Global Information Assurance Certification Paper

Seeking Security: The New Paradigm for Government Agencies

Stephan H. Chapman
01MAR2002
GSEC Version 1.3

Introduction: While large federal government agencies like the Internal Revenue Service have great visibility and even greater budgets, the country is peppered with smaller federal and state agencies that are wrestling with IT security issues. These agencies often have difficulty obtaining funding, staffing, and interest from upper or executive management levels because network security is largely thought to be the responsibility of some larger, paternal entity. Operations personnel know this is not true, but what security measures must be implemented before attackers compromise our systems? This is one approach. Although this document will appear to be targeted to the federal sector, it is viable for any sized government agency, domestic of foreign, with a security problem.

Abstract: It is often difficult for IT professionals to differentiate *de facto*[1] responsibility from *de jour*[2] responsibility for agency programs, policies, and security issues. Provided are the legal authorities and responsibilities applicable to government IT professionals, given the frequent inability to identify jurisdictional or authoritative basis.

This document serves as a roadmap by using the U. S. Federal Government Agency IT community as an example of how to overcome bureaucratic inertia. This guide is divided into five comprehensive activities to be used by *"Any-Agency"* IT operations personnel to begin to eliminate the security vulnerabilities associated with IT assets. These five essentials are:

1. Immediate triage and Asset Identification
2. How to conduct a Risk Assessment and analysis
3. Determine and implement Risk Mitigation activities or procedures
4. Write and implement a comprehensive Security Policy
5. Repeat steps 1-3 for Risk Mitigation measurement

Finally, a process is outlined to begin to change the culture and mindset of many agencies and managers from territorial elitism to cooperative interoperability.

---

[1] *De facto*: Latin: "as a matter of fact;" something which, while not necessarily lawful or legally sanctified, exists in fact. URL: http://www.duhaime.org/dict-d.htm#D.

[2] *De jure:* Latin: "of the law." The term has come to describe a total adherence of the law. URL: http://www.duhaime.org/dict-d.htm#D.

Who's On First?

Costello: Are you the manager?
Abbott: Yes.
Costello: You gonna be the coach too?
Abbott: Yes.
Costello: And you don't know the fellows' names.
Abbott: Well I should.
Costello: Well then who's on first?
Abbott: Yes.
Costello: I mean the fellow's name.
Abbott: Who.
Costello: The guy on first.
Abbott: Who.
Costello: The first baseman.
Abbott: Who.
Costello: The guy playing...
Abbott: Who is on first!
Costello: I'm asking you, who's on first?[3]

When many Americans think of "The Government," the image conjured is frequently some amoeba-like mass whose gelatinous head would not be locatable. The properties of this blob are often likened to those of a black hole: Inescapable, and there seems to be more going in than coming out. Like the early twentieth-century "Abbott and Costello" skit, the players and roles in the many government agencies are often difficult to determine.

Many will be challenged to remember seventh-grade American Government classes regarding the U. S. tripartite form of federal government: The Executive Branch, the Legislative Branch, and the Judicial Branch. Here is a brief outline of those jurisdictions with some insights about federal government agencies not commonly understood:

Executive Branch: Recommends or requests Congress to write laws, acts, and statutes. Has some law-making capability through issuing Executive Orders[4] (EO's). An important and sometimes confusing distinction is that EO's only apply to executive branch agencies such as the State Department, Office of Personnel Management (OPM), Department of Agriculture (USDA), and the Defense Department (DOD), among many. The other branches of government are frequently under no obligation to conform to an EO, and in fact, often ignore Executive Orders. Important recent EO's include EO13228 "Establishing the Office of Homeland Security and the Homeland

[3] Author unknown. Excerpted. Performed by various artists in vaudeville and stage. Made famous by Abbott and Costello in 1943 during a live performance, and later by this same duo for The Naughty Nineties radio show in 1945.

[4] Executive Orders are official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government. The text of Executive Orders appears in the daily Federal Register as each Executive Order is signed by the President and received by the Office of the Federal Register. The text of Executive Orders beginning with Executive Order 7316 of March 13, 1936, also appears in the sequential editions of Title 3 of the Code of Federal Regulations (CFR). URL: http://www.nara.gov/fedreg/eo.html#orders

Security Council,"[5] and EO13231 "Critical Infrastructure Protection in the Information Age."[6] Note that most executive branch agencies maintain individual security strategies, IT divisions, structures, and policies particular to that agency.

Legislative Branch: Includes not only the House of Representatives and the Senate, but also the Library of Congress. Congress *creates* federal legislation, whether at the request of constituents (Read: Lobbyists), other branches of government, or their own initiative, and submits passed bills to the executive branch to *enact* into law by signing them. Congress also has an extensive history of *excepting* itself from legislation that it crafts. Notable examples include exceptions to the requirements of Occupational Safety and Health Administration (OSHA), Americans with Disabilities Act (ADA), and OPM requirements. These positions have recently been changed[7], however, and the Congress has been more responsive to making itself subject to the laws it imposes on the rest of the land. The legislative branch maintains several small, excepted-service agencies that support varied functions. Again, the federal agencies supporting the U.S. Congress are not subject to EO's like those noted above. Important legislation, either passed or being considered, includes: HR2435 "Cyber Security Information Act,"[8] HR3400 "Networking and Information Technology Research Advancement Act,"[9] and the Senate's S.1014 "Social Security Number Privacy and Identity Theft Prevention Act of 2001."[10] The GAO (General Accounting Office)[11] is given as an example of a legislative branch entity that has process power over any other federal government entity. The legislative branch maintains within itself several IT entities, each with unique polices, procedures, and responsibilities.

The Judicial Branch: Article III of the Constitution established The Supreme Court as the highest court in the land. Congress created all other federal courts and court systems. Courts decide arguments about the meaning of laws, how they are applied, and whether they conform to the Constitution. The courts can "engineer" legislation by striking down laws and Executive Orders that conflict with judicial precedents or goals. Like the other two jurisdictions, the federal courts maintain individual security strategies, IT divisions, structures, and policies particular to that jurisdiction.

