Separation of duties (SoD) in Information Technology

The technology group should understand the basic separation of duties issues within the technology area as well as the principle of least privilege. However, technology does not normally have the expertise to determine the separation of duties issues within the business. Although conflicting access rights may be a cause for concern, it is not technology's responsibility to identify these separation of duties issues. However, following the reasonable person rule, technology does have the responsibility to bring a separation of duties issue to management attention when they observe them. The audit function usually has more training and expertise to map business logic to information flow and suggest where separation of duties makes sense. Ultimately, it is business management's responsibility to adequately address separation of duties issues. For daily operational purposes, Compliance may be sought to review user access rights to address separation of duties concerns. Internal Audit would review user access during audits for separation of duties issues. Note that Internal Audit would not do it on a daily operational basis as it would become a separation of duties issues for Internal Audit. Where Internal Audit performs this function, Internal Audit will not have the appearance of being objective during their audit.

Intellectual property is the lifeblood of an organization and process should be designed to protect it. Some specific tips:

Software developers should never have access to production systems. Production systems should not have compilers installed. A configuration management board or equivalent should be involved in the decision to place code that has been developed into a production environment. No code should ever be installed in a production environment that has not been approved. As a general principle development and production should always be separate with no crossover (at a minimum, the root/administrator password on development systems should not work on production systems. Better practice is not to allow developer accounts on production systems and to use network access control so that developer VLANS cannot access production systems other than office automation production systems so they can read their email.) Developers may be granted access to production for emergency changes using pre-established accounts for this purpose at the time of need. Controls need to be implemented to administer distribution. Emergency change procedures should only be initiated for operational problems occurring at night where a process must be completed and developer intervention is required. Additional controls will need to be implemented to ensure that changes are tested and approved properly. This problem is not unique to software development. Change control can be applied to many operational aspects of IT as well, such as having a manger approve firewall rule changes before they are applied.

Source code, or other intellectual property repositories should always have a monitoring counter to detect excessive use. For instance, NNMC might have a courseware repository. Since courses are commonly six days, but there might also be lab manuals, the counter might be set to ten. When an instructor is preparing to teach a class, they download the latest version of the courseware for each day. However, if they download more than ten files from the repository over a certain span of time, an alert might be sent to management or it could even trigger an account logout.

Backups are important and we want to encourage backups, but not everyone that has administrator or super user privilege should be allowed to create backups since this gives them a copy of all of the intellectual property. Approved backup operators should be identified in writing with the appropriate procedures. In general, it is far safer to use disk replication to an alternate site. Backups made to small HDD's that easily fit in a pocket or briefcase are the highest risk. Backup HDD's may need to be produced for regulatory compliance and should be protected in a manner consistent with the sensitivity of the information.

Outsourced maintenance personnel should be restricted to the systems they are working on. This can be done by creating a unique VLAN, or DMZ. All contractors should have contracts that meet the company's privacy requirements, including non-disclosure agreements. A vendor management policy and privacy policy should be implemented and enforced. Privacy Policy needs to address the data classification of intellectual property.

Network and Security administrators have the ability to see anything that is sent across the network. Only authorized sniffers may be used. Only authorized signature sets may be used. When possible, portable sniffers should not be used; use investigation enterprise level devices with a console. Only with written permission should the sniffer be a piece of software on the network administrator's laptop; it is highly recommended to have a corporate device stored appropriately and checked out for use as needed.

Database administrators are the hardest position to control. If you want the database to work, all tables probably have to join. DBAs should only have DBA authority, not root or administrator. It may be possible to encrypt the content of some sensitive fields in the database. Consider tools that manage and audit database access, such as Imperva. All activity for accounts with elevated privileges should be logged and reviewed daily by an independent party. It should be noted that Oracle has made significant progress in the past few years to allow separation of duties.

To enforce accountability, generic administrative accounts should be disabled - and an alert issued if they are used - since generic accounts can be used to bypass role-based access controls. In addition, the principal of least privilege suggests that each Administrator and DBA should have two accounts, one with elevated rights and one with normal user rights. The normal account should be used to perform mundane functions such as checking email, while the account with elevated rights should only be used to perform tasks requiring administrator\\\\super user level access. If a process is particularly sensitive, two factor authentication may be used to further ensure that the person performing the task is the person authorized to do so.

Logging for systems, network equipment, databases, etc., should be directed to a write-only logging system. The logging system should be administered by a group separate from the people

responsible for network and systems administration, and access to the logging system should be role-based so that administrators may only see the logs for their own systems.

Even if IT is the custodian of the information, employee's may be able to access sensitive information. Two classic examples are contact lists and contracts. If a salesperson is leaving an organization, it is a time honored tradition to try to leave with the entire customer contact list. Receiving and providing contracts give a clear picture of the revenue and cost structure of an organization. These should be protected not only with digital means, but also with physical security protections.

Positions involving management duties can create conflict of interest or the appearance of same. The CIO or other officer responsible for roll out should not have signature authority over security or compliance workers or tasks.