Organizations should always be looking for ways to minimize their exposure to legal entanglements. No one wants to be sued, to be subject to regulatory sanctions or to become involved in criminal prosecutions. As an information assurance (IA) professional, you will consistently be called on to ensure that your employers or your clients are compliant with all relevant regulations; you may be asked to verify such compliance as part of your job and in collaboration with or as principal in audit procedures that protect the organization by demonstrating due diligence in the exercise of fiduciary responsibility.

Security consultant Gordon Merrill continues his series on fundamental management tools for IA professionals in general and IA security consultants in particular. His insights and recommendations will also help clients choose consultants wisely and judge their performance appropriately.

* * *

Looking at the Record

When you take on the task of assessing compliance with the regulatory and legal environments, whether as a new task in your existing position, as a new job, or as a consultant approaching a new client, you should ask the organization for all previous compliance reports for at least the past three years. If necessary, a client can protect trade secrets by sanitizing the reports, but you should already be under non-disclosure; indeed, as a security professional, your default state, with or without a contract, should be non-disclosure (talking about confidential details of a client’s business to someone else is a kiss of death for your career).

Kazman, Port and Klappholz, in their article “Risk Management for IT Security” in the Handbook of Information Security, Volume III (Wiley, 2006; ISBN 978-0-471-64832-1, p. 786-810),<http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471648329.html > argue that a consultant needs to see how a potential client views compliance before deciding to take on the risk of a contract. For example, one red flag is repeated failure to meet compliance for the same requirements; you are going to want to find out why. If they seem to think they are not responsible for a certain compliance regulation but you know that they are, there may be serious problems. An IA professional I know spoke with a potential national client in the nursing home business and was told firmly that they did not need to worry about any compliance regulations because they were a private company. The consultant politely ended the meeting, excused himself, and left quickly. Being private only got them out of regulations like Sarbanes Oxley; it did not excuse them from regulations concerning personally identifiable information and the handling of Medicare funding.

Legal Appraisal

If you are an employee, you must form a close and constructive relationship with the Corporate
Counsel to help assess issues of compliance with laws and other statutory and mandatory regulations. If you are an external IA consultant, you should be working professionally with an attorney who has experience in the court room on compliance litigation. The attorney’s expert opinion on compliance matters is essential; you must never be put in the position of offering legal advice or legal opinions, since it is illegal in the United States for nonlawyers to dispense legal advice (for more information see the American Bar Association’s “2009 Survey of Unlicensed Practice of Law Committees”<https://www.abanet.org/cpr/clientpro/09-upl-survey.pdf>).

Top-Management Support

Once you have done your preparatory analysis and prepared your proposal, you should do everything possible to ensure that you have as many of the key people present as possible when you present the proposal. Because security assessment and policy involve such widespread investigation and, in a sense, interference in production across the entire enterprise, you need support from all the C-level officers who will be able to sign, authorize, or change the scope of the project. Having complete support and agreement from the start will significantly minimize the risk of last minute scope changes and milestone delays.

For more information about implementing security policies, see


In the next part, Gordon discusses client-vendor relations.

***

Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and to six foreign countries. Gordon’s information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. You may contact him by e-mail.<mailto:merrill.ia@gmail.com>

This series is based on some of the papers Mr Merrill wrote during his MSIA Program<http://infoassurance.norwich.edu/> at Norwich University<http://www.norwich.edu> from 2007 through 2008. Mr Merrill and I have collaborated closely in rewriting his research for this series.

M. E. Kabay, PhD, CISSP-ISSMP<mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>

Copyright © 2009 Gordon Merrill & M. E. Kabay. 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.