



# Career Corner

## *The Comeback of Business Continuity and Disaster Recovery*

**By Jeff Combs**

*jeff@altaassociates.com*

### **Introduction**

Business Continuity and Disaster Recovery is defined as the ability of an organization to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy.

Sounds pretty important, right? Yet for some reason, Business Continuity and Disaster Recovery (BCDR) is a discipline that often gets second or third billing when companies set their Information Protection priorities. For as long as I've been recruiting, it seems that the focus has been on fighting fires such as emerging threats and vulnerabilities and meeting regulatory requirements. In worst-case scenarios, companies paid little attention to BCDR and what is in place is woefully inadequate. In many cases, BCDR has been an add-on responsibility to somebody's existing job more as an audit requirement than anything else. Unfortunately, it appears that companies that have taken a proactive approach to BCDR are in the minority.

### **An Increase in Businesses Hiring BCDR Professionals**

Fortunately, this is starting to change. In the last six months there has been an increase in the number of companies hiring dedicated BCDR professionals. While the core drivers of BCDR haven't changed, there are a number of other factors that are influencing this resurgence of activity in the field. A number of companies have completed the majority of their Sarbanes-Oxley assessment work and have moved on to the remediation phase. One aspect of ensuring that there are adequate controls in place is being able to recover that information when systems break. In addition to compliance drivers, the geo-political environment and the threat of global terrorism have been influencing companies' BCDR activities. And we can't ignore Mother Nature, either. With the increase in natural disasters like hurricanes Katrina and Rita, changing weather patterns, and pandemics such as the bird flu companies are recognizing that if they don't have reliable counter-measures in place, they could find themselves out of business. Shareholders and insurance underwriters also recognize this.

So what are companies looking for? Each organization has its own unique requirements but there are several common objectives that all companies appear to share. In many cases, companies are recognizing that although they have BCDR plans in place, those plans need to be updated to take new threats into consideration. In one extreme example, a hiring manager told me (off the record) that his company's BCDR plans were so outdated they were completely useless. In his case, he was looking for somebody who could completely rebuild their program and make it viable.

Some companies have BCDR staff and policies in place but are working to augment and increase the effectiveness of their BCDR efforts. For example, one of the largest health insurers in the US is looking to grow their BCDR team and increase their skill levels. The hiring manager described the existing team as "ad hoc" with people representing different skill sets and backgrounds. Her goal was to increase the bench strength on this team by adding dedicated BCDR professionals who could take the lead on enterprise-wide BCDR initiatives. Another client, an established Midwestern financial services firm, had previously divided and shared BCDR responsibilities among several people in different departments. However, change was initiated when their existing BCDR plans were put to the test with poor results. This resulted in a decision to elevate the role and hire a dedicated BCDR professional reporting to their CSO.


In some cases, BCDR has been put at the forefront of organizations' operational risk management efforts. For example, one global investment bank recently made business continuity a major corporate-wide business objective by establishing a council of the company's senior-most executives focused on business resiliency. Their goal is to re-define their approach to business resiliency on a global scale and develop a program that will address emerging threats for the next several decades. In this case, they're searching for a leader who can coordinate global efforts to define policies, build disaster recovery infrastructure, and move corporate assets into areas of less risk. In addition to hiring for this leadership role, they will be building out BCDR project management teams in North America, South America, Europe, and the Pacific Rim.

### **BCDR and the Infosec Professional**

So what does this mean to the general Information Security practitioner? It could mean several things. If you're the type of person who likes to envision worst-case scenarios and then work to prevent them, BCDR could be another career avenue for you to explore. Regardless of what your role is, security professionals will benefit from keeping the big picture in mind. When looking at Information Security as part of an organization's operational risk management strategy or by taking a "defense in depth" approach, one should always incorporate business continuity and disaster recovery in their thinking. Why? Because even the best-laid plans fail and when they do, you need a backup.

### **Conclusion**

Recently I was speaking with Robbin C. Roberts, a global Business Continuity and Disaster Recovery professional with numerous certifications and years of experience. When I asked Robbin how she views BCDR, she put it this way, "In many way it's like an insurance policy. But when bad things happen instead of giving money back, a good Business Continuity and Disaster Recovery program gives you your business back. And this is

something that directly affects the lives of every employee, shareholder and business partner." 

---

*Jeff Combs has been a recruiter with Alta Associates since 1999.*

# The ISSA Journal

