BROTEMARKLE, DAVIS & CO. LLP

Putting People First

Reduce Your Risk of Fraud with Good System Security

By Sam Martin

Fraud can occur in any business when all of the following elements exist:

- A person has an *incentive* (pressure) to commit fraud .
- There is an *opportunity* for the person to commit fraud
- The person *can rationalize* the fraudulent behavior (attitude)

A well-designed computer security system is one way you can reduce the number of opportunities for fraud to occur in your business.

Start your security system review by closing these common gaps identified by the The SANS (SysAdmin, Audit, Network, Security) Institute.
http://www.sans.org/top20

1. Default installs of operating systems and applications. Don't install program components that you don't need. They can create openings for potential hackers. Limit the number of people or create a department that has the rights to install programs onto the server or desktops. This will help prevent unauthorized installations which could open a port to the server or allow outside access.

2. Accounts with No Passwords or Weak Passwords. Don't use blank passwords or the word "password" on secure information. Also, don't accept built-in or default accounts. These accounts usually have the same password for all installations of the software and are easy for hackers or criminals to break. (And those 3M Post-it notes containing your password which are taped to your monitor aren't a good idea either.) There should be a requirement that the password be changed every 45-60 days, not allowing the previous password to be used.

3. Non-existent or Incomplete Backups. This really isn't a fraud opportunity, but it is an important consideration for the long term continuity of your business. Ensure that backups are placed in a secure location; leaving the backup sitting next to the server is a creating an opportunity for it to be misplaced or copied.

4. Large number of open ports. Have your IT person check to see if this is an issue in your business. Open ports are easy paths of entry for outsiders who know how to exploit them.

5. Not filtering packets for correct incoming and outgoing addresses. Performing filtering on traffic coming into your network (ingress filtering) and going out (egress filtering) can help provide a high level of protection from outside attackers. Again, have your IT staff ensure that you are taking appropriate steps.

6. Non-existent or incomplete logging. You should have system logs for your operating system and audit trails in your accounting software to keep track of who does what and when. There should be a system in place that will lock out a login name after three unsuccessful login attempts. This will help prevent outsiders from trying to gain unauthorized access to the system through password pirating.

7. Develop the perception of detection. If employees begin to feel that management is monitoring what they are doing on the system, they will be less likely to try to attempt fraudulent behavior. An easy way to begin to establish this is by randomly reviewing the logins with employees to confirm that they logged into the system when the report shows they did so.