This is the second part of a guest article presenting an analysis of compliance issues by Graydon S. McKee IV, CISSP, GSEC and Joseph Faraone, CISSP of Unisys Corporation.

* * *

In the first part of this two-part article, we reviewed developments of federal guidelines presented in the National Institutes of Standards and Technology (NIST) “Special Publication 800-53: Recommended Security Controls for Federal Information Systems” <http://tinyurl.com/mq3cp> and the soon-to-be-released Federal Information Processing Standard (FIPS) 200 that will be applied to US federal information systems.

Those in the private sector are probably scratching their heads right now wondering why this should be important to them. NIST publications and the methodology for conducting certification and accreditation are freely available and constitute an untapped publicly available security resource. Inputting the government regulations (Sarbanes-Oxley, Health Insurance Portability and Accountability Act, etc.) into this framework allows the private sector to document, measure, assess, track and report upon the security posture of their information systems and how well government regulations are adhered to. The private sector can now assess the maturity of their information security programs and determine how well these programs integrate into their overall business processes.

A word of warning however: You are still at risk of missing the forest for the trees.

Although NIST has developed and framed their guidance to allow for the proper view of information security management, it is often applied improperly. Managers place their emphasis on simply being compliant rather than leveraging the power of the framework to assess the effectiveness of their programs. They go through the motions to be compliant and focus on the required technology and checking boxes.

The two most basic elements of any system are overlooked or under-emphasized: the information being protected and the people who use the information. You can put in all the high-security devices you want in a system, but if you do not account for the people who need to use the information system, you still will not be secure. We believe that the comment about the “choice of either being secure or being compliant” mentioned in the first part of this analysis was referring to this conflict between security and usability.

People are the key to everything. We need a holistic view of the network and security with the emphasis on being secure. Compliance is simply a milestone on that journey.

The beauty of this is that the information that you need to implement this framework is _free_ and fully available at the NIST Website <http://csrc.nist.gov/publications/nistpubs/>. Do you need to hire high priced consultants to come and set this up for you? No, you don’t. Although
consultants can save you some time on the learning curve, the guidance available through NIST will allow you to begin the process on your own. You can then use consultants to give you an independent review of your program or to bolster areas where you might feel less comfortable. This efficient resource utilization in turn allows you to prioritize on areas that need to be improved.

The CIO implementing this approach can concentrate on the details of how information is protected and used rather than scurrying about wondering how to bring order to the new herd of cats that legislation has unleashed.

Where to begin? Take the framework that NIST has so diligently given us; plug in the requirements that you are subject to, and then sit down with your network architects, your user representatives and your key project managers and find a way to work efficiently but securely. With the NIST framework, you will be able to assess, measure, track, and deliver a more secure and user-friendly network and in the process: achieve compliance.

Alternatively, keep enjoying your view of the forest.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay, G. S. McKee & J. Faraone. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.