INFORMATION SYSTEM SECURITY EVALUATION TEAM SECURITY INSURANCE?

Information systems are becoming more complex and ubiquitous. Consequently, the opportunities for compromise increase. Networks once found only in relatively large offices are now found in the smallest of offices. These networks are typically connected to the Internet through Wide Area Networks (WAN). This poses a problem for maintaining a high degree of security in these systems especially where an organization is split into many smaller entities whether dispersed geographically or located in one building. This document proposes an idea that can help these organizations establish and maintain a relatively high degree of security and reduce the risk of disruption of business operations. I will call it the Information Systems Security Evaluation Team or ISSET in keeping with today's need for acronyms.

This particular prototype is currently being developed to improve the security posture of a small federal agency. It is typical of many government agencies that have a mission that requires people to be located in many different states, each operates relatively independently of the headquarters in Washington but must still communicate and share information both internally and externally. There is a headquarters, three regional offices, a finance center, debt collection division, ten field offices and 7 area offices. Headquarters, regional and field offices have their own network with at least one system administrator. Area offices are supported remotely over the organizations WAN. The WAN and its associated firewalls and routers is administered from the headquarters. While this particular prototype is designed for a federal agency, it could be easily adapted for an kind of public or private activity.

Purpose

The purpose of the ISSET is to provide information security expertise to:

- Help the agency leadership meet their responsibility to protect agency information assets.
- Audit agency systems and sites to insure adequate implementation of information security measures and agency policies.
- Validate agency security policy and its consistency with laws and directives.
- Provide a pool of trained security specialists that systems administrators can use as a resource to supplement their training and experience.

Team Structure

There are a number of options for how to structure the team. It should, however, have a minimum of three members. This provides for at least two members to conduct on-site audits and one to cover any issues that occur while the other members are not available. Three members also provide depth to the team to cover vacations, illness or similar absences.

The size of the team could also be affected by areas of expertise. An example would be if the organizations uses several different operating systems. In the agency this team is be developed for networks are using Novell, Windows NT and 2000, Linux, and a couple flavors of Unix. Desktops are operating on Windows 95, 98, NT and 2000. There are certainly some common security procedures for all these however the specific configuration of security features in each require some significant operating system knowledge. Having team members with specific experience in a given operating system may be necessary.

The team should be made up of permanent members but not necessarily full time members. The basis for this is the training necessary to have the expertise to audit security programs. This whole concept is targeted at organizations with limited resources so the costs of rotating and training new team members would probably be prohibitive. This is not to say however that the team members only job is security. Team members may have other duties. They may be System Administrators, Information System Security Officers, or other information technologist that have the adequate training and experience to perform security audits. It might also include experts in the agency's program areas where that knowledge is essential to determining if the appropriate security is being accomplished. The Membership on the team may be an "additional duty" however it is imperative that sufficient time is allowed by the team member's supervisor to allow for training and study so currency in information security theory and practice can be maintained.

Another option is to have a core of permanent team members and then augment that with employees who either have special knowledge of an area or with systems administrators from other offices. There is a bonus in using temporary team members in that it provides them a training experience and can enhance their knowledge of information security techniques and procedures.

Team members also do not necessarily have to be assigned to the same geographical location. The use of groupware, email and phones can accommodate most team activities with perhaps quarterly meetings to go over operational plans, review policies and guidelines, or develop audit schedules.

In the case of the agency this prototype is being developed for, the team is made up of six permanent members as follows

1 – headquarters – program area specialist
1 - finance center – financial applications manager
1 - debt collection division – financial auditor
2 - regional offices – system administrator and information security officer
1 – field office – system administrator

The makeup of this team is influenced by the need to have secure financial systems to insure unqualified annual financial audits. Team members are located throughout the U.S. and get together at various sites for organization and planning meetings. Most business is conducted through email and a custom website.

Supervision

This can be a sensitive political issue in many organizations. It is especially true when the team members are performing the team functions on an "additional" duty basis and in essence have two supervisors, one for day to day duties and the other for the ISSET. However, in order for this type of team to be effective it must be able to operate without any appearance of (or actual) conflict of interest. The team should not report to the Chief Information Officer (or equivalent) or the Chief Financial Officer The only exception might be if the team reports to a board of directors or executive committee and that person is a member of that group. Ideally the team should report to the agency director or deputy director (president, CEO or vice president in a private company).