The New Kid on the Block—The Office of Homeland Security[12]: Created by EO13228 (October 8th, 2001), and given teeth by EO13231 (October 16th, 2001). This newly created office by the current Bush Administration has the potential to become the central authority for federal government IT security related issues. Over time, it is

[5] EO13228 (October 8, 2001). URL: http://www.nara.gov/fedreg/eo2001b.html.

[6] EO13231 (October 16, 2001). URL: http://www.nara.gov/fedreg/eo2001b.html.

[7] The Office of Compliance was established to implement and enforce the Congressional Accountability Act of 1995. Known as the CAA, the Act generally extends the rights and protections of employment and labor laws to employees of the legislative branch. URL: http://www.compliance.gov/

[8] URL:<http://thomas.loc.gov/cgi-bin/query/D?c107:33:./temp/~c107fOgSX5::

[9] URL: http://thomas.loc.gov/cgi-bin/query/D?c107:3:./temp/~c107fOgSX5::.

[10] URL: http://rs9.loc.gov/cgi-bin/query/D?c107:5:./temp/~c107OnIeSd::.

[11] General Accounting Office: The General Accounting Office is the investigative arm of Congress. GAO exists to support the legislative branch in meeting its Constitutional responsibilities and to help improve the performance and accountability of the federal government. URL: http://www.gao.gov/.

[12] The Office of Homeland Security.URL: http://www.whitehouse.gov/homeland/.

realistic to expect that this will happen, and if there is another significant act of terrorism in this country, expect this executive branch agency to flex its muscles immediately. There are repeated media reports detailing the difficulties the various executive branch[13] agencies are having sorting out areas of responsibility, jurisdictional authority, and other complex issues of inter-agency operations. Despite significant protest from some agencies, expect these challenges to be met.

Revisiting "Who's on First?": The population of the country is wondering exactly who or what is establishing IT security policy. Many Americans think that our government actually has some comprehensive document or central resource in place to address security and information protection issues. This is not the case. The numerous jurisdictional entities previously described have security policies ranging from no policy to strong security policy implementations. Our security activities—or lack thereof—have a rippling effect starting with the federal government and including state governments, foreign and domestic, and extending to international commerce and communities.

Government agencies must act to protect the intellectual property they generate and accumulate. The accumulations of some agencies, such as the IRS or Social Security Administration, are "crown-jewel" assets that require a focused and comprehensive plan for protection. It is the intention of the executive branch that the Office of Homeland Security will be the authoritative entity crafting national policy. That will be "Who's on First." [Note: Bookmark the above footnote reference, 12, as this Internet site will assume increasing importance as a reference.]

"We Have Seen the Enemy…": Many professionals with an interest in protecting government IT assets fall victim to the resulting inertia of waiting for upper management to provide leadership, support, or managerial expertise. This in no way mitigates any vulnerability or removes IT professionals from associated risk reduction responsibilities. Many IT operations specialists are in the best position to make highly accurate risk analyses relative to exposed assets, and are *significantly* aware of the level of risk of an attack against principal assets. A "head-in-the-sand" approach to risk management will ultimately result in risk identification anyway; as soon as an attacker compromises a "crown-jewel" asset and either destroys it or denies availability to users. *When* this occurs, involved personnel will most likely be offered a change in employment moments after the asset is restored. Accepting the role of an IT professional requires reasonable effort to safeguard and protect IT assets, and an elevated role in bringing the known risks of asset attack to the attention of management. Consider the following five steps to network security as:

I. TRIAGE—First Steps To Managing the Risk—Staunch the Flow:

- Stop waiting for direction, encouragement, or authority from above. Despite the

[13] URL: http://www.infoctr.edu/fwl/fedweb.exec.htm.

confusing and sometimes contradictory jurisdictional avenues available, most IT professionals already have all the authority needed. Print and read the *Federal Legislation Affecting Information Management*[14] document and get the supporting facts required to show management a basis in law. At a bare minimum, conformation *should or must* be made to the following laws and acts, included in the above reference: The Computer Security Act of 1987,[15] The Paperwork Reduction Act of 1995,[16] and The Clinger-Cohen Act of 1996.[17]

- Federal agencies are required to have a CIO. If an agency does not have a CIO, then the agency is in violation of The Clinger-Cohen Act of 1996. The role of the CIO is to develop, maintain, and facilitate the implementation of a sound, secure, and integrated IT architecture. The important concept in the preceding sentence is "secure." Inform management of this requirement, if there is no CIO in the organization. (Does anyone *really* think that this will escape the attention of a GAO audit?)

- Print and discuss the following two articles Fed Systems Still too Vulnerable,[18] and Agencies Flunk Security Review[19] with managers having executive responsibility. Merely reading the article titles will give pause for concern. Actually reading them will motivate IT staff out of cubicles and into action.

- Go to the SANS Institute's (System Administration, Networking, and Security) Top Twenty Most Critical Internet Security Vulnerabilities[20] and implement the recommended solutions to common vulnerabilities. Focus on the no-cost or low-cost items, which will begin to protect IT assets, as well as provide an immediate credibility boost for IT staff. [Example: Item "G2 - Accounts with No Passwords or Weak Passwords"[21].] Starting with these kinds of protection strategies will consume mostly time, and ordinarily does not require the purchase of anything. These are also the kinds of tasks and activities that can be completed during the gestation period of a full-blown Security Policy. Yes, this recommendation comes before the design and implementation of a fully-funded and comprehensive Security Policy. Continuing to wait for that to happen will delay risk mitigation for years. IT assets will not remain untouched by attackers during this time interval.

