

The Bulletin

Technical Tips

By Tom Snyder Ph.D.

A Holistic Approach to Compliance

Few issues in the last couple of years have been more bewildering and frustrating for organizations than government rules regarding the security and retention of electronic data.

More than one organization has probably wished there was a way to comply, in one fell swoop, with all the regulations, from the Sarbanes-Oxley Act to the Health Insurance Portability and Accessibility Act (HIPAA) to California's SB 1386.

Unfortunately, there is no checklist for complying with all the rules. But there are some basic strategies companies can use that will help.

Be security and privacy conscious

Simply being security- and privacy-conscious goes a long way toward compliance. For example, a company that implements sound user authentication practices is going to do better at protecting personal health information -- a major requirement of HIPAA. Strong user-authentication processes, along with other security policies, may also constitute "internal controls," which companies are required to have under Sarbanes-Oxley. And implementing a sound security plan would defend against the consequences of SB 1386. That law, which affects all companies that do business in California, requires them to notify a customer when there's been a security breach regarding that customer's personal information.

It's all in the planning

Planning for the regulations is often an enlightening process. Preparation makes companies concentrate on areas, such as security and privacy, in ways they may not be used to. For example, many federal regulations require a risk assessment. A thorough risk assessment may show holes that the company didn't know existed. A risk assessment may also help identify programs to cut.

The risk assessment stage is one area in which thinking holistically about compliance can be fruitful. A good strategy is to have one risk assessment for all the regulations. Or, if that's not possible, use the same firm for the assessments.

Mark Doll, Ernst & Young's director of security and technology solutions for the Americas, was once asked by a client to reconcile a HIPAA risk assessment with one for the ISO 17799 standard."It would have been cheaper for us to have done a new assessment," he said.

Don't be myopic in your approach

Companies sometimes take a myopic approach to compliance. They think of compliance as an issue for specific departments, rather than the entire organization. For example, HIPAA requires that patient data be handled properly. So a company may implement procedures for protecting the servers housing that data. The problem with this approach is users outside the department housing the servers won't be sure which data is or is not private and may not know the proper procedures for handling private information.

To avoid such issues, an organization needs to assemble a group that oversees compliance. For example, in larger organizations, a chief risk officer (CRO) is often appointed. Ideally, the chief information security officer and the chief security officer, who handles physical security, would report to the CRO. The chief security officer should be involved in compliance efforts because the regulation of physical security, such as access control, is an important element of both the Gramm-Leach-Bliley Act and HIPAA.

Compliance can also reach beyond company boundaries. A company that falls under SB 1386, for example, needs to add language to its contracts so that partners know about issues that may be problematic. For example, if you have an offshore outsourcer, you need to add language to their contract that requires them to notify you if their information systems get compromised. This will allow you to notify your customers and fulfill your obligation under SB 1386.

Given the above and the fact that your compliance group also needs to communicate with the rest of the organization on how compliance affects their daily actions, you may want to add legal and department head representatives to

your compliance over site group. Please visit www.isaca.org/cobit for the best compliance resource we've found to date.

===== If you have questions or concerns about your particular situation, please e-mail me at tpsnyder@xantrion.com. I will use your input to direct future columns. =====