's Guide to Securing External Devices for Telework and Remote Access"

Network Security Monitoring

CAG Critical Controls: 5, 13, 17

No matter how much time and effort you devote to preventing problems on your network, eventually something will go wrong. *Prevention eventually fails!* 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 ("baselining"), you will be able to detect anomalies. Your network security monitoring solution should be configurable and precise enough so that you can quickly adjust it to monitor select traffic more in depth if you suspect a problem or infection. Be sure you have a process in place for what to do when a problem is found.

Crucial Security Tip

- Suggestion: Read *The Tao of Network Security Monitoring* by Richard Bejtlich (Addison-Wesley, © 2005) and its sequel *Extrusion Detection* (Addison-Wesley, © 2006). Mr. Bejtlich advocates network security monitoring as the *first* step to take to secure a network (http://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html).[9]
- Suggestion: Consider implementing a system so that network administrators are automatically informed when anomalous events occur. But remember, an automated system *will not* detect all

[9] The NSA makes no endorsement of the services offered on this website.

anomalies! A team of experts (either internal, external, or in partnership with other organizations) must still conduct regular log reviews, looking for new problems and new attacks.

- Suggestion: Consider using a network intrusion detection/prevention system (IDS/IPS), such as Snort (www.snort.org). Note that for quick response—like when your network is under attack—preconfigured versions of Snort are available on live CD/DVD.
- 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

CAG Critical Control: **14**

Your logs (gateway, proxy, and firewall logs, router logs, IDS logs, DNS logs, host OS logs, virus scan and HIPS alerts, etc.) contain information that can help with troubleshooting, compliance, incident 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. Be sure you review your logs within a short enough time from when they were generated so as to be actually useful—it's no good first noticing malicious activity a year after it happened!

- Suggestion: Deploy a centralized logging solution. Consider using syslog, an application like Splunk (www.splunk.com) or Snare (www.intersectalliance.com), or a commercial Security Information and Event Management (SIEM) solution.
  - If your network includes virtual machines, be sure your log management solution supports retention of transient log data from virtual sessions, and event correlation and user attribution across virtual sessions.
  - For log management solution suggestions from actual users, see the SANS WhatWorks website (www.sans.org/whatworks), section 6.1 Log Management and Security Information and Event Management.[10]
- 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 network administrators are automatically informed when anomalous events occur. But remember, an automated system *will not* detect all anomalies! Regular log reviews will still be necessary.
- Suggestion: For suggestions on what to look for in logs, see the "Critical Log Review Checklist for Security Incidents" (www.sans.org/security-training/course_sums/1217.pdf). Note especially the following:
  - *Windows OS, Object access denied:* If you have restricted access to your important directories and files, denied accesses to those are suspicious (auditing must be turned on).
  - *Network Devices, Bytes transferred:* Large byte transfers to or from unexpected machines or at unexpected times are suspicious.
  - *Network Devices, Administrator access:* Admin accesses from unexpected accounts (non-person service accounts, the Guest account, etc.) or at unexpected times are suspicious.
  - *Web Servers, Error code 200 on files that are not yours:* Successful (status code 200) GETs or POSTs of files that you don't recognize are suspicious—especially if they are large (bytes transferred is a large number) and/or compressed (file extension is .zip, .rar, .tar.gz, .tgz, .sit, etc.). This may indicate that your data is being exfiltrated.
  - *An additional suggestion (not on the checklist) for Database Servers:* High privilege actions (running stored procedures, creating or destroying links, etc.) that are unexpected are suspicious. Note that auditing must be turned on; most databases do *not* have auditing on by default.
- Suggestion: For additional recommendations on log management, including details on syslog, see NIST Special Publication 800-92: "Guide to Computer Security Log Management" (Available at http://csrc.nist.gov/publications/PubsSPs.html).

[10] Note that the products mentioned have not been evaluated by the NSA and might not be approved for use in your organization.

Configuration and Change Management

CAG Critical Controls:
3, 10

To better control your network and to keep it reliable and stable as it is upgraded and expanded, your organization may want to create a formal configuration and change management process. This process establishes review of changes before they are made, as well as backup of configurations so that any changes that break things can be quickly undone. (Note that the milestones of the Manageable Network Plan already established rudimentary configuration and change management; this Network Security Task is about *formalizing* the process.)