- Understand the differences between *triage* and applying a *Band-Aid.* Triage is a series of stabilizing "life-saving" actions taken in advance of performing well-understood restorative processes or procedures. Applying a Band-Aid is a

[14] URL: http://irm.cit.nih.gov/policy/legislation.html.
[15] URL: http://irm.cit.nih.gov/policy/legislation.html.
[16] URL: http://irm.cit.nih.gov/policy/legislation.html.
[17] URL: http://irm.cit.nih.gov/itmra/itmra96.html.
[18] URL: http://www.fcw.com/fcw/articles/2001/0402/web-cyber-04-06-01.asp.
[19] URL: http://www.fcw.com/fcw/articles/2001/1112/news-score-11-12-01.asp.
[20] SANS (System Administration, Networking, and Security) Institute. URL: http://www.sans.org/top20.htm.
[21] SANS Institute. URL: http://www.sans.org/top20.htm.

prophylactic measure implemented to cover an injury and wait for the wound to self-heal. *Vulnerabilities do not self-heal, and executive managers tend to be strong advocates of Band-Aids. Triage "yes!" Band-Aids "no!"*

The Four Guiding Principles in Securing Networks:

When beginning to develop the "how" of implementing security in a network, consider the Four Guiding Principles of Network Security:[22]

1. ***Know Thy Network.*** IT professionals have to know their networks. Translated, all of the network assets must be identified and documented. Answer the questions: "What is it that requires protection?" and "What interest would an attacker have in this network?" There are generally five broad categories of network assets subject to great scrutiny:

    i. **Intellectual property:** The data that users generate or that agencies collect or manufacture. This is usually stored on hard drives, magnetic media, optical media, and more currently, SAN (Storage Area Networks) devices. It is pervasively everywhere. Users put it on floppy disks and take data home. It is located on the hard drives of desktop machines and central data-stores, tapes, jukeboxes, printouts and PDA's. The stuff is everywhere, and often it is replicated in or on unexpected devices.
    ii. **Operating Systems:** The software and related configuration files used by the Operating System (O/S). Included are RPC's (Remote Procedure Calls), services, processes, loadable modules, and applets that installed applications must have to run. Patch libraries, service packs and "mods" for an O/S are also in this category. Remember that the OEM media must be included in any complete inventory.
    iii. **Application Software:** Includes COTS (Commercial Off-The-Shelf) software, custom software and proprietary software running on the O/S platforms described under 1.ii. Again, remember that the OEM media must be included in any complete inventory.
    iii. **Network Infrastructure:** Consists of all the hardware supporting OSI Model[23] layers one through three and includes all cabling, wiring, fiber, terminations, appliances, patch-panels, light-boxes, switching/routing/bridging equipment, filters, firewalls, IDS's (Intrusion Detection Systems), wireless technologies, and more. If users are provided with wireless services, evaluate these assets for exposure to "war-

[22] SANS (System Administration, Networking, and Security) Institute, Eric Cole, Washington SANS Conference, December, 2001. Eric Cole is a nationally recognized speaker on IT vulnerabilities from an attacker viewpoint. He recently published the book Hacker's Beware, annotated in the bibliographical section of this document.

[23] In 1978, the International Standards Organization (ISO) introduced the Open Systems Interconnect (OSI) model as a first step toward international standardization of the various protocols required for network communication. For a basic discussion see: URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q103881.

driving"[24] attacks. OEM media must be included in this inventory as well.

iv. **The telephone system in use** by an agency must be analyzed for vulnerability to "war-dialers"[25] and other similar technologies.

Learning about the principal assets in a network can be a daunting task. Large networks will have to be broken down into manageable segments with assignments to multiple staff members. WAN (Wide Area Network) links can often establish logical boundaries for asset grouping.

A powerful tool for network asset identification is probably something used on a daily basis: A Network Management System (NMS). The most powerful of these tools include Hewlett-Packard's "Open View," Aprisma's "Spectrum," as well as products from Computer Associates and Tivoli. If a NMS is correctly installed and is accurately configured to represent the network, it will yield significant information about the network and the logical and physical relationships of IT assets.

Whatever the tools, IT professionals working on asset identification must agree that the resulting inventory is comprehensive and accurate. All other steps in this process are dependent upon this accuracy and completeness.

2. ***Adhere to the principle of "Least Privilege" for users.*** Users should have access to systems and resources only to the extent required to perform a job-related function. The mind-set in government agencies has historically been one of granting users "Most Privilege." This concept needs to begin to change to one of "Least Privilege," consistent with performance requirements.

   Change within organizations is often difficult and time-consuming. Many of the risk abatement techniques in this document can only be implemented with the cooperation and assistance of users, workgroups, and the participation of a supportive management structure. Please refer to **Changing the way we think…"You All" to "Us:"** which is discussed later in this document.

3. ***Defense in Depth.*** Adopt strategies to protect network assets in multiple layers of defense. Deny attackers (from any source) the easy path. This must begin with a User Access Policy, a document that many agencies currently do not have. A comprehensive Security Policy that is uniformly applied throughout the agency must follow this. Begin to think of ways to protect assets by "wrapping" them in "layers" of protective strategies.

4. **Prevention *is ideal, but* detection *is* ***mandatory!*** 100% prevention, per se, is

[24] The act of driving around blocks of corporate buildings and downtown business districts with a wireless LAN receiver, trying to "tune-in" networks that can be used for gaining internal access or access to the Internet.

[25] A program designed to detect a carrier presence using a modem and POTS (Plain Old Telephone System) telephone lines. It will sequentially dial all telephone numbers in a range or exchange, searching for a modem to answer when it calls. URL: http://www.wikipedia.com/wiki/War_dialing.

never achievable because of continually evolving unknown risk factors. Therefore *intrusion detection* must be incorporated into asset protection. Most IDS's are implemented in multiple layers around *all* mission-critical assets. Many government agencies have not implemented *any* IDS protection as of yet.

II. Second Series of Actions: What Are the Risks? Now that principal assets are known and documented, conducting a risk assessment mapped to those assets becomes the next step in the process. A frequent approach in government agencies is to retain the services of firms experienced in risk assessments. If this is the approach selected, the benefits of conducting a parallel in-house assessment cannot be understated, if only for verification purposes of the contracted service provider. For the purposes of introducing the reader to a basic risk assessment process, this document will limit discussion to topics easily researched using the sources listed in the **Who Can Help Me?** section of this paper. Details about the components of comprehensive risk assessments may be found in the provided URL's, major book references in the attached Bibliography, and by attending immersion-training conferences from specialists in this subject matter like the SANS Institute.

A "bare-bones" risk assessment must include the following components:

- A physical access analysis of all the assets identified in the *Know Thy Network* process. Answer questions like "Who has access to wiring closets or other IT assets?" "What access is possible to fileservers and data-stores?" "Where are copies of backup media stored?" "What are the ways data may be distributed by users?"

- Read a book such as Hacking Exposed: Network Security Secrets and Solutions: Third Edition.[26] This will teach thinking like an attacker, which will result in preparations as a defender.

