Segregating Your Technology Personnel
Daniel Shaffer

Introduction

Numerous information assurance white papers concentrate on many of the common areas of protecting one's information assets. Look around. Certainly, you'll find no shortage of documents pertaining to installing firewalls, initiating intrusion detection, or implementing monitoring programs, and although these issues are certainly worthy of mention in the information assurance realm, many users continue to overlook an area that could lead to serious compromises in any information system – duty segregation for in-house or contracted information technology personnel.

What is segregation of duties?

Duty segregation (also known as separation of duties) is a fundamental internal control concept focusing on the need to prevent incompatible activities. Essentially, different personnel should perform distinct, key operational activities thereby ensuring some level of procedural review and reducing the risks associated with erroneous and inappropriate actions. Auditors love this concept, and it is generally an area under sharp scrutiny during most information technology reviews. If you don't have sufficient segregation in place, auditors will thoroughly conduct system integrity tests, which means more time spent at your site, which means more time spent with audit staff. For some, that's not considered an unpleasant experience. However, if the subject of being audited causes undue stress, then thoroughly documenting, implementing, monitoring, and enforcing proper duty segregations will permit auditor system testing to be reduced accordingly.

The avoidance of time spent with auditors is not, nor should it be, a serious factor in one's decision to pursue proper duty segregations. Due diligence dictates that duty segregations should be considered a professional and custodial responsibility for any information technology manager's security posture.

The Federal Government, Office of Management and Budget has published OMB Circular A-130[i], which offers the following segregation of duty guidance:

> "Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process.
> Nevertheless, in some instances, individuals may be given the ability to bypass some significant technical and operational controls in order to perform system administration and maintenance functions (e.g., LAN administrators or systems programmers). Screening such individuals in positions of trust will supplement technical, operational, and management controls, particularly where the risk and magnitude of harm is high."

Why implement duty segregations on information technology personnel?

All operational levels in any organization have established controls. Since most of an organization's information is maintained in a small, central location, compared to the large file rooms associated with the pre-information technology era, those desiring to cause harm to a large amount of information in a short time span now have a convenient means to do so. Remember, the Federal Bureau of Investigation recently reported that 71% of those questioned reported unauthorized access by inside personnel[ii]. Information technology personnel should have predefined operational limitations and they should be held accountable for any unauthorized activities outside of those limitations. Furthermore, the knowledge of computer operations held by information technology staff is significantly greater than that of the average user. That knowledge could be used for malicious purposes.

I am not advocating a position of mistrust towards any particular body, and managers should take great strides to avoid the appearance of such while implementing duty segregations. Access to information systems need to be restricted to those personnel having a need for that access – and even then, in a very limited capacity. Rarely does every user need to be a system administrator.

How to implement critical segregation of duties:
Although the organizational structure of large information technology departments vary, the following sub-units generally exist:

1. Development Unit: This unit has responsibility for systems development, which includes maintaining and replacing program code and hardware. The initial program design, as well as its subsequent documentation, development, and testing, will occur in this unit – although these activities should be assigned to different individuals within the unit.
2. Computer Operations Unit: This group has responsibility for ensuring the continuing availability of the systems, including back-up and recovery operations. Many times this unit also assigns a "librarian" function that provides needed system disks, tapes, and documentation to users as applicable.
3. Data Base Administrators: DBAs administer the database for the system owner and users. In smaller organizations, this function may be assigned to the Computer Operations Unit.

The following items represent "best-practices" for ensuring proper segregation of duties at an organization:

1. Information technology departments should be segregated from information user departments.
2. Program developers should be segregated from program testers, and each of their activities should be conducted on "test" data only. This will assist in ensuring an independent and objective testing environment without jeopardizing the integrity of production data.
3. The Computer Operations Unit should not have direct access to program source code. This will ensure that members of the Computer Operations Unit do not intentionally or unintentionally introduce source code that has not been properly tested and it will lessen the opportunity of introducing malicious code. Object-oriented program languages have mitigated some of the risks associated with administering versus developing software. However, it has not been eliminated, and organizations should continued to pursue segregating the two functions whenever possible.
4. Individuals in the Development Unit should be restricted from accessing "live" production data. Again, this will help to ensure the integrity of the data relied upon for operational obligations.
5. Data base administrators should not also be program developers. Allowing individuals to create, promote, and administer a software program is not an advisable practice.
6. The responsibilities of the Computer Operations Unit should be segregated from the Development Unit. The developers create and enhance programs. They shouldn't be able to promote its use on a production system.

Some smaller organizations do not have the resources to implement all of the above-recommended practices. Whether or not resources are available, other control mechanisms, including efficient and effective personnel hiring, bonding, training, monitoring, and evaluation practices, can improve any organization's security posture. Furthermore, the principle of least privilege, which "gives the user no more privilege then is necessary to perform a job[iii]," will supplement any security posture possessing deficient duty segregations.

Large corporations and government entities should also implement assignment rotations for their personnel and ensure that employees are occasionally forced to take vacations. These two practices will assist in identifying long-standing undesirable activities.

Why is segregation of duties being overlooked?
The abundance of off-the-shelf accounting software is enticing many companies to work within the software's canned confines. Since canned software dramatically reduces or eliminates the programming portion normally associated with propriety software development, the necessary segregation between programming and implementation is also reduced or eliminated. This is particularly helpful to those small businesses that simply do not have the resources to support proper duty segregation – not to mention the costs associated with software development and its subsequent testing. However, companies using or developing proprietary software products should mandate proper duty segregations for its personnel.

Conclusion:
The implementation of proper duty segregations will supplement any organization's "defense-in-depth" security posture. It is not meant to be a full-proof control -- no security method ever is, but if used effectively, it will help deter errors and irregularities performed by those developing, accessing, or administering computer systems.

---

[i] Office of Management and Budget; "CIRCULAR NO. A-130"; February 8 1996; URL: http://www.whitehouse.gov/OMB/circulars/a130/a130.html (11/7/00)

[ii] Federal Bureau of Investigation; "Congressional Statement"; April 21, 2000; URL: http://www.fbi.gov/pressrm/congress/congress00/gonza042100.htm (11/7/00)

[iii] Ferraiolo, David and Gilbert, Dennis; "Assessing Federal and Commercial Information Security Needs"; November 1992; URL: http://security.isu.edu/isl/secneeds.html (11/8/00)

Last Updated: August 17th, 2017

Upcoming Training

Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401**	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
Community SANS New Orleans SEC401	New Orleans, LA	Oct 23, 2017 - Oct 28, 2017	Community SANS
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 30, 2017 - Dec 06, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event