COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK AND COMPLIANCE

Avoiding Segregation-of-Duties Woe in IT

By Jaclyn Jaeger ‹ October 14, 2008

With the United States in the grips of an economic crisis, now is as good a time as any for Corporate America to reassess its internal controls. And segregation of duties is always crucial to reducing the occurrence of fraud or error within an organization.

³Generally, fraud tends to increase as the economic environment gets worse,² notes Lynn Lawton, president of the Information Systems Audit and Control Association (ISACA). Segregating duties is ³a good, strong control,² because the responsibilities for particular process streams are divided among several people. If anyone wanted to commit a fraudulent act, collusion would be required, ³which is always more difficult than just doing it yourself,² says Lawton.

Particularly vulnerable to potential fraud are workers in the IT department. ³Most IT people have very wide-ranging access to systems and very powerful utilities,² Lawton says. ³If the duties aren¹t properly segregated, it gives them access to change a lot of things‹possibly innocently, possibly with fraudulent intent.²

According to a segregation of duties matrix published by ISACA, the three IT jobs with the most access and technical knowledge‹and therefore, carrying the most risk of a segregation-of-duties conflict‹are the applications programmer, systems programmer, and computer operator. In each of these jobs, executives should never also give those workers ³anything to do with an end-user role or anything to do with implementing their own changes,² Lawton says.

Take a systems programmer as one example. If that person is also, say, the end-user of a payroll system, he or she has the power to create new employees that don¹t exist and to have them paid in bank accounts that that programmer has access to, Lawton says. The systems programmer could then make sure that those employees never appear on any reports or any screens,

other than when he or she was logged on.

Lee Barken, IT practice leader at accounting and auditing firm Haskell & White, cites as another example what is often referred to as the ³salami attack.² That scheme was made minorly famous as a sub-plot in the movie ³Superman III,² where Richard Pryor¹s character systematically stole a fraction of a penny from thousands of coworkers and directed the sum into his own paycheck.

The result is an ongoing diversion of assets so minuscule that the victims, whose assets are vanishing, fail to even notice. ³Having a segregation of duties can be a control to prevent those sorts of things from happening,² says Barken.

For reasons such as these, access to certain system processes should be severely restricted. Other examples may be if the live software needs to be patched in some area due to interoperability issues with other software, if it opens a new vulnerability, or hurts the program¹s availability. In each of those scenarios, only a software developer should evaluate the problem, calculate implementation costs, design a fix, and review the ramifications of that fix. Another person or group in charge of quality assurance should then perform the subsequent review, inspection, and approval.

And no change to a process should be allowed without the proper authorization given, for example, by an IT governance board or a manager, Lawton says. To ensure proper authorization of a given duty, consider having only a single user ID and password to gain access to that particular system that needs to be fixed, she says.

Barken explains that this could mean having different hardware machines and having people with different access rights to those hardware machines. ³In an ideal software development environment, you really want to separate the people who are doing the programming, the people who are doing the testing, and the people who are moving the code into production,² he says.

A further preventive measure may be to write down that password and lock it in a safe, so if someone wants to access that system, he or she also needs the code to the safe, Lawton says. It¹s an excellent control and demonstrates the risk of sloppy segregation-of-duties. ³If the applications programmer and the computer operator are one in the same person, there are plenty of opportunities to bypass that sort of check,² she warns.

Another important control, says Barken, is having general network security

in place, making sure the network, in and of itself, is ³secured properly, so you¹re not vulnerable to outside attackers.² One such preventive measure is to end the user access rights of any employee who leaves the company immediately, he says.

³With so much volatility in the marketplaces, that should be an issue high on people¹s lists,² he says. ³The risk of disgruntled employees in that environment is heightened.²

This is particularly so in today¹s turbulent economy, where many people are strapped for cash and are tempted to commit crimes they may not normally commit. According to one IT fraud examiner¹s anonymous posting on InfoWorld, for example, certain individuals at a company had access to customers¹ personal information, including phone numbers and home addresses. They downloaded that data onto their desktops and then converted it into Excel spreadsheets, which they would then resell to other parties who want such personal data for sales leads.

Even innocent changes not intended to cause harm to an organization or an organizations¹ clients could still cause problems, if the proper testing procedures are not in place. ³It¹s happened in a number of banks, where relatively minor changes have been made and implemented without going through the testing and led to security breaches,² Lawton says.

In one instance, a change to the security program at one banking organization resulted in certain automated teller machines failing to perform PIN number verifications. As a result, anyone with a debit card could access the cardholder¹s account without knowing the PIN.

In another example, a bank made a change to its Internet banking system, but did not have proper security locks in place. When users logged on the following day, they could see not only their own account details, but also those of the users who logged on before them, Lawton says.

Also important to keep in mind is that job titles and organizational structure will vary depending on the size and nature of the business. Smaller organizations, typically, have to use more caution, Lawton notes.

³The smaller the organization, the less likely you are able to have proper segregation of duties, not just in IT, but in any of the financial and operational roles,² she says. ³Usually in that size organization, the management is very much dependent on their own oversight and their own diligence, and looking at what people have done, and checking the sense of

it.²

³If you can¹t enforce certain controls because of lack of resources‹whether that¹s people or systems‹then you have to be more vigilant on your periodic review,² Barken says. That means either quarterly or annual reviews, depending on the control, he says.

³Small companies are definitely struggling with this [enforcement] issue, but at the end of the day you can¹t eliminate all risks, you just have to manage it as best you can.²

IRS Circular 230 Disclosure: To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. tax advice contained in this communication (including attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code, or (ii) promoting, marketing or recommending to another party any matters addressed herein. The information contained in this electronic transmission, including any and all attachments, is intended only for review and use by the individual(s) to whom the transmission is addressed, and may contain privileged and confidential information. If the reader of this transmission is not the intended addressee, you are hereby notified that any review, dissemination, distribution or copying of this transmission, or any attachments, is strictly prohibited. If you receive this transmission in error, please immediately notify the sender by reply email and destroy any and all electronic and paper copies. Thank you.