- Research the SANS Institute's "Top 20" Threats and Vulnerabilities List (available at URL: http://www.sans.org/top20.htm), and *map* "Any-Agency" to quickly assess common vulnerabilities. A proposed format is illustrated below:

[26] Kurtz, George, McClure, Stuart, and Scambray, Joel. Hacking Exposed: Network Security Secrets and Solutions: Third Edition. Berkeley: Osborne/McGraw-Hill, 2001.

How "Any-Agency" Maps to the SANS Institute's "Top 20" Threats and Vulnerabilities List (DEC2001)

Item Number	SANS Institute Vulnerability G = General; W = Windows; U = Unix; N = NetWare	Applicability to "Any-Agency"	"Fix This!" Priority 1=L;2=M;3=H
1	G-1: Default installs of operating systems and applications.	We do almost nothing (detectable) at "My Agency" to harden an O/S, or an application during installation.	3
2	G-2: Accounts with no passwords or weak passwords.	The results of the LC3 compromise demonstrate our significant vulnerability to this threat.	3
3	G-3: Non-existent or incomplete backups.	We still have consistency problems with the W&N backups…U is unknown. Is there a written policy governing off-site stores?	3
4	G-4: Large number of open (TCP) ports.	Our scan is incomplete, but we are not finding this to be a pervasive problem in. U = unknown	2
5	G-5: Not Filtering packets for correct IN/OUT addresses.	We have nothing in place that makes this comparison.	2
6	G-6: Non-existent or incomplete logging.	We do not have any staff members that routinely monitor logs as a scheduled activity for any system.	3
7	G-7: Vulnerable CGI programs.	If all web servers are located in the DMZ (SSN), then this is probably a low risk.	2
8	W-1: Unicode vulnerability (Web server folder traversal).	This is called "directory walking" via overlong sequences. Un-patched IIS servers are vulnerable.	2
9	W-2: ISAPI extension buffer overflows.	Idq.dll is vulnerable to buffer overflow attacks on un-patched (IIS) servers.	2
10	W-3: IIS RDS (Remote Data Services) exploit.	If IIS is un-patched, it is vulnerable.	2
11	W-4: NETBIOS unprotected Windows networking shares.	If IIS is un-patched, it is vulnerable.	1
12	W-5: Information leakage via NULL session connections. An intruder can get an "Administrator" equivalent connection using this technique.	Try using <net use \\a.b.c.d\ipc$ "" /user:"">	1
13	W-6: Weak hashing in SAM (LM Hash).	Every workstation running WinNT4 is vulnerable in our network.	3
14	U-1: Buffer overflows in RPC services.	Have the procedures to test for this.	1
15	U-2: SENDMAIL vulnerabilities	Have the procedures to test for this.	1
16	U-3: Bind weaknesses (Allows IP address discovery by querying DNS entries by name).	There is probable exposure to this threat in. Have the procedures to test for this.	2
17	U-4: "R" commands (using trust relationships).	Have the procedures to test for this.	2
18	U-5: LPD (remote print protocol daemon).	Solaris is particularly vulnerable to this.	2
19	U-6: Sadmind and mountd (Allows remote administration access to Solaris systems, providing a GUI for most functions).	Solaris is particularly vulnerable to this.	2
20	U-7: Default SNMP strings (SNMP is used to control network devices).	We use the factory defaults of "public" and "monitor" pervasively in "My Agency.".	2

- Run a port-scanning utility to determine "listening" ports on all fileservers, data-stores, and network resources. Download "Nessus,"[27] and install the application on a dedicated Linux server. Always run the scanning processes in the least

invasive mode available, or the risk of creating a Denial Of Service (DOS) is significant in a production environment. Analyze the scans of the reported segments for vulnerable ports and unnecessary services running on selected hosts. [Note: Excellent installation and product use instructions are available at the Nessus Internet site. URL: http://www.nessus.org/ Also see Pocket Nessus by Tony Enriquez, available at URL: http://rr.sans.org/tools/pocket_nessus.php [28] for a comprehensive primer in the use of this powerful tool.]

- Spend three-hundred dollars for two items: First, a full featured copy of L0phtCrack[29] ver. 3.0 ($249.99), which will support "brute force" password cracking capability against Windows Security Account Manager (SAM) files, and second, a copy of the previously referenced book Hacking Exposed ($49.99). If the predominant O/S on desktop machines and fileservers is Windows NT 4.0, then Chapter 5 of this book will illustrate everything needed in determining vulnerabilities and the prescriptions to fix them. Recipe-like instructions to compromise and then protect every major operating system are found in the relevant chapters. Spend time with L0phtCrack to gain an understanding of how most password-cracking utilities work. This will help in the design of a more secure password policy for users.

- Summarize the threats, vulnerabilities, and risks discovered in asset charts similar to the partial chart sample below:

[27] Nessus is free software designed to probe targeted hosts on a network for listening TCP/UDP ports, exploitable RPC's, and many other features and functions. It is an important tool in performing an audit on a network. URL: http://www.nessus.org/.

[28] Enriquez, Tony. Pocket Nessus. URL: http://rr.sans.org/tools/pocket_nessus.php.

[29] L0phtCrack is a tool to identify Windows user account passwords. It has several methods of achieving this, via simple "dictionary" cracks or full-fledged "brute force" cracks. It achieves a 90% success rate in 48 hours or less. URL: http://www.atstake.com/research/lc3/.

SAMPLE: Risk Assessment of Assets for "Any-Agency:" i. Intellectual Property

Intellectual Property	Qualitative Value	Threat	Vulnerability	Risk	Mitigation	Priority of Mitiga-tion
1 CADD drawings Housed on 1 of 8 CADD servers located in (Rm 410). Protected by daily backups to magnetic media by the MIS Division's Technical Support group. Off-site positioning of media is unknown.	For all practical purposes, these drawings are IRREPLACABLE. This is estimated to be "Any-Agency's" most valuable asset.	1.1 Disgruntled or malicious staff, especially MIS. 1.2 Theft of host server, drive array components, or tape media. 1.3 Accidental or deliberate file system damage, or to data or system configuration files. 1.4 (Continued)	1.1 Easy access to Rm 410, especially for an MIS staff member. 1.2 Access to servers. See 1.1 above. Tapes are unsecured, and access to the fileservers is not secure. There is a central point of failure if the backup device(s) fail. 1.3 See 1.1 above. 1.4 (Continued)	1.1 Drawing files on the host servers can be accessed by anyone who can get physical access to the servers in Rm 410. 1.2 No policy(ies) by default is a state of permission. Tapes can be stolen and used to mine data. 1.3 See 1.1 above. 1.4 (Continued)		

Be aware that in analyzing Nessus scan reports, there will be an almost overwhelming quantity of information. The Nessus reports will contain estimates of the significance of the risks it identifies, but ultimately determinations will have to be made quantifying how much, if any, of the risk an organization is willing to absorb.

