As an information assurance (IA) consultant and as an in-house IA professional, you are a vendor to your client or your employer. How you handle vendors during a consulting project or in your day-to-day work can affect the success of your security project. More generally, vendors can profoundly affect information security and you will need to study how the client or employer researches vendors before contracting with them. You yourself, as an employee or a consultant, need to have a good system for evaluating the competence and trustworthiness of vendors before recommending them. Finally, for to safeguard your reputation with trusted colleagues, you will also want to know how your employer or your client normally treats vendors so that you don’t alienate your own business contacts.

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.

* * *

**Presenting Yourself as a Vendor**

In your initial contacts with any organization, whether as a candidate for employment or as a potential consultant, you are a vendor of your own competence and services. In an interview about the initial contact, one CISO said that if she grants a consultant an hour of her time for a meeting, she does not want to hear anything about the consultant’s firm – she can look that up; she does not want to hear all about how good an expert you are – you will have a chance to prove that; and she does not want snap decisions without taking the time to get to know her operation and her business. She wants to hear your plan for *learning* her operation, her business and her needs. Only then will you be able to make a wise decision and have the opportunity to impress her.

**Being a Good Vendor**

A major part of your being a good vendor is learning to work with the contact people you have available to you at your client company. The CISO I interviewed expects every vendor and consultant to have a background check done at their own expense and provided to her company. In some cases, simply realizing that the people you are going to work with have had bad experiences and that they have no reason to expect at first blush that you will be any different will go a long way to prepare you for the journey to win their attention, their trust and their contract or the job. Put yourself in your employer’s or client’s shoes and work hard to understand their experiences and perceptions; don’t take an oppositional stance, take a supportive and understanding position so you can earn their trust through your commitment to excellent service whether you are an employee or a consultant.
Researching Vendors

Before you go to your client and recommend a vendor to them for a product or software you must research that vendor. Before putting your reputation on the line you should look at the vendor’s experience, their business track record, their product support, the viability of the company, and the degree of completeness and detail of their security documentation.


There is also a short narrated PowerPoint lecture (in a WinZIP file) on “Working with Vendors” <http://www.mekabay.com/courses/academic/norwich/msia/msia_s6_w02_vendors_ppt.zip> from the Master of Science in Information Assurance <http://infoassurance.norwich.edu> program that may be helpful to readers.

In the next and last part of this series, Gordon discusses problem management.

* * *

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.