- Suggestion: For information on developing a formal configuration and change management process, see "The Definitive Guide to Enterprise Network Configuration and Change Management" (http://nexus.realtimepublishers.com/dgenccm.php).
- Suggestion: For additional information, see the "Service Transition" volume of the IT Infrastructure Library (ITIL), and the Change and Configuration Service Management Function (SMF) of the Microsoft Operations Framework (MOF). The complete ITIL and MOF are both good general "best practice" lifecycle frameworks for delivering quality IT services.
  - IT Infrastructure Library (ITIL) (www.itil-officialsite.com/Publications/Core.asp)
  - Microsoft Operations Framework (MOF) (http://technet.microsoft.com/en-us/solutionaccelerators/dd320379.aspx)
- Suggestion: For recommendations on configuration management with a focus on information security and using the Security Content Automation Protocol (SCAP), see NIST Special Publication 800-128: "Guide for Security-Focused Configuration Management of Information Systems" (Available at http://csrc.nist.gov/publications/PubsSPs.html).
- Consider: For another approach to getting a network under control, based on ITIL and change management, see *The Visible Ops Handbook* by Behr, Kim, and Spafford (IT Process Institute, © 2004).

Audit Strategy

CAG Critical Controls:
All

To verify that everything is working, that your network is in compliance with your security policy, and 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 all the protocols and applications currently running on your network are approved, and gather metrics about your network. Your audit strategy should address *what* gets audited, *when* it gets audited, *what* you're looking for, and *what* you're going to do (based on risk considerations) if you find something non-compliant.

- Suggestion: Consider using a network vulnerability scanner and/or a Security Content Automation Protocol (SCAP) validated tool (http://nvd.nist.gov/scapproducts.cfm).
- Suggestion: Consider at least gathering the following information:
  - How many total devices/hosts are on your network? How many of these currently cannot be contacted by the administrator? How many currently do not comply with your documented baselines? How many currently are running unapproved applications? How many currently are not fully patched?
  - How many total user accounts exist on your network? How many of these are old, unused, or disabled (and perhaps unauthorized) accounts? How many currently have incorrect privileges? How many currently have weak passwords?
  - Do you have any unauthorized "rogue" wireless access points? (Check by warwalking/driving.) Do you have any rogue wired access points, such as modems?
- Suggestion: Read *Security Metrics* by Andrew Jaquith (Addison-Wesley, © 2007).
- Suggestion: Consider using the Microsoft Security Assessment Tool (MSAT). The MSAT assesses your network based on your responses to questions, and provides recommendations based on accepted best practices and standards (http://technet.microsoft.com/en-us/security/cc185712.aspx).
- Suggestion: For additional recommendations on information security measurement, see NIST Special Publication 800-55: "Performance Measurement Guide for Information Security" (Available at http://csrc.nist.gov/publications/PubsSPs.html).
- Suggestion: Have a yearly independent audit of your network done by a well-known provider.

Quick Reference

Readings Mentioned

NIST Special Publications are available at http://csrc.nist.gov/publications/PubsSPs.html.
NSA Fact Sheets are available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml.

Introduction

- NIST Special Publication 800-39: "Managing Information Security Risk: Organization, Mission, and Information System View"
- "Top 35 Mitigation Strategies" (www.dsd.gov.au/infosec/top35mitigationstrategies.htm)
- NIST Special Publication 800-117: "Guide to Adopting and Using the Security Content Automation Protocol (SCAP)"
- Consensus Audit Guidelines (CAG) (www.sans.org/cag)

Network Architecture (Milestone 3)

- *Top-Down Network Design, Second Edition* by Priscilla Oppenheimer (Cisco Press, © 2004)
- *Microsoft Windows Server 2008 Security Resource Kit* by Jesper Johansson (Microsoft Press, © 2008)
- NIST Special Publication 800-146: "Cloud Computing Synopsis and Recommendations"
- "Security Guidance for Critical Areas of Focus in Cloud Computing" (https://cloudsecurityalliance.org/research/security-guidance)
- NIST Special Publication 800-125: "Guide to Security for Full Virtualization Technologies"
- OWASP secure Web app development guide (www.owasp.org/index.php/Category:OWASP_Guide_Project)
- OWASP Web app testing guide (www.owasp.org/index.php/Category:OWASP_Testing_Project)
- OWASP Enterprise Security API (ESAPI) (www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API)
- OWASP AppSensor (www.owasp.org/index.php/Category:OWASP_AppSensor_Project)
- "DoD Legacy System Migration Guidelines" (www.sei.cmu.edu/library/abstracts/reports/99tn013.cfm)
- NIST Special Publication 800-30: "Guide for Conducting Risk Assessments"
- ISO 31000:2009 - "Risk Management – Principles and Guidelines" (Available at www.iso.org)