Researching the SANS Institute's "Top 20" Threats and Vulnerabilities List will identify other risks prevalent in most networks. More risks can be identified when an "attacker" mindset is adopted. Initiate discussions with asset supervisors to determine the weaknesses and vulnerabilities of IT systems. These IT professionals are often the designers and implementers of major technologies, and are well aware of implementation weaknesses, flaws and vulnerabilities.

Charting risks by asset type has the advantage of allowing the prioritization of the risks and abatements that are developed. Establish multiple "sorts" of collected data based on the ability to complete risk reductions "in-house," subcontracted activities, or task assignment lists sorted by specific staff member. Organizing this information by asset type and by network segment will assist greatly in the construction of persuasive managerial reports.

III. Third Group of Activities: Analyze Data and Implement Risk Abatement Procedures.

As risks and vulnerabilities become evident (step II above), thematic problems across operating system platforms and hardware platforms will emerge. Crafting risk

abatement procedures for one asset frequently can be "kernalized" and applied to other vulnerable assets.

During the risk analysis process, "brainstorming" sessions with other IT professionals can lead to unexpectedly creative results in risk mitigation strategies. Examine the sample chart below as a guide to risk mitigation strategies for a physical access problem:

SAMPLE: Risk Assessment of Assets for "Any-Agency:" i. Intellectual Property

Intellectual Property	Qualitative Value	Threat	Vulnerability	Risk	Mitigation	Priority of Mitigation
1. CADD drawings Housed on 1 of 8 CADD servers located in (Rm 410). Protected by daily backups to magnetic media by the MIS Division's Technical Support group. Off-site positioning of media is unknown.	For all practical purposes, these drawings are IRREPLACABLE. This is estimated to be "Any-Agency's" most valuable asset.	1.1 Disgruntled or malicious staff, especially MIS. 1.2 Theft of host server, drive array components, or tape media. 1.3 Accidental or deliberate file system damage, or to data or system configuration files. 1.4 (Continued)	1.1 Easy access to Rm 410, especially for an MIS staff member. 1.2 Access to servers. See 1.1 above. Tapes are unsecured, and access to the fileservers is not secure. There is a central point of failure if the backup device(s) fail. 1.3 See 1.1 above. 1.4 (Continued)	1.1 Drawing files on the host servers can be accessed by anyone who can get physical access to the servers in Rm 410. 1.2 No policy(ies) by default is a state of permission. Tapes can be stolen and used to mine data. 1.3 See 1.1 above. 1.4 (Continued)	1.1 Security Policy with published list (with picture ID's) of permitted staff. Badge readers should limit the hours of access to most staff. New staff should NEVER be given Admin, Super-User or other high-level access to resources without some probationary period. 1.2 Be sure all serial numbers of all devices are recorded, and that the local Police is given a copy of the document semiannually. Store electronic backup media offsite, in at least two separate locations, and use two different kinds of media. Bar-coding of media is preferred. 1.3 See 1.1 above. 1.4 (Continued)	1.1 High 1.2 High 1.3 High 1.4 (Cont.)

Completing risk mitigation charts for all network assets will produce what will seem to be an overwhelming "to-do" list. Notice, however, that reduction of mitigation strategies to sorted lists has the actual effect of breaking implementation into manageable and do-able chunks. Further, these task lists should be prioritized and require item completion dates.

It is the recommendation of this writer that prescriptive mitigation strategies be written at two levels: One list is written at a "high-altitude" executive management level, and other itemizations are written to operations personnel responsible for the asset. The

first sample illustrates a "Global-ONE" priority list directed towards decision-makers:

SAMPLE: "Global-ONE" Risk Mitigation Strategy for "Any-Agency"

Priority #	Risk Mitigation Strategy	Date to Complete
1.	Change "Any-Agency" mindset from one of "Most Privilege" to one of "Least Privilege." This is evolutionary, not revolutionary. This will also require extensive, near academic contact with the user community.	15JUN2005
2.	Develop a Security Policy. Begin with a User-Access Policy immediately.	31JUL2003
3.	Use the NMS tools to advantage. Dedicate the primary responsibility of these systems to a dedicated employee, and provide two trained backup staff.	30SEP2002
4.	Require that network administrators learn the network in depth. Assign overlapping administrative responsibilities across operational functions.	30DEC2003

When the above priority list is presented in report form to executive management, include all the subordinate task lists for operations personnel. This will have the added benefit of demonstrating to executive managers the depth and breadth of the security vulnerabilities that "Any-Agency" is exposed to. Better, plan a multi-format presentation to executives with these materials.

Examine the abbreviated sample below:

SAMPLE: Risk Mitigation Strategy for the UNIX Administrator for "Any-Agency"

Priority #	Risk Mitigation Strategy	Date to Complete
1.	Learn the network by learning the NMS from an ADMIN USER standpoint.	30DEC2003
2.	Develop a schedule to "harden" all production and redundant platforms. Remove all protocols, services, procedures (RPC's), protocol components and capabilities not actually in use. Shut down UDP/TCP ports not required to support applications or functions.	30MAY2002
3.	"Clean-up" unused accounts and remove "blind" accounts from the O/S and hosted applications (where appropriate). Have administrators use discreet credentials, and restrict privilege to actual job function. Enforce strong, non-dictionary based passwords of at least 12 characters. Use a password-protected screen-saver at system consoles.	Immediately
4.	Store backup media in a secure environment with limited access. Rotate complete media libraries to offsite storage locations.	Immediately

Mitigating the risks of important assets will include a comprehensive IDS design. If the network infrastructure does not include these asset protections in depth, then network penetrations will be undiscovered. This is akin to maintaining a checking account at a bank, and not realizing that the funds are available to a "group." The predictable results at the bank are parallel to the permissive state of operating a network with no IDS implementation.

