White Paper: Best Practices for Structuring a Strong Corporate Information Security Policy Process

By Brian Gray

In the age of fast information, one of the biggest challenges that companies have is keeping their information secure. To be successful, companies must effectively cover many different areas such as users, technologies, mandates from third-party agencies, as well as threats. Companies often respond with knee-jerk reactions once a breach or a threat has been identified; in this white paper, I propose that the extra time spent creating strong corporate policies, standards, and procedures will help reduce, if not altogether prevent, the need for such reactions. A security posture founded on a holistic approach to documentation begins a strong framework for an organized and affective information security department where efforts can be better focused on protecting an organizations intellectual property.

The Outside Story

Depending on your organization, you may or may not be aware of outside agencies or governing bodies that have an input into your information security. If you work in healthcare, you are likely very familiar with the Department of Health and Human Services' HIPAA guidelines, or perhaps the Food and Drug Administration's guidelines that must be followed during pharmaceutical development. If you're in the e-commerce industry, you hopefully are aware of the Payment Card Industry (PCI) standards. And, most businesses are aware of the compliance requirements that stem from the Sarbanes-Oxley (SOX) act.

For many, audit times can be filled with stress and fear. However, if you begin your security policy path with the applicable standards and provide traceability back to them as you progress in your planning, you will find that audits are no longer as anxiety-provoking as they once were. Because each of these groups, and others like them, issue standards that are updated every few years, you have a slowly-changing collection of standards from which to start your internal discussion. It's important to note, though, that these standards are not actionable at the organization level. You could not take them an implement something from the standards directly as a user procedure. There needs to be some translation and modification of these standards to make them work for your business environment, and this is where your security team comes in.

Highest Internal Discussions

Within many organizations, implementation of these standards is sponsored by a centralized point of authority and responsibility for authorship and compliance. These organizations may live in different departments and be staffed by different people

depending on your unique organizational needs, but these groups all have one common theme: Successful internal standards implementation must be provided by an overlying corporate mandate. This corporate mandate gives the internal standards team its charter and direction, and formally tasks the team with ensuring that they are the starting point for how external standards are brought into the company and integrated into the corporate culture. They have a very important job, as they are the ones who will need to have deep understanding of the third-party standards, and they will make the first determination of how these standards are to be brought into the organization, while at the same time maintaining audit compliance.

This highest-level internal team is most often made up of representatives from multiple departments. It's very important when you are forming this team that all appropriate departments are included in this team's important work. Their work often focuses on the review of third party standards and the determination of which standards are appropriate for their given business environment. For example, an encryption standards document that offers ten different types of encryption might not be fully relevant because the company only supports three of the ten encryption technologies.

Once the internal standards team arrives at a decision of which of the third party's standards are to be followed, this information is provided to the appropriate teams for internal policy creation.

Creating Internal Policies

The internal policy team(s) are tasked with receiving the standards that the internal standards team felt were most relevant to the organization and creating corporate policies that support those standards. Depending on the subject area, these teams may be cross-functional, e.g. consisting of business and technology members, or single-functional, e.g. consisting only of technology members.

At the core of their work, the internal policy team is to create objectives, requirements, and rules that address what the company needs to do to meet the standard, who needs to do the activities, what actions are acceptable, and why. There is a critical component to this work, however, and that is that the internal policy team should never directly address ***how*** a standard is to be met. Including this level of direction at this level will unnecessarily open the company up to audit scrutiny. Instead, well-written policies produced by a highly organized and recognized internal policy team provides an audit trail that makes it simple for an auditor to ensure the standards are being addressed and met within the organization.

Because the goal of this process for most companies is ultimately audit compliance, the process for creating and approving these policy drafts must be highly vetted and highly organized. Document drafts should be created and provided for review and acceptance by the internal standards board and other high-level, internal organizations. Once these drafts are approved and accepted, they policies become part of the company. Often, they are in effect for five to seven years.

The Role of Corporate Standards

The concept that the policy team is not to answer the question of how the third party standards are implemented in the organization makes many uncomfortable. Their instinct is to make the third party standards as consumable and implementable as quickly as possible so that they can get back to their daily work at hand. For the reasons mentioned above, primarily that of unnecessarily opening up audit issues, there is more work to be done. When the policy is initially approved, it still is a very idealistic, theoretical document that could be implemented in many different ways of implementation in the organization. If simply sent to the users at this point, the company would have a tremendous problem because the policies would be implemented differently by individual users – that is, if the policies were implemented at all. Some internal planning is definitely called for in the form of the corporate standards board.