Device Accessibility (Milestone 4)

- *Group Policy: Fundamentals, Security, and Troubleshooting* by Jeremy Moskowitz (Addison-Wesley, © 2008)

User Access (Milestone 5)

- NSA Fact Sheet: "Enforcing No Internet or E-mail from Privileged Accounts"

Patch Management (Milestone 6)

- NIST Special Publication 800-40: "Creating a Patch and Vulnerability Management Program"
- Using WSUS to patch third-party applications (www.windowsitpro.com/article/patch-management/Secure-non-Microsoft-applications-by-publishing-3rd-party-updates-to-WSUS.aspx)

Baseline Management (Milestone 7)

- Securing Web browsers (www.us-cert.gov/reading_room/securing_browser)
- Microsoft Baseline Security Analyzer (MBSA) (http://technet.microsoft.com/en-us/security/cc184924.aspx)
- Center for Internet Security (http://cisecurity.org) [Windows, Linux, Solaris, Apple, Oracle, Cisco, etc.]
- NSA configuration guides (www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml)
- NIST National Checklist Program (http://web.nvd.nist.gov/view/ncp/information)
- DISA Security Technical Implementation Guides (STIGs) (http://iase.disa.mil/stigs/index.html)
- *Protect Your Windows Network* by Johansson and Riley (Addison-Wesley, © 2005)

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

- *Incident Response & Computer Forensics, Second Edition* by Mandia, Prosise, and Pepe (McGraw-Hill/Osborne, © 2003)
- Remediation considerations (http://blog.mandiant.com/archives/1525)
- NIST Special Publication 800-34: "Contingency Planning Guide for Federal Information Systems"
- NIST Special Publication 800-61: "Computer Security Incident Handling Guide"
- NIST Special Publication 800-83: "Guide to Malware Incident Prevention and Handling"

Security Policy (Business Functionality Network Security Task)

- The SANS Security Policy Project (www.sans.org/security-resources/policies)

Training (Business Functionality Network Security Task)

- DISA Information Assurance training (http://iase.disa.mil/eta/online-catalog.html)
- NIST ITL Bulletin October 2003: "Info. Tech. Security Awareness, Training, Education, and Certification" (Available at http://csrc.nist.gov/publications/PubsITLSB.html)

- NIST Special Publication 800-16: "Info. Tech. Security Training Requirements: A Role- and Performance-Based Model"
- NIST Special Publication 800-50: "Building an Information Technology Security Awareness and Training Program"

Executable Content Restrictions (Host-Based Network Security Task)

- "Application Whitelisting Using Software Restriction Policies" (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml)
- Windows AppLocker (http://technet.microsoft.com/en-us/library/dd548340(WS.10).aspx)
- NSA Fact Sheet: "Data Execution Prevention (DEP)" [Windows, Linux, Solaris, Mac OS X]
- NSA Fact Sheet: "The Microsoft Office Isolated Conversion Environment and File Block Functionality with Office 2003"

Personal Electronic Device (PED) Management (Host-Based Network Security Task)

- Enforcing restrictions with Group Policy (http://msdn.microsoft.com/en-us/library/bb530324.aspx)
- NSA Fact Sheet: "Disabling USB Storage Drives" [Windows, Linux, Solaris, Mac OS X]
- NSA Fact Sheet: "Security Tips for Personally-Managed Apple iPhones and iPads"
- Managing iOS devices in an enterprise (www.apple.com/support/iphone/enterprise)
- NIST Special Publication 800-124: "Guidelines on Cell Phone and PDA Security"

Data-at-Rest Protection (Host-Based Network Security Task)

- NSA Fact Sheet: "How to Securely Configure Microsoft Windows Vista BitLocker"
- U.S. Government selected companies (www.gsa.gov/portal/content/102647)
- NIST Special Publication 800-111: "Guide to Storage Encryption Technologies for End User Devices"

