

Button Up

Regulatory compliance and data security go hand-in-glove for today's IT professionals.

by Chris Gay

Helping to manage and respond to ever-evolving compliance requirements has become a mainstay for IT professionals in today's insurance industry.

In companies across the country, data monitoring teams are focused not only on maintaining tight security of records, but also preparing for, and correctly interpreting, audit requirements.

Even if no audit requirements were in place, a proactive monitoring program is a valuable tool for responding to mandated compliance regulations. Every day there are more types of security threats that could compromise compliance. Forward-thinking monitoring teams develop compliance management programs that reflect this reality. They adopt daily monitoring of critical files as well as groups, e-mails, public drives, data leakage and

Contributor Chris Gay is director of Disaster Recovery and Monitoring for Blue Cross and Blue Shield of Florida. He can be reached at chris.gay@bcbsfl.com.

other internal processes.

A study by storage management company BridgeHead Software stated that failing to comply with federal regulations, such as the Health Insurance Portability and Accountability Act and Sarbanes-Oxley Act, leaves companies open to huge fines that could cripple a business financially. No insurance IT professional wants to place the company in the position of facing huge financial penalties. The data monitoring team must be able to understand the complexities of the alphabet soup of compliance.

The best-known ingredient in this soup is HIPAA. In a survey conducted by the Managed Care Information Center, HIPAA is the most pressing IT priority among health care providers. Other ingredients in the mix include the forthcoming Model Audit Rule and requirements for some government-affiliated organizations from the Centers for Medicare & Medicaid Services.

A number of tools are available to help in the compliance process and to improve an insurer's state of readiness. One is the National Institute

► **The Situation:** IT professionals must keep insurance companies compliant with ever-changing federal and state regulations.

► **The Issue:** The threat of data breaches has IT monitoring teams concerned that compliance might also be compromised.

► **The Upshot:** A program of best practices that uses the latest technology helps reduce the danger of unwarranted data access.

of Standards and Technology. NIST's software improves information system quality, safeguards patient data and enables secure remote access to servers at approximately 170 hospitals. NIST also allows users to access systems that span multiple organizations without having to re-authenticate their identities.

While NIST has a long track record of offering measurement tools and other assistance to the health care industry, they may become outdated in the future. NIST's standards will be forced to change as regulations become more stringent with advancing technology.

Monitoring Data

In 2008, more than 244 million records containing sensitive personal

information were involved in security breaches in the United States, according to the Privacy Rights Clearinghouse. Monitoring teams must be especially vigilant regarding privileged users, to make sure they don't abuse access rights and that proprietary data stays protected. Many insurance companies have tools that "crawl" their drives and quarantine information so no one else can access it.

Insurers must also keep up with access permissions to make sure there are no loopholes for people to get through. Best practices recommend that monitoring teams re-evaluate their programs regularly and include specific daily, weekly and monthly checks as part of their ongoing program. The ability to track data that leave the network on portable devices, such as thumb drives, is becoming a priority for many organizations. They recognize the need to be preventive instead of reactive.

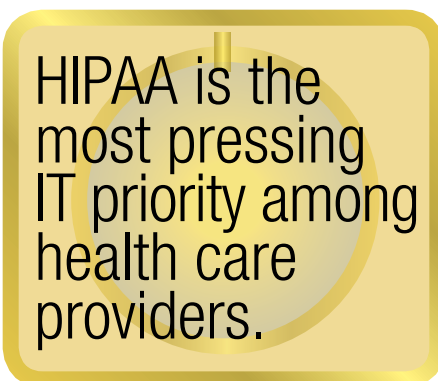
For example, insurance companies are starting to have corporate-approved, encrypted thumb drives that are password-protected, and after a certain number of failed attempts, the thumb drive clears the data on its own.

Most monitoring professionals believe that even if no audit requirements were in place, a proactive monitoring program is a critical element for responding to mandated compliance regulations. It's always better to keep an incident from happening, or to stop it in its tracks, than to lose the data and have to get it back.

If data escape the firewall, hackers can very quickly use it to do malicious things. So, monitoring teams are taking a heightened approach to securing data. Computer security incident management, which involves monitoring and detecting security events on the network and responding appropriately, is becoming popular with many teams.

In a 2008 report, Gartner analysts Eric Ouellet and Paul E. Proctor stated, "We have long believed that integrated network, endpoint and discovery capabilities—with a centralized management console capable of distribut-

ing a consistent set of policies, and providing usable event analysis and workflow for alerting on and remediating violations—was the ultimate goal and destination of this market." Not surprisingly, Gartner has a realistic



HIPAA is the most pressing IT priority among health care providers.

outlook on how to prevent data loss.

Various tools support proactive monitoring, such as those from San Francisco-based SenSage. One of its more useful tools, for example, looks at logs and provides real-time reports, compiling tests into one single location. Dashboards that monitor the entire infrastructure and allow monitoring teams to immediately see threats are also extremely helpful. Other tools notify teams via an automated response if a certain threshold is reached, and then shut down the affected data sector so that nothing leaves the network.

Getting Started

Getting a proactive monitoring program up and running can be a challenge, one that's best tackled with a step-by-step approach. The first is to develop a strategy for monitoring, then setting milestones for implementing and executing it. Make sure senior management buys in and approves the program.

At the outset, everyone is likely to have a different vision for a monitoring program: What will it monitor? How will it monitor? When will it monitor? What type of monitoring will it be? The tried-and-true method for success is to make sure, before implementing the actual program, that everyone is on the same page.

The single best practice related to monitoring and compliance is auto-

mation. Doing all the work manually not only takes more time, but may not even be possible in today's world of limited staff resources. Automation can help by setting a baseline for a server so it's configured a certain way. Tools can notify the team when a setting is changed, and automatically change it back if required.

Automation can ensure that users are constantly monitored to see that they are handling data appropriately. Rules can be set up so that tools shut down at ports when something doesn't seem right; notification then goes to the monitoring team for further action.

A *Wall Street & Technology* article last year shared two revealing statements from New York-based Deloitte & Touche's Center for Banking Solutions, which had surveyed chief compliance officers, chief risk officers and other senior executives.

The survey noted the continued growth of compliance costs since 2006 but found that processes to streamline audits had not yet been integrated within the IT infrastructure of most businesses. Businesses weren't investing in technology tools to help. Instead, their staffs did the work, as if each audit was a singular event rather than an ongoing effort to maintain data security.

Monitoring teams today must respond to both internal and external audits. Sometimes the auditors ask the monitoring team for information; at other times, they turn to the repository of previously requested data, which cuts down time on the front end. The repository is a plus, especially for those audits that occur on an ongoing basis.

Internal audits are usually part of an organization's ongoing compliance initiative. One key lesson here is to not provide more information than what is being requested.

Automated auditing and compliance reporting technology is a definite benefit in today's economy. Automation, either for auditing or ongoing monitoring—or in the best-case scenario, for both—enables the monitoring team to continue to do its best, even if staff reductions occur. **BR**