

Compliance Strategies: Compliance does not equal security, security does not equal compliance

By Randy V. Sabett – ISSA member, Northern Virginia, USA chapter



Earlier this year I wrote about the problems that can result from the misperception that “compliance equals security” and the dangers from the associated complacency. That view, however, only tells half the story. The complete thought (which I emphasize with my clients and during my speaking engagements on this topic) is that neither “compliance equals security” nor “security equals compliance.” Instead, a compliance strategy must be based on a pragmatic approach to security.

We can easily show, via numerous previous cases, that compliance does not equal security. Just a cursory glance at some of the higher profile data breach cases bears this out. Going back to 2005, CardSystems was compliant with the predecessor to the PCI data security standard and yet ended up suffering a breach that resulted in a sell-off of its assets to PayByTouch. Several years later, TJX was reportedly PCI-compliant at the time it suffered a breach. More recently, Hannaford Markets suffered a breach after gaining PCI compliance.

What exactly, then, do these examples mean? Is the standard defective? Is the compliance process flawed? Or does it mean that certain organizations fell out of compliance after having gone through an audit? Perhaps the hackers have simply gotten smarter? Actually, it could be any of these. The point, however, is not to look back and determine what the problems might have been. Instead, organizations should learn their lessons from these cases and design their compliance strategies accordingly.

Two specific techniques have proven effective in past engagements for creating an effective compliance program. First,

compliance by a company or other organization inevitably involves an audit by a third party. As such, consistency amongst all people responsible for responding to the audit is critical. Keeping a mind set of having a “united front” can help facilitate that consistency. In a nutshell, a united front means that every person in the company having a responsibility in the audit process responds the same way for a given situation. In order to achieve a united front, different companies have used different approaches but perhaps the most important is having an effective internal audit function. This allows the company to practice in advance of the actual audit by the external auditor. As a colleague of mine says: “Internal audit is our friend.”

A second effective technique for putting in place an effective compliance program applies to organizations having multiple compliance requirements (e.g., HIPAA and GLBA being applicable to the same company). In such an instance, having a cross-compliance matrix has proven to be an incredibly valuable tool. Such a matrix can allow a company to map its information security controls to multiple compliance requirements that originate with different standards. Utilizing such a matrix can show where additional controls might be needed or where a particular control can actually help meet multiple compliance requirements.

I would be remiss if I did not mention here that the legal department within an organization can play a vital role in both developing a united front and also performing cross-compliance. Since compliance often calls for interpretation of rules and requirements (that of-

ten stem from actual laws), the input of a company’s attorneys can help guide the compliance program of that organization.

Ultimately, though, compliance must be tied back to good security practices. A client of mine once said that the best approach to compliance involves four straightforward steps. First, determine the threats to your network and assets (i.e., do a threat and risk assessment). Second, assess what can be done that is within budget to protect those assets and implement accordingly. Third, determine what minor adjustments must be made in the security of the system to not only be secure but also to meet all necessary compliance requirements. Finally, determine what additional provisioning might be necessary to meet any outstanding compliance requirements.

So the takeaways this month are straightforward – perhaps for many in the audience they are not only natural but pure common sense. First, present a united front to the external audit function. Second, use a cross-compliance matrix to address multiple requirements. Finally, make sure that in meeting your compliance requirements, you have not left a gaping hole in your security.

About the Author

Randy V. Sabett, J.D., CISSP, is a Partner in the Internet, Communications, and Data Protection (ICDP) practice group at Sonnenschein Nath & Rosenthal LLP, an adjunct professor at George Washington University, and a member of the Commission on Cyber Security for the 44th Presidency. He may be reached at rsabett@sonnenschein.com.