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

- NSA Fact Sheet: "Port Security on Cisco Access Switches"
- Windows Network Access Protection (http://technet.microsoft.com/en-us/library/cc730902(WS.10).aspx)
- NSA Fact Sheet: "Hardening Authentication"

Security Gateways, Proxies, and Firewalls (Network Monitoring and Control Network Security Task)

- NIST Special Publication 800-41: "Guidelines on Firewalls and Firewall Policy"

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

- NIST Special Publication 800-46: "Guide to Enterprise Telework and Remote Access Security"
- NIST Special Publication 800-48: "Guide to Securing Legacy IEEE 802.11 Wireless Networks"
- NIST Special Publication 800-97: "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i"
- NIST Special Publication 800-114: "User's Guide to Securing External Devices for Telework and Remote Access"
- NIST Special Publication 800-121: "Guide to Bluetooth Security"

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

- *The Tao of Network Security Monitoring* by Richard Bejtlich (Addison-Wesley, © 2005)
- *Extrusion Detection* by Richard Bejtlich (Addison-Wesley, © 2006)
- As first step to security (http://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html)

Log Management (Network Monitoring and Control Network Security Task)

- "Critical Log Review Checklist for Security Incidents" (www.sans.org/security-training/course_sums/1217.pdf)
- NIST Special Publication 800-92: "Guide to Computer Security Log Management"

Configuration and Change Management (Network Monitoring and Control Network Security Task)

- "The Definitive Guide to Enterprise Network Configuration and Change Management" (http://nexus.realtimepublishers.com/dgenccm.php)
- IT Infrastructure Library (ITIL) (www.itil-officialsite.com/Publications/Core.asp)
- Microsoft Operations Framework (MOF) (http://technet.microsoft.com/en-us/solutionaccelerators/dd320379.aspx)
- NIST Special Publication 800-128: "Guide for Security-Focused Configuration Management of Information Systems"
- *The Visible Ops Handbook* by Behr, Kim, and Spafford (IT Process Institute, © 2004)

Audit Strategy (Network Monitoring and Control Network Security Task)

- *Security Metrics* by Andrew Jaquith (Addison-Wesley, © 2007)
- NIST Special Publication 800-55: "Performance Measurement Guide for Information Security"

Tools Mentioned

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

Map Your Network (Milestone 2)

- Nmap (http://nmap.org)
- arpwatch (http://ee.lbl.gov)
- NetReg (http://netreg.sourceforge.net; Carnegie Mellon's version: www.net.cmu.edu/netreg)
- Wireshark (www.wireshark.org)
- tcpdump (www.tcpdump.org)
- WinDump (www.winpcap.org/windump)

Device Accessibility (Milestone 4)

- Puppet (www.puppetlabs.com)
- PuTTY (www.chiark.greenend.org.uk/~sgtatham/putty)
- WinSCP (http://winscp.net)

Patch Management (Milestone 6)

- Windows Server Update Services (WSUS) (http://technet.microsoft.com/en-us/wsus/default)
- Puppet (www.puppetlabs.com)
- Spacewalk (http://spacewalk.redhat.com)
- SANS WhatWorks (www.sans.org/whatworks), 4.4 Patch and Security Configuration Management and Compliance

Executable Content Restrictions (Host-Based Network Security Task)

- Enhanced Mitigation Experience Toolkit (EMET) (www.microsoft.com/download/en/details.aspx?id=1677)

Personal Electronic Device (PED) Management (Host-Based Network Security Task)

- Free tools for U.S. Government organizations (www.iad.gov, under Mitigations - Tools)

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

- SANS WhatWorks (www.sans.org/whatworks), 3.2 Network Access Control

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

- Snort (www.snort.org)

Log Management (Network Monitoring and Control Network Security Task)

- Splunk (www.splunk.com)
- Snare (www.intersectalliance.com)
- SANS WhatWorks (www.sans.org/whatworks), 6.1 Log Management and Security Information and Event Management

Audit Strategy (Network Monitoring and Control Network Security Task)

- SCAP validated tools (http://nvd.nist.gov/scapproducts.cfm)
- Microsoft Security Assessment Tool (MSAT) (http://technet.microsoft.com/en-us/security/cc185712.aspx)

Index