The corporate standards board is most often a cross-departmental effort that has the goal of creating highly suggested actions, rules, or regulations designed to provide the newly-created policies with the internal support structure and specific direction to be meaningful and effective across multiple departments. At this level, the corporate standards board provides specific technical requirements and details that need to be met within the company. Members of different departments meet, review the policies, and agree that they will address specific policies in similar ways, coming up with appropriate communications that will go downward into their respective departments. It's critical to note here that this team is not responsible for determining ***how*** the policies are to be implemented. We have all likely experienced the firsthand reason for this: if you have ever been asked to complete an activity that you know was created by someone who has no idea of your job, you know firsthand the frustration that would result from dictating how to specifically address policies at this level. Because this information could potentially be audited as well, the corporate standards board should be highly organized, and their recommendations should be thoroughly vetted. The work products of this group should typically be in existence for three to five years.

Finally: Getting to How

At this point, let's take a moment to pause and reflect on what's happened so far. A third party has issued standards that they will expect compliance on in an upcoming audit cycle. A standards review team within the company has reviewed these standards and determined which are appropriate for their company. They have passed this information on to the policy team, who has generated appropriate corporate policies by blending organizational information with third party standards expectations. These policies have then been passed on to the corporate standards board, who determines the approach to handling these new policies to ensure consistency within departments across the company. Finally, it's time to get to the question of how employees will meet these standards, and this comes in the form of procedures.

Procedures provide a company a high-level, functional definition of what is to be done under their roof. These procedures must be traceable, e.g. they must have roots somewhere up the standards workflow. They shepherded by teams that are both cross-functional and cross-departmental, and they lay the framework for how the policies and standards are to be actually implemented within the company. Thinking of them as operational steps or methods for how to achieve shared company goals is appropriate at this point, although they will likely not contain individual tasks or finite steps at this point because of their cross-departmental focus. The main difference between the procedures team and the internal standards team lies in the distance from the workers. In many organizations, the procedures team may consist of team leads or managers from different groups or departments. The internal standards team may consist of directors or vice presidents.

Like the other steps in the workflow, these procedures must be formally approved within the organization, and because they're created in conjunction or collaboration with multiple business units, it's critical that there is user or departmental buy-in to be truly successful. Done thoroughly and properly, the lifespan of company procedures produced in this way is generally one to three years.

The Most Specific Level: Processes

Once the departments have agreed on procedures, it's now up to the local departments to determine the processes that they would like to employ to meet the standards. Processes reflect the end of the line for the workflow that began with the standards review board. They provide the most functional definition of what to do, and answer the question of how to accomplish specific tasks. Like the other processes and documents in this workflow, the processes must be fully vetted and appropriately managed. By living at the local level, they can be created by workers who have the highest level of subject matter expertise for their jobs. This intelligence can ensure that the steps needed to maintain compliance with standards – resulting in a good audit – are easily and painlessly adapted into the workers' days. Departments should be aware that processes can change quickly, and they should easily be able to adjust to changes in technology and improvements in overall organizational process efficiency. Most processes have a lifespan of about one year, and changes are often driven by technology improvements.

A Note About the Role of Audit:

During an audit, you should be aware that policies, standards, and procedures are open and subject to audit because these are corporate-level, cross functional activities. Processes are not visible to auditors because they are worker-level, worker-defined steps that drive the daily work toward meeting a prescribed goal or requirement. When a company opens this level of information to audit scrutiny, the company is accepting a significant risk. At the process level, actions should be custom-designed steps that meet specific business unit or worker-level needs to accomplish or meet the corporate procedures, standards, and policies. The bottom line is that auditors may not have the complete or appropriate level of contextual understanding of the subtleties of the actions

needed at the business unit or individual level. By exposing these processes to audit, a corporation is essentially asking for the auditor's opinion in areas in which they may not have appropriate expertise.

Brian Gray is a Security Analyst with Norfolk Southern Railroad in Atlanta, GA.