GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Segregating Your Technology Personnel

Daniel Shaffer

Introduction
What is segregation of duties?
Why implement duty segregations on information technology personnel?
How to implement critical segregation of duties:
Why is segregation of duties being overlooked?
Conclusion:

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: April 30th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS