InformationShield

5 Steps to Documented User Compliance

By David J. Lineman

In today's regulated environment, organizations are responsible for educating employees on information security policies. In this paper we present 5 key steps for providing audit documentation that all employees and contractors have read and understood the information security policies that apply to them.

I never saw that policy!

Many large data breaches have occurred in recent months as a result of laptops or portable devices, which contained unencrypted sensitive data, being lost or stolen from employees. In some cases, companies have issued statements to the effect that "our employee was acting against our stated policy."

This is an interesting defense, since it could be interpreted as a statement that "we *have* information security policies, but our employees are not aware of them or not following them." Which is the greater lapse – not having policies at all, or having policies but not educating users on how to properly follow them? Of course, neither of these is acceptable if an organization is following a program of due-care in writing and maintaining information security policies.

This is also shaky legal ground, since in many instances employees who were terminated for not following policies, and claimed ignorance as their defense, where later reinstated because the organizations could not demonstrate in court that they had used due-diligence in training their employees on the policies.

Legal issues aside, these breaches do point to an interesting question that all organizations should be able to answer: How do we know that everyone in our organization has read and understood our information security policies? Furthermore, if we got into a legal or audit situation, could we demonstrate

this to a 3rd party? In the following sections we discuss five steps that organizations can use to design a security policy program that can answer these questions.

Step 1: Target your documents

The first step in creating an auditable security policy program is to start with the end in mind. Our goal is to be able to show management a report which documents (1) that everyone who is supposed to read a particular document has done so, and (2) that everyone who claims they have read it can demonstrate this by passing a very basic quiz about the information in the document.

To accomplish this end goal, you must first start by targeting your documents at various user roles within the company. In other words, policies that should be read by every user, such as internet acceptable use, should not be lumped with policies designed for a limited audience, such as technical auditing policies for servers. Each document should have a target user role as its primary audience. This is a critical first step that enables the rest of the reporting and auditing process.

Step 2: Publish your documents and require acknowledgement with auditable tracking

Documents should officially be "published" to the user population they are targeting. For example, an email message from the CEO could be sent to all employees announcing the importance of the new Acceptable Use Policy that everyone is required to read.

Once users are directed to an intranet site or other system that can perform electronic tracking or logging, users should be required to provide digital acknowledgement that they have read and understood the policy. This step provides the greatest technical challenge, but these features are now readily available in workflow, document management, computer-based training, and email programs, or via dedicated policy document software.

Step 3: Create consequences for non-compliance

The publishing process should include the consequences of not reading and digitally "signing" the documents. The consequences for not participating in the policy auditing process can be different than the consequences of not following the written policies (which would be included in the policy documents themselves). For new employees, they might not be allowed access to email or other critical systems until they have demonstrated their knowledge of policies. For existing employees, cutting off key IT privileges, such as internet access, after a period of time can work as an enticement. Of

course, managers at all levels must be responsible for overseeing the compliance of their staff.

Notice the fundamental difference between this step, and the generic statement by management that "information security is important and everyone should know our policies." The formality of this process not only sends a clear message of management support, it provides a precursor for the possibly more severe consequences of not following published policy.

Step 4: Test user's knowledge with a basic quiz

Digitally "signing" documents should be the first step. Next, users should demonstrate their knowledge of key policy documents by passing a quiz or CBT module based on the policy content. Each organization can use their own judgment on how formal they want the quizzes to be, and how much knowledge is required for a passing grade. The idea here is to force the user to pay attention when reading the documents. Organizations who want to add some positive motivation can create drawings for prizes for all people who pass one or more policy quizzes. It is an easy way to both motivate people and demonstrate management's commitment to information security.

Step 5: Run management reports

The final and most technically challenging step is to run management reports that summarize the compliance process. A key report would be a summary (see table 1) showing all employees, grouped by department or organization unit, whether they have read the policy, and their quiz scores. These reports can be compiled manually or through custom reporting from intranet servers. For organizations who wish to track this information to more granular levels, including multiple policy documents and multiple departments, automated policy or CBT software can provide these reports.

Table 1: Sample Policy Compliance Report

Department	**# of employees**	**# read (%)**	**Quiz Score (Ave)**
Marketing	100	80 (80%)	80%
Sales	200	100 (50%)	85%
Finance	40	35 (90%)	90%
Engineering	150	105 (70%)	88%
IT	20	20 (100%)	95%

Once management reports are gathered, progress can be demonstrated on a weekly or monthly basis until you can make this important statement: *We are confident that everyone in the organization has read and understood our information security policies, and we have auditable data to prove it.*

Automated Solutions

These "simple" 5 steps might appear daunting to organizations with thousands or tens of thousands of users. However, modern policy automation software packages, such as the VigilEnt Policy Center ™ by NetIQ provide complete solutions for this problem. Other workflow automation tools, such as document management systems or computer-based training systems can natively provide these functions or be customized to do so with varying degrees of effort.

In the end, providing this level of auditable data will not only create a more effective security policy program, it will demonstrate to both employees and external auditors that your organization is serious about information security, and is willing to take the steps to prove it.

References:

[1] Information Security Policies Made Easy, by Charles Cresson Wood, CISSP, CISA, CISM. Published by Information Shield, Inc. 2002-2005. [http://www.informationshield.com]

[2] VigilEnt Policy Center – Automated information security policy management software. [http://www.informationshield.com/vpcmain.html]