

# Conditioning for Security Compliance

*Corporations are realizing that the human element is often overlooked in their quest for compliance. Organizations are helping employees make the right decisions by revamping that age-old risk management tool: the security policy.*

By Mathew Schwartz

What's the best way to promote security on an everyday basis for workers, and thus better comply with numerous regulations? To help, organizations are increasing the scope of their security policy.

The goal of a security policy is simple: to help employees know how to do the right thing; accounting for regulations doesn't alter that prerogative. In fact, "all policies are really compliance-related policies," notes David Lineman, president of Information Shield Inc., which sells "Information Security Policies Made Easy," a widely used security policy guide, which is organized in ISO 17799 format, and cross-mapped to various regulations and security standards. "Access control is not new just because it is required in HIPAA."

To promote everyday security, however, organizations must take regulatory requirements into account when designing and updating security and privacy policies. For example, while access controls might not be new to a healthcare company, demonstrating that those access controls are HIPAA-complaint is a relatively new requirement.

With that in mind, here are six tips for companies to assess their existing security and privacy policies, update them, and craft new ones, to ensure better everyday security and compliance:

## 1. Revisit Security Policy Basics

Security policies don't work simply because you write them. In fact policies face two special challenges: "senior management support for the information security function, and making people aware of information security policies," says Lineman.

Interestingly, such challenges are not new. "According to our conversations with customers, the top challenges have not changed in the last 5-10 years, despite the new regulations." And according to the CSI/FBI 2005 Computer Crime and Security Survey, organizations still rank security policies—as well as security management—as the most important areas in which to train employees.

Beyond training and buy-in, however, many organizations—and especially small companies—face an even more basic problem: not having security policies in place, or not enforcing the policies they do have. "There are still many smaller organizations out there that would fall under HIPAA and don't even have any up-to-date security and privacy policies," says Lineman. (One useful starting point for companies in need of policies is the SANS Institute's Security Policy Project, a free, online compendium of security policy templates.)

## 2. Review Existing Policies

To ensure security policies also satisfy regulatory requirements, regularly revisit every one of your existing security policies. (Of course your company should already be doing this on a regular basis, perhaps even employing a security policy steering committee to help.)

When reviewing policies, keep in mind two rules: “We want to enable people to do the right thing, and we want to set the bounds on acceptable behavior for people and the configuration of systems,” notes Stephen Northcutt, CEO of the SANS Institute.

Studied in light of today’s regulations, your existing security policies may need substantial tweaking. “With compliance policy, the real trick is trying to fashion setting the bounds of behavior in a positive tone that people are more likely to receive,” he says. For example, “‘always configure wireless devices to use AES encryption’ is a more powerful statement than ‘never send patient information unencrypted over wireless [networks].’”

Also reexamine security policies in light of today’s top actual security risks. In particular, “data leakage, especially from laptops and PDAs, is becoming a crisis, and managers are starting to lose their jobs—with the Veteran’s Administration and Ohio University as the most recent cases in point,” notes Northcutt. Do your current security policies include guidance to help prevent such data theft, such as requiring IT to include automated hard drive encryption on all laptops?

### **3. Add Compliance-Specific Policies**

Companies may also require entirely new security policies, such as those regulated by Sarbanes-Oxley (SOX). “Policies related to the configuration of IT systems processing—or leading to the processing—of financial data are crucial,” says Northcutt. “In particular, you want to look at your change-management process. There should only be one avenue by which change should occur,” and it needs to be enforced using automated controls.

Meanwhile, HIPAA specifically focuses on safeguarding access to people’s private information, and that requires policies aimed at both information access as well as data at rest. In light of recent data breaches, “in terms of policy, push for encryption of data at rest on the disk, and also implement random audits of access to patient records,” says Northcutt. “You would be amazed at how many people abuse their access to see what is going on with friends and neighbors. Random but fairly [frequent] audits serve as deterrence to bad behavior, and are a powerful control for protecting patient privacy.”

### **4. Keep it Simple**

Whether revising or crafting policies anew, remember users require clear, simple, and short policies that help them do the right thing. Regulations—despite the “bureaucratise” in which they’re written—do not alter this fundamental requirement. “There is nothing about SOX or compliance that forces long, drawn-out policy statements,” says Northcutt. “On the other hand, both lead to a large number of policy statements, so they really do need to be concise and clear.”

In the past, when it came to security policies, organizations often battled employee apathy. In an age of identity theft and spyware, however, there's a bright side: "The massive security problems that individuals have at their home computer makes them much more likely to see the benefits of security at work," says Lineman.

### **5. Find a Security Policy Framework**

Companies with well-established security policies often have a policy management problem and they don't want to have to maintain a separate access control policy for HIPAA, SOX, or any other regulation. Instead, they want one access control policy that demonstrably complies with all applicable regulations.

To address this goal, organizations are increasingly adopting security frameworks such as ISO 17799. "That's the 'unified compliance' approach that you now here a lot of people talking about," notes Lineman. "Hang your hat on a common framework, and then show how coverage overlaps between the various regulatory requirements," and map the framework to different regulations, or even to such IT service or governance best practices as ITIL or CobiT.

### **6. Understand the Limits of Policies**

Security policies help codify the practices needed to keep a company secure. Remember, however, that policies only go so far and simply won't arrest some of the most prevalent security, privacy, and --by extension-- regulatory threats, and especially the ones focused on physical assets. "Two of the recent high-profile losses of customer information—including the VA case—are related to theft. Thieves break into a house or car and take the laptop, because a laptop with a quarter-million financial records is worth a lot more than jewelry or stamp collections," says Northcutt.

Security policies must also take these non-network types of threats into account, since they pose an equal risk to corporate data. "As bad as things are on the cyber front, never underestimate the power of brute force," he says.