IDS's should "wrap around" the architecture of principal assets in the network. Costs can be justified for protecting fileservers, firewalls, important service hosts (like DNS), and even switching or routing devices. IDS's can be multi-vendor, but should all be implemented with identical system configurations to permit the analysis of successful penetrations or attacks. A properly designed and deployed IDS will fulfill the "defense in depth" strategy as well as the "prevention is ideal, but detection is mandatory"

requirement.

IV. Fourth Item to Complete: Write a Comprehensive Security Policy.

Readers are advised to use the following as a topical outline for developing a comprehensive Security Policy. Note that considerable material is offered in the bibliographical portion of this document. Extensive use of Internet sources will yield multiple approaches to writing security policies, as well as quantities of samples that can be used as models. Consider *any* security policy to be a dynamic, living document.

From the SNAC guide:

> A security policy is a formal statement of the rules that people who are given access to an organization's technology and information assets must abide. The policy communicates the security goals to all of the users, the administrators, and the managers. The goals will be largely determined by the following key tradeoffs: services offered versus security provided, ease of use versus security, and cost of security versus risk of loss.
>
> The main purpose of a security policy is to inform the users, the administrators and the managers of their obligatory requirements for protecting technology and information assets.
>
> The policy should specify the mechanisms through which these requirements can be met.
>
> Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization.
>
> A good security policy must:
>
> - Be able to be implemented through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods.
> - Be able to be enforced with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible.
> - Clearly define the areas of responsibility for the users, the administrators, and the managers.
> - Be communicated to all once it is established.
> - Be flexible to the changing environment of a computer network since it is a living document.[30]

Comprehensive security policies for an agency will take many months of internal negotiations, drafts and re-writes, and significant consensus building before they can be implemented. Like Nike says: “Just do it!”

[30] The Sixty-Minute Network Security Guide (First Steps Towards a Secure Network Environment). Systems and Network Attack Center (SNAC), National Security Agency, Fort Meade, MD. Unclassified document.

V. Fifth Group of Things to Do: Measure and Monitor Risk Mitigations.

The first four activities in this plan are difficult, time consuming, and potentially costly. This completion step can actually provide some fun, positive reinforcement, and professional satisfaction. In a nutshell—repeat the first three steps of the plan.

The reason these steps must be duplicated is that security professionals must be able to measure the risk mitigation strategies that were put into place. Some of the significant benefits in repeating this cycle are that:

- The effectiveness of risk mitigation strategies will be measured.
- It's easier the second time through.
- Asset inventories probably will not have changed significantly, and fine-tuning them makes them more accurate.
- The momentum of researching current security issues, exposures, and trends will be maintained.
- There will be an atmosphere of heightened security, asset protection, and professionalism permeating the network environment that will propagate to users.

The "Never-Ending Story": Security evaluations should be conducted at frequent intervals. The best practices indicate that risk assessments should be conducted whenever IT assets change, new technologies are adopted (or discarded), or whenever new risks are identified. Regular scanning of many of the Internet sites referred to in this report will assist security professionals in planning for future risk assessment methodologies, as well as attack mechanisms.

Changing the way we think…"You All" to "Us": The executive branch of the government has taken the unprecedented and surprising lead in trying to change the mindset of the way agencies think and behave. Here is an opportunity not to ignore in changing personal mindsets and those of all agencies. Proposed strategies for changing the "you all" in government to "us:"

- Readers will note significant Internet references to articles, sites, and sources of information within this document. Print these references and assemble them into a small binder. Distribute copies to colleagues and management as background reading. What will emerge is awareness that other government agencies are facing similar problems and are effecting change. Individual agencies must change as well.

- Connect with users. Recommend to management that the IT shop develop an "infomercial" of IT security basics. Presentations should include information concerning the nature of the significant IT assets; why they are valuable and how they must be protected. Explain the User Access Policy,[31] no matter what it

is, and why this policy is necessary. The presentation format should include several of the following: An intranet site, postings to bulletin boards, newsletters, system login banners, "TOTD" (Tips of the Day) appended to internal e-mails, live presentations, and CBT's (Computer-Based Training) that can be developed with a video camera and a CD burner (or insert them as videos on intranet sites). Begin to make the user community aware of security issues. This near-academic contact can take shape in many formats.

- Connect to management. Often, IT managers have limited experience with actually implementing technology. IT managers are usually focused on negotiations for services or resources, getting staff paid, responding to upper management layers, and other tasks too numerous to detail. Agencies supporting dedicated security divisions are usually populated with IT staff that had previous experience and responsibility for network administration. Security may have been a marginalized consideration because in considering cyber-attacks "…those kinds of things don't happen to us." Historically, the amount of "coverage" applied to security issues did not generally require dedicated staff and resources.

