Health Information Compliance Alert

SECURITY COMPLIANCE: HOW YOU CAN AVOID THE AUDIT CONTROL TRAP

Expert advice to keep your systems running smoothly

Have you pinpointed which of your systems must be audited? Are you reviewing and storing audit logs? If you answered 'No' to either of these questions, you could be headed for a system meltdown. Here's help.

BOOST PERFORMANCE

Audit controls enhance your system's performance by creating a daily record of activity. **First step:** Examine your applications'and system's auditing functions to determine how much activity you can catch and what you need, experts advise.

To benefit from your audit capabilities, you have to make crucial decisions, says **Ali Pabrai**, chief executive and co-founder of Chicago's HIPAA Academy.net. **Important:** Your security officer should draw up a list of what has to be audited "for your system, the applications themselves and any data flowing to the network," he states.

"Make sure you only use the auditing, logging and monitoring functions that you need," stresses **Kevin Beaver**, consultant for Principle Logic in Kennesaw, GA. Auditing "every function and all information going into or out of a computer or across a network," will create unnecessary slowdowns, he explains.

Tip: Know where audits overlap, Pabrai advises. "You'll find there aren't as many things that the application needs to record because the system is providing those capabilities," he says.

Here's the real kicker: "The big performance hit is not from audit controls," confides **Fred Langston**, a principal consultant for VeriSign in Seattle, WA. "The real hit is from the storage and monitoring of audit logs," he says.

SAVE SPACE

You have to audit critical information without recording so much that your logs lose value, Pabrai warns. You don't want to log more activity than you have the resources to review and evaluate, he adds.

"You end up with a high volume of log data that you have to look at, monitor and store," Langston explains. This process could eat up precious system space, he cautions.

Strategy: Make a plan for migrating your log files, Langston recommends. Move your files "after a certain number of days to a centralized place, or burn them to a CD," he advises. This way you can review them and catch any security hits without tying up your resources, he says.

THE BOTTOM LINE

"Be careful not to impact the end user's experience," Pabrai reminds. Time also factors in: "A nurse doesn't have time to wait on audit controls," he stresses.

Audit controls are "necessary evils that are part of general business best practices," Beaver affirms. Yet, with optimized hardware and software, they don't have to be a big concern. Most important: "Your approach to auditing must balance security, convenience and usability," he declares.