"Embracing A Security Audit"

In the April 2004 edition of *Information Security* magazine, George Wrenn writes about "Surviving an Audit". In the article he gives advice from a client's perspective on how to best work with an auditing team, whether the team is internally or externally based. Mr. Wrenn provides many good tips on how to gain the most benefit from a security audit, and most important on what to do after the audit is complete.

In my Information Technology career I have been on both sides of the desk following an audit. Being on the receiving end of an audit can be a very unnerving experience. The normal human emotion is fear and nervousness. The last thing you want is someone from the outside world coming into your organization and pointing out all of your flaws. You can't help but take anything that is said a little personal. My goal in writing this article is to help convince you to embrace an audit instead of fearing it.

Security audits are a vital part of any companies overall security strategy. Policies and procedures are created to guide the information technology staff in managing corporate resources. Budgets are another important consideration when securing company resources. As the economy fluctuates over time, security officers struggle to receive their fare share of the budget. When you add in legal requirements, such as those imposed by HIPAA, GLBA and Sarbanes-Oxley, the job of securing a corporate network can be very imposing.

The final piece of the puzzle is training and real-world experience for security and network administrators. Many security officers perform double duty as network administrators and have little time to stay current on the latest operating system and application vulnerabilities. This is where external security auditing companies can provide a tremendous amount of benefit. The hard part is accepting that someone else will be examining everything that your department has built and making recommendations.

Regardless of why your company is performing a security audit, the overall goal is to increase the security posture and reduce the risk of unauthorized access to company resources. Too often the staff of the company being audited takes the audit personal and allows their ego to interfere. When this happens, the effectiveness of the audit is

diminished. When planning a security audit, it is important that these goals be carefully explained to employees and assurances made that there will be no blame or criticism assigned after the audit is complete.

As pointed out in the *Information Security* article, what happens after the audit is complete determines whether or not the investment was a good business expense. Once the recommendations have been provided, create a plan to evaluate and implement the appropriate recommendations. Some recommendations may not be implemented immediately for many reasons, but make a concerted effort to fix as many issues as possible in the immediate future. The tendency is to put off making changes in one area until changes are completed in another area. In reality, this means that the changes are never completed and the same findings are reported at the next audit.

When budgeting for security audits, always factor in the cost of remediation regardless of who will be implementing the recommendations. Sometimes remediation involves purchasing hardware or software, or perhaps more security training for employees. It is not uncommon for policies and procedures to need updating to match the current business processes.