govtech.com http://www.govtech.com/policy-management/Government-Must-Attract-More-Cyber-Security-Talent.html

Government Must Attract More Cyber-Security Talent (Opinion)

Mark Weatherford, chief information security officer, California Photo courtesy of Mark Weatherford

As if running a government cyber-security program weren't already challenging, a recently released report by Booz Allen Hamilton and the Partnership for Public Service titled *Cyber In-Security* reminds us that one of the critical, nontechnical problems lurking on the horizon is the shrinking number of qualified cyber-security experts interested in working for the government.

The report is a result of a survey of CIOs, chief information security officers and HR officials from the federal government. It found, among other things, that "the pipeline of potential new talent is inadequate." The report further states that "there are concerns that America is not developing enough IT experts, creating labor shortages in both the public and private sector." We've been hearing for a few years now about the IT work force "retirement bubble," but this is the first report I'm aware of that focuses specifically on the cyber-security work force.

While risk management is a fundamental component of any good cyber-security program, the overall goal of risk management isn't simply to protect an organization's IT assets, but to protect the institution's ability to carry out its mission. If we accept the definition of risk management as "the process of identifying, assessing and reducing risk to an acceptable level and implementing the right mechanisms to maintain that level of risk," our cyber-security work force issue means, "Houston, we have a problem."

Bruce Schneier, an author and security technologist, defined risk as "the relative likelihood that a bad thing will happen." As I thought about the cyber-security talent deficiency addressed in the report, it occurred to me that government IT may face an increasingly risky future because the likelihood of something bad happening grows in direct proportion to the shrinking pipeline of talent.

America's cyber-security talent deficiency is our vulnerability because the cyber-threat environment is growing daily and shows no signs of slowing. In fact, a recent Gartner report, *Security in 2013 and Beyond,* called the likeliest future state of information security as "a perpetual arms race, between hackers and criminals on one side and enterprises and governments on the other side."

If cyber-security is, as many of us believe, an interesting, exciting and somewhat noble profession, what's the problem? Why aren't more people interested in becoming part of the government cyber-security community of professionals? More importantly, how are we applying risk-management principles to address the cyber-security talent shortage?

On a federal, state and local government level, there are numerous issues that need to be addressed. The Gartner report identifies a number of programs that I believe should be developed as a part of a risk management plan, including:

- a career path for cyber-security professionals, from new hire to retire;
- training and development programs that expose people to new organizational opportunities and technologies; and

- recruiting plans that take advantage of social networking sites.

One national-level risk management initiative addressing the cyber-security skills shortage is the U.S. Cyber Challenge -- a program of national competitions that include the CyberPatriot Defense Competition sponsored by the Air Force, the Digital Forensics Competition sponsored by the U.S. Defense Department's Cyber Crime Center, and NetWars sponsored by the SANS Institute. The goal of the Cyber Challenge is to identify 10,000 young Americans, primarily high school and college students, who have the skills and aptitude to become cyber-security specialists.

We can't continue with casual discussions about government's IT work force retirement bubble and cyber-security work force shortage and expect the issue to resolve itself. It takes time -- many years, in fact -- to address these skill problems and develop the expert talent we need to keep our government IT systems operating securely. We must begin to employ risk-management principles to mitigate the lack of qualified cyber-security experts by developing specific strategies to identify talent, deliberately recruiting and knowingly investing in growing the next generation of cyber-security professionals.

* The views expressed are solely mine and nothing stated in or implied from the article should or may be attributed to the state of California or any of its agencies or employees.