

## **The Resurgence of Professional Services**

### **By Jeff Combs**

When I started with Alta five years ago, the market for security consultants was red hot. The Internet was booming, high-profile hacks were making the headlines, and companies just couldn't keep up with their security hiring needs. As a result, professional services firms that specialized in security were in high demand from clients across all verticals. In fact, the demand was so great that a whole crop of dedicated security consulting firms was launched in response. Unfortunately, within a couple of years, bad things started to happen to good companies. The bubble burst, corporate accounting scandals took their toll, global terror changed our lives, and the economic slowdown caused companies' security budgets to be slashed. It was a dark time.

### **The Changing Landscape**

Well I'm happy to report that the darkest days for security consulting practices are behind us, and things have been improving over the last year or so. I hesitate to say that anything good could come from the events of 9/11, corporate accounting scandals, and the war on terror, but there was an impact on the growth and resurgence of professional services firms. In general, society is more aware of the risks that face us all and has better appreciation of just how severely events can affect our economy.

Corporate accounting scandals have led to new legislative requirements like Sarbanes-Oxley. Prior to SOX, security architectures and controls had no regulatory standard to define them. Now every publicly traded organization is in the process of re-evaluating their security controls to ensure that they will be SOX-compliant. Further, in a global economy where the de-perimeterization of information security is the norm, organizations recognize the need to address significant areas of risk, such as application security and identity management.

To address the changing landscape, professional services firms have been developing a range of new offerings to complement traditional services like penetration testing and vulnerability assessment, security architecture reviews, infrastructure integration, policy development, and security program management. Some of these newer services include but aren't limited to: SOX 404 assessments, application security, vulnerability management, identity and access management, data classification, risk profiling and process re-engineering.

This all translates into a greater demand for consultants and increased hiring activity. In fact, in the last two quarters of 2004, the number of our active professional services clients has tripled. Clearly this is good news, but there are some caveats that need to be addressed. Professional services firms are hiring, but the bar has been raised and standards for employees are higher.

### **Two Major Influences**

In the past almost anyone who had working knowledge of security, a reasonably client-facing image, and the willingness to travel could get a job as a security consultant. Things have really changed since then, and it's important to know why and how. From the big picture perspective, there

are two major influences causing this change.

The first is competition. For every opening there are several candidates competing for it. This does not necessarily mean that every candidate is a good fit, but they do make it harder for the truly qualified folks to get the attention they deserve. As a recruiter, my job is to separate out and identify the candidates that I believe stand out. So, as a job seeker, you will really need to be able to differentiate yourself from the competition in a clear and meaningful way.

The second major influence is that security as a career path is maturing and security professionals are being held to higher standards of conduct, professionalism and communication. As a result, candidates who relied solely on their technical expertise in the past are having a harder time getting the jobs. It's not enough to be technically gifted anymore. Candidates need to understand the bigger picture of the businesses that they'll be servicing. Candidates also need to project a professional image that will mesh well with client environments. And finally, strong communication skills are absolute requirements. This goes beyond writing and speaking; candidates need to be able to listen. The ability to listen critically and understand the message behind the words is what allows one to respond effectively and in context. Listening to clients and responding to their needs is what consulting is all about.

Another sign of the maturation of our industry is that more companies are requiring degrees. This is based on the premise that security consulting firms are providing *assurance* services. One way consulting firms promote their services and win clients is by presenting the backgrounds and pedigrees of their staff. With the "Big 4" and similar companies, degrees have become a hard requirement. With smaller firms, the requirements may be more flexible, but a degree and subsequent certifications are differentiators that will help candidates stand out from the crowd.

### **Conclusion**

So, in summary, the opportunities to get into security consulting are the best they've been in the last four years. Companies are growing their practices, expanding their offerings, and searching for the people that can deliver them. However, interested candidates need to recognize that times have changed since the late 90s and hiring requirements are tougher. Candidates need to "elevate their game" and find ways to differentiate themselves from their competition to succeed. This is true of all information security professionals, not just consultants. It's worth it, though; the rewards are there. It just takes an extra measure of courage, confidence and dedication to be in the winner's circle.

*Jeff Combs is senior recruiter with Alta Associates. Jeff has a depth of experience recruiting security professionals at all levels for corporate clients, professional services firms, and security vendors.*