In some organizations this maybe difficult to accomplish but every effort should be made to have the team supervised by some one with decision making authority and no direct supervision over the systems the team audits or inspects.

Concept of Operations

The ISSET's primary purpose is to insure that the agency's information assets are protected. In order to do this it will be necessary to conduct audits and on-site inspections of the various office's and department's information networks, applications, and services. The team needs to develop audit plans which include a schedule for what will be audit and when. The audit schedule should be published so that each site knows when the team will be there. Audits using automated tools to test the security of servers, firewalls, and routers should also be employed where appropriate to insure the best level of protection is being used.

It is essential that an audit checklist be developed to insure that all areas are covered in the audit. This will be especially important if the team uses temporary members.
The US Government Accounting Office has developed a Federal Information System Controls Audit Manual (FISCAM)[1] that contains some very good information about planning and conducting an audit regardless of whether the organization is public or private. The prototype team will use this as the basis for developing their audit checklist

This manual divides the audit into 6 major categories These categories are: (from FISCAM, Chapter 3)

> • ***entitywide security program planning and management*** *that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls;*
>
> • ***access controls*** *that limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure;*

- ***application software development and change controls** that prevent unauthorized programs or modifications to an existing program from being implemented;*

- ***system software** controls that limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system;*

- ***segregation of duties** that are policies, procedures, and an organizational structure established so that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records; and*

- ***service continuity** controls to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.*

FISCAM further divides each of these categories into several critical elements representing tasks that are essential to establishing adequate controls.

In developing a checklist, tables should be built that list the categories and critical elements that need to be evaluated. These tables can also contain information about what should be checked to validate that the appropriate controls are in place. A table with some sample entries is shown below. Some additional references for developing detailed audit procedures on operating systems is listed at the end of this document.

Control Activity	Control Techniques	Audit procedures	Policy References
Security Plan is documented and approved	A security plan has been documented that - covers all major facilities and operations - Approved by key mangers - Complies with all policy directives (list specifics if needed	- Review security plan - Determine if plan complies with existing policy or directives - Interview key managers and staff	OMB Cir A-130 Agency IT Policy Directive

Facility Mgmt: Visitor Control	- Visitors escorted - access codes changed and controlled	- Review visitor logs - Observe entries and exits to facility during and after hours - Interview guards if applicable - Last time codes changed - review access list	(List any policy directives that apply)
Audit Servers	- Is audit turned on	- checked the server to determine if auditing is activated. Novell- Start Auditcon and check configuration settings, review logs Windows NT/2000 – Start policy editor or user manager and validate audit settings. Use event reviewer to review logs Linux – check config files for level of auditing, review logs	(List any policy directives that apply

The audit checklist needs to be tailored to your organization and the operating environments that exist. It should address the six categories listed above but the critical elements used to determine whether a site has implemented the appropriate security controls will vary with each activity.

How will the audits be conducted?
The team needs to establish some protocols on how audits will be conducted. It is recommended that as a minimum the following takes place.

- An entrance briefing takes place with key managers and IT staff to introduce the team members, outline the purpose of the audit, how it will be conducted and the assistance expected from the activity.

- Auditors should be careful not to disrupt normal activities any more than necessary

- An exit briefing takes place with same managers as the entrance briefing and details of the audit results should be presented as well as who the final reports will go to. Ideally a draft copy of the final report should be left with the activity.

- A common practice is to allow the activity to review the draft report, make comments on it and those comments be included with the final audit report.

SUMMARY COMMENTS

This paper provides on a brief outline of the concept of a IT security audit program. While each organization would have to tailor it to its unique operations, it is essential to start with the major categories listed above to insure that all areas of information security are evaluated. Obviously some activities won't have development programs and others may not have any "sensitive" information so some controls would not apply.

The structure of the team is also dependent on the size and business of the activity as well as the level of information operations. The team could consist of 2 employees or 15. They could be permanently assigned or detailed, it could be a primary duty or an additional duty.

