THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor, Kirk J. Nahra, CIPP
October 2011 • Volume 11 • Number 8

Getting support for privacy and data compliance: not a hard sell if done right

By Ronald Raether, CIPP

It is that time of year again. I am not talking about football, corn mazes and haunted houses. No, I mean budgets and funding for next year's projects. For employees charged with data privacy and security, this period can be particularly frightening. What will I ask for this year? What will I end up with at the end of the budget process? Maybe I should just ignore compliance for another year?

When I first started dealing with privacy and security, these questions were easy to answer. My clients were either defendants in litigation, the subjects of government investigations, or both. It was easy to get approval for resources to address all issues. The desire to avoid fines and judgments was present and real. But without the immediate pressure of a crisis, it can be harder to get these resources even though the threats of fines and judgments are still real.

As I have said before, a dollar paid now can saves hundreds in the future once an incident occurs. Companies that failed to adopt solid compliance programs can speak to this point; the numbers of affected companies are increasing, so the chorus is becoming louder. With HIPAA enforcement on the rise and the new Consumer Financial Protection Agency, the number of companies forced to pay large sums of money to address issues in the middle of a crisis will only increase. Compliance just cannot be ignored.

The place to begin is defining what projects to include, which alone can be daunting. Even with experienced companies, each year brings a host of new issues. With the Massachusetts privacy law, employee privacy issues, social media issues and the broadening of HIPAA's business associate rule (regulating companies and individuals that handle data for doctors, hospitals and insurers), many companies are just beginning their journey into the privacy maze.

While the knowledge and experience may be different for each entity, the practical questions remain the same: What projects should I champion? How will I get executive support, i.e., funding?

Stated simply, the goal should be to demonstrate quick success to management and eliminate risk and maximize protection for consumers. I have seen too many companies that want to eliminate every privacy and security risk immediately (usually because no one knows where to start). The projects become unwieldy, result in cost overruns and often do not solve the issue and reduce the company's risk of fines and judgments. Rather than wanting to immediately resolve all privacy and security problems, you should define discrete projects that have defined and timely deliverables.

So where to start? I always begin with a five-question survey that is sent to each area of the business where sensitive information may be collected, stored, accessed or distributed. These questions cover topics such as what personal information is kept, its source, and how it is used. With the questions, one can quickly determine which areas of the business have regulated data, what laws and rules likely apply and, most importantly, the level of risk posed by that business or function.

You can then focus your energy on those sensitive areas of the business and determine what rules, processes and procedures currently are in place. At the end of this process, the company ends up with a list of issues that require attention, the level of risk and the amount of effort required. One note of caution here; I would include counsel in this process as the final product will list weaknesses in the existing compliance structure and the company will want to claim privilege.

So what should be on this list? As I mention above, the goal is to identify projects that will deliver timely, solid results. The temptation should be avoided to define the project as "compliance with all HIPAA requirements applying to a business associate," or "creating a comprehensive plan for compliance with all European directives on privacy." Rather, identify discrete projects such as creating a breach notification plan or creating a policy for cross-border transfers of our employee data at the German facility.

Even better, identify projects that have utility beyond just the business unit or practice at issue. For example, many laws require a breach notice plan. The creation of a plan satisfies requirements in HIPAA, the Massachusetts regulations, the laws of 47 other states and beyond. Improving discrete areas of the company's data security regime is another example of a project that can achieve results across numerous business units and improve compliance with multiple laws.

It also is important to think beyond just the risk avoidance factors. Identify projects that provide a marketing advantage, provide enhancements to existing products and services or maybe even develop a new product concept. For example, with one client in the software services industry, assurances of compliance with HIPAA provided a market advantage to its customers who were now looking at compliance with the HITECH Act's business associate requirements. To state the obvious, it is much easier to get funding for a project when revenue—not just cost avoidance—is involved.

Also, good compliance is a long-term process; it actually never ends and is iterative. A company cannot achieve compliance at a single point in time and then ignore issues going forward. In other words, each year these budgeting issues will come up. Likewise, we all know that funding priorities change throughout the year. For these reasons, it is important to have frequent deliverables with quantifiable results. A progress chart that has completed items instills more confidence than a chart that has even 95 percent complete beside a project.

Privacy and data security compliance presents unique challenges mainly because many companies are unfamiliar with the issues presented. Climbing a mountain without the proper equipment is challenging enough; not knowing the size or features of the mountain makes the challenge even greater. With the right expertise and guidance, these challenges can be overcome, and the road to compliance can be less intrusive and less costly. Bottom line, the goal is to enhance compliance with applicable laws in the most cost-effective and efficient manner. Demonstrating these concepts to the business will not only improve the budgeting process but also provide the company with the best path to compliance. All admirable goals.

***Ronald Raether, CIPP**, is a partner at Faruki Ireland & Cox PLL in Dayton, OH.*