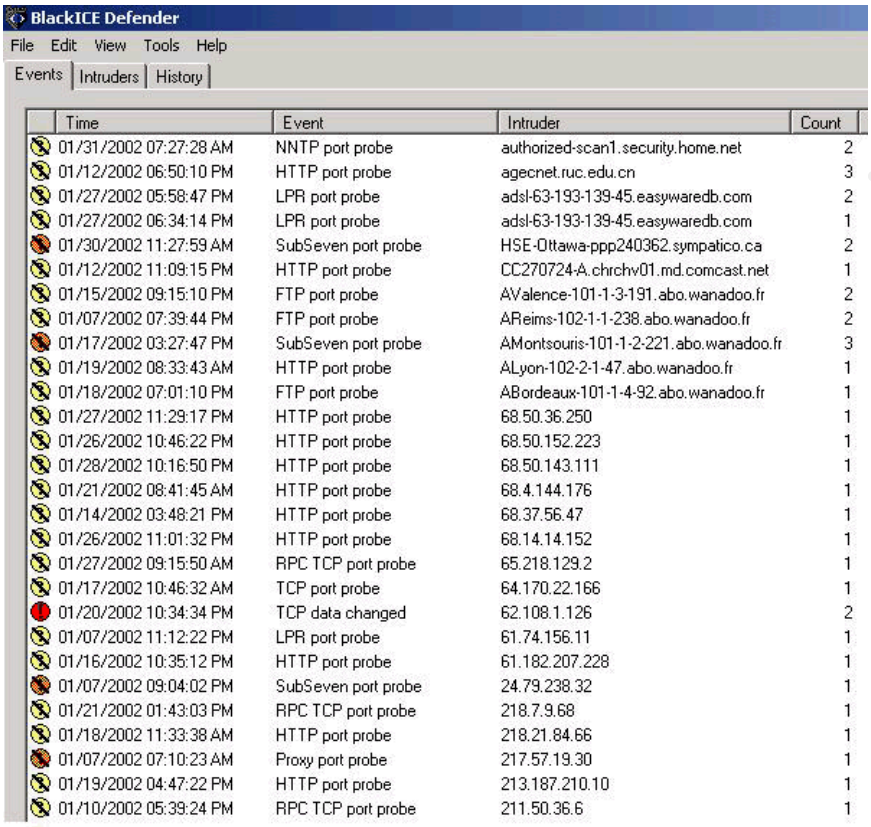
  It can be reasonably argued that those days are gone, if they ever truly existed. Managers today often experience a gap between the way they perceive the technical world, and the reality of that technical world. It is the argument of this paper that IT professionals concerned with security and IT operations have a responsibility to educate these managers. The truth has been known for a long time.

  The first reaction from many managers when first broached with the subject of risk could be one of denial. At the minimum, expect a complete lack of appreciation for the dimension and severity of the problems. Interpreted, discussions about the parameters of risk in the network must be frequent.

  Want to get risks in context in a hurry? Explain the following screen capture, generated by the personal firewall application "BlackICE"[32] from a home-based personal computer:

[31] User Access Policy: Usually a component of a comprehensive Security Policy. Not having a UAP is, in effect, granting a complete state of permission to assets. A UAP is often the first policy written to begin to establish parameters on risk management. Sample policies are readily available from the sources listed in the "Who Can Help Me" section.

[32] BlackICE, a home firewall/IDS application package is the product of Network ICE Corporation, All rights reserved, Copyright ©1998-2000. URL: http://www.networkice.com/products/blackice_defender.html.



Time	Event	Intruder	Count
01/31/2002 07:27:28 AM	NNTP port probe	authorized-scan1.security.home.net	2
01/12/2002 06:50:10 PM	HTTP port probe	agecnet.ruc.edu.cn	3
01/27/2002 05:58:47 PM	LPR port probe	adsl-63-193-139-45.easywaredb.com	2
01/27/2002 06:34:14 PM	LPR port probe	adsl-63-193-139-45.easywaredb.com	1
01/30/2002 11:27:59 AM	SubSeven port probe	HSE-Ottawa-ppp240362.sympatico.ca	2
01/12/2002 11:09:15 PM	HTTP port probe	CC270724-A.chrchv01.md.comcast.net	1
01/15/2002 09:15:10 PM	FTP port probe	AValence-101-1-3-191.abo.wanadoo.fr	2
01/07/2002 07:39:44 PM	FTP port probe	AReims-102-1-1-238.abo.wanadoo.fr	2
01/17/2002 03:27:47 PM	SubSeven port probe	AMontsouris-101-1-2-221.abo.wanadoo.fr	3
01/19/2002 08:33:43 AM	HTTP port probe	ALyon-102-2-1-47.abo.wanadoo.fr	1
01/18/2002 07:01:10 PM	FTP port probe	ABordeaux-101-1-4-92.abo.wanadoo.fr	1
01/27/2002 11:29:17 PM	HTTP port probe	68.50.36.250	1
01/26/2002 10:46:22 PM	HTTP port probe	68.50.152.223	1
01/28/2002 10:16:50 PM	HTTP port probe	68.50.143.111	1
01/21/2002 08:41:45 AM	HTTP port probe	68.4.144.176	1
01/14/2002 03:48:21 PM	HTTP port probe	68.37.56.47	1
01/26/2002 11:01:32 PM	HTTP port probe	68.14.14.152	1
01/27/2002 09:15:50 AM	RPC TCP port probe	65.218.129.2	1
01/17/2002 10:46:32 AM	TCP port probe	64.170.22.166	1
01/20/2002 10:34:34 PM	TCP data changed	62.108.1.126	2
01/07/2002 11:12:22 PM	LPR port probe	61.74.156.11	1
01/16/2002 10:35:12 PM	HTTP port probe	61.182.207.228	1
01/07/2002 09:04:02 PM	SubSeven port probe	24.79.238.32	1
01/21/2002 01:43:03 PM	RPC TCP port probe	218.7.9.68	1
01/18/2002 11:33:38 AM	HTTP port probe	218.21.84.66	1
01/07/2002 07:10:23 AM	Proxy port probe	217.57.19.30	1
01/19/2002 04:47:22 PM	HTTP port probe	213.187.210.10	1
01/10/2002 05:39:24 PM	RPC TCP port probe	211.50.36.6	1

Note in this graphic the frequency of probes and their nature. There are two "SubSeven[33] probes (orange slashed circles), a specific port probe from 217.57.19.30, and an attempt to intercept the TCP connection between the ISP (red slashed circle) and this computer, a laptop connected to the Internet via a cable-modem. These explorations and attempted system attacks comprise an insignificant fraction of the incidents that government agency portals experience.

What About Money? Recent world events have brought security issues to the forefront of managerial thinking as never before. The terrorist attacks in Washington, DC, and New York City of September 11th, coupled with the anthrax contamination of several Capitol Hill buildings and Metro-Area Post Offices are unprecedented in the history of America and the world.

The emerging worldwide collective-consciousness acknowledges the shared lack of preparedness to be faced. It is generally acknowledged that implementing defense strategies is going to cost a lot of money. In this writer's experience, budget officers are lending a willing ear and checkbook to help protect valuable, but vulnerable infrastructure and assets. Reasonable, convincing presentations for funding, particularly those illustrating the return on the investment, will be welcomed in most financial and executive circles.

