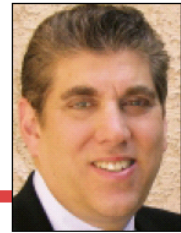


Ask The Expert

Evan Scott, president of
Evan Scott Group International



Q What's the current landscape for executive recruiting in the government security sector?

A There's an increased demand today for executive talent that understands -- and has years of experience -- selling to the federal government. A lot of the companies that are chasing the federal dollar, particularly in homeland security, don't have a lot of experience selling to the integrators or the federal government.

Q What do you consider to be the unique skills that somebody needs to sell into the federal government?

A They have current relationships with individuals within the various agencies. For instance, DHS is now comprised of 