Regardless of how the team is composed it is imperative that management support it with funding, time to do planning, preparation, and conduct audits, as well as training to insure team members competency in information security procedures. Management must also enforce the correction of deficiencies found by the team or the whole effort is a waste of resources.

There are a couple of other functions that such a team could perform and would depend on what the agency's needs are. (Both of these functions will be included in the agency's implementation of this prototype.) They include:

- Serve as the focal point for expertise in risk analysis. Risk analysis is the first step in setting up a good security plan. Current federal government standards do not always require a "formal" plan but it defines adequate security as *"security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act*[2]. Dr. Gerald Kovacich lists risk management as an integral part of an information security program[3]. However risk assessment can be a daunting task and even with the use of software products requires some training and expertise. Many organizations have found that designating focal points to oversee and guide the risk assessment process enhanced the quality and efficiency of risk assessments[4]. This could be a good use of the ISSET resources.

- Serve as a educational and training resource. This derives from the fact that the members of this team should be the most knowledgeable and best trained employees in information security and its related disciplines. The goal of any good information security program is to insure the confidentiality, availability, and integrity of systems and applications. Organizations with geographically dispersed small offices often have limited information system's expertise or perhaps only one computes specialists whose duties include every aspect of information systems management and systems administration. It will often be impractical or even impossible for these employees to have all the necessary training in security they need. The ISSET could be used to develop handbooks, manuals, checklists, or perhaps even conduct classes to provide these technicians with the knowledge and tools to implement the organizations information security program.

There are two schools of thought concerning audit teams. One being that they are there to find problems and punish the employees/managers who allowed them to exist. The other is that they are there as a form of insurance, to make sure that everything is being done that can be to protect the activities information assets. This prototype subscribes to the latter. In that context the teams job is not only to audit but to educate. The goal being to find and mitigate unacceptable risks by identifying them, insuring actions are taken to close the "holes" and to use the information to educate managers and IT staffs on how to preclude similar situations. (It should only become the former if repeated security deficiencies become the norm.) If used in this manner I believe that such an information system security evaluation team can indeed provide **security insurance.**

SOME LINKS TO INFORMATION RELATED TO IT AUDITS

ITAudit.org (http://www.itaudit.org/),
Produced by The Institute of Internal Auditors (http://www.theiia.org/)

There are also some very good references available for specific operating systems including the following:

Windows NT/2000
Windows NT Security Step by Step, The SANS Institute[5]
Guide to Securing Microsoft Windows NT Networks, National Security Agency[6]
Windows 2000 Security Recommendation Guides, National Security Agency[7]
Novell
Novell Netware Security – Administration Guide[8]
Auditing the Network – Netware 5.1[9]

Linux

Securing Linux Step by Step, The SANS Institute[5]

Routers

Cisco Router Security Recommendation Guides, National Security Agency[10]

GAO/AIMD – 12.19.6, Federal Information Systems Controls Audit Manual, Volume 1 – Financial Statement Audits, June 2001.
http://www.gao.gov/ (click on "other publications, then "computer and information technology", direct link to document is not permitted)

[2] Section B, Appendix III, Office of Management and Budget Circular A-130
http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

[3] Kovacich, Dr. Gerald L., Information Systems Security Officer's Guide, Butterworth-Heinemann, 1998

[4] GAO/AIMD-00-33, Information Security Risk Assessment – Practices of Leading Organizations, November 1999. http://www.gao.gov/ (see footnote 1)

[5] Windows NT Security Step by Step, Version 3.03, February 2001, The SANS Institute
http://www.sans.org/newlook/home.htm

[6] Guide to Securing Microsoft Windows NT Networks, National Security Agency, Ft Meade, Maryland

[7] Windows 2000 Security Recommendation Guides, National Security Agency, Ft Meade, Maryland http://nsa1.www.conxion.com/win2k/index.html

[8] Novell Netware Security – Administration Guide, Netware 5.1, January 2000Novell, Inc (http://www.novell.com/documentation/lg/nw51/docui/index.html)

[9] Auditing the Network – Netware 5.1
(http://www.novell.com/documentation/lg/nw51/docui/index.html)

[10] Cisco Router Security Recommendation Guides, National Security Agency, Ft Meade, Maryland
http://nsa1.www.conxion.com/cisco/index.html

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401**	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event