[33] "SubSeven" is a common "Trojan-Horse" that, placed on a computer, allows the attacker to remotely control that computer, and possibly other computers. A "Trojan-Horse" program is one that conceals a destructive purpose. While running such a program, an unsuspecting PC user may destroy files or create a "back door" entry point that enables an intruder to access the compromised system and/or other connected systems.

Conclusion: Securing any network is an ongoing endeavor. It will take money, diligence, professional staff resources and an enlightened management. The development or acquisition of any one of these inputs may present significant challenges. These inputs, forged into a dynamic security strategy, can become a defensive strength beyond the capabilities of most network attackers.

About the Writer: The writer of this report is a ten-year federal government employee providing IT security and integration support to a small Legislative Branch agency. All charts, inclusions, and examples are fabricated solely as relevant illustrations of presented topics, and have no basis in fact concerning any single government agency.

Who Can Help and "TIPS" Page

Who Can Help? Government agencies have an overwhelming amount of resources immediately available to them. Five principal resources are listed below:

1. The SANS Institute Internet site: URL: http://www.sans.org/ for examples of policies, Risk Assessment procedures, current threats and vulnerabilities, and the priceless "Reading Room."
2. Federal Computer Weekly: URL: http://www.fcw.com/links/legislation/techleg.asp deals with current IT news and trends relative to the U. S. Federal Government. Remember that this is a commercial business when analyzing journalistic content.
3. The National Institute of Standards and Technology: URL: http://www.nist.gov/ is a repository of all laws, statutes, acts, EO's, and policies for IT issues in the federal government. Excellent source for samples for policy writing.
4. The Office of Homeland Security, The White House: URL: http://www.whitehouse.gov/homeland is the emerging iron fist of the executive branch. Don't underestimate presidential resolve of this group to make a positive difference.
5. The Sixty-Minute Network Security Guide (First Steps Towards a Secure Network Environment) published by the Systems and Network Attack Center (SNAC) of the National Security Agency. E-mail SNAC.Guides@nsa.gov for the current URL of this valuable tool.

Other Tips:

- The above principal URL's have links to other major repositories of current information.

- Form an informal weekly discussion group with colleagues to achieve information sharing. [Note: You are having coffee with these people anyway. Have something of substance to discuss for a change.]

- Consider creating topical e-mails to group participants to help elevate the exposure of all participants to the latest news and ideas.

Works Cited

Books:

Cole, Eric. Hackers Beware: Defending your Network against the Wiley Hacker. Boston: New Riders, 2001.

Gangemi, G.T. Sr., and Russell, Deborah. Computer Security Basics. Cambridge: O'Reilly and Associates, Inc., 1991.

Kurtz, George, McClure, Stuart, and Scambray, Joel. Hacking Exposed: Network Security Secrets and Solutions: Third Edition. Berkeley: Osborne/McGraw-Hill, 2001.

Security Complete. Alameda: Sybex, Inc., 2001.

United States. Systems and Network Attack Center (SNAC), National Security Agency.
The Sixty Minute Network Security Guide. Fort Meade: NSA, 2001.

Conferences:

Cole, Eric. Windows Security. Proc. Of SANS Institute Conference, Cyber Defense Initiative East, November 27 through December 3, 2001, District of Columbia: Grand Hyatt Hotel.

Performances:

Abbott, William A. "Bud," and Costello (Cristillo), Louis F. "Lou." "Who's On First?". Author unknown. Perf. Abbott and Costello, The Naughty Nineties, a radio show, various locations, 1943 through 1945.

Internet Uniform Resource Locators:

Center for Information Technology. 26 Mar. 2001. Federal Legislation Affecting Information Management, Bethesda. 28 Feb. 2002 < http://irm.cit.nih.gov/policy/legislation.html >.

Duhaime.Org. C. 2002. Affordable Justice, Duhaime and Company, Victoria. 26 Feb. 2002 < http://www.duhaime.org/dict-d.htm#D >.

Enriquez, Tony. "Pocket NESSUS." SANS Institute Information Security Reading Room (23 Jan. 2002) 1 Page. 28 Feb. 2002 < http://rr.sans.org/tools/pocket_nessus.php >.

Frank, Diane. "Agencies Flunk Security Review." Federal Computer Weekly. (12 Nov. 2001) 1 Page. 28 Feb. 2002 < http://www.fcw.com/fcw/articles/2001/1112/news-score-11-12-01.asp >.

Frank, Diane. "Fed Systems Still Too Vulnerable." Federal Computer Weekly. (6 Apr. 2001) 1 Page. 28 Feb. 2002 < http://www.fcw.com/fcw/articles/2001/0402/web-cyber-04-06-01.asp >.

Lyman, Jay. "Feds, Security Groups Release Top-20 Vulnerability List." NewsFactor. (3 Oct. 2001) 1 Page 28 Feb. 2002 < http://www.newsfactor.com/perl/story/?id=13907 >.

Microsoft Product Support Services. 30 Jul. 2001. Microsoft Corporation, Redland. 28 Feb. 2002 < http://support.microsoft.com/default.aspx?scid=kb;EN-US;q103881 >.

National Archives and Records Administration. 19 Feb. 2002. The Federal Register, Washington. 28 Feb. 2002 < http://www.nara.gov/fedreg/eo.html#orders >.

Nessus. 24 Feb. 2002. Nessus, Unknown. 28 Feb. 2002 < http://www.nessus.org/ >.

The Federal Web Locator. C. 2002. The Federal Executive Branch, Washington. 28 Feb. 2002 < http://www.infoctr.edu/fwl/fedweb.exec.htm >.

The Twenty Most Critical Internet Security Vulnerabilities (Updated). Ver. 2502 30 Jan. 2002. SANS Institute Resources. 28 Feb. 2002 < http://www.sans.org/top20.htm >.

The White House. 12 Feb. 2002. The Office of Homeland Security, Washington. 28 Feb. 2002 < http://www.whitehouse.gov/homeland/ >.

Thomas: Legislative Information on the Internet. 26 May 1998. Library of Congress, Washington. 24 Feb 2002 < http://thomas.loc.gov/ >.

Wikipedia: The Free Encyclopedia. 25 Feb. 2002. Wikipedia, Unknown. 8 Feb. 2002 < http://www.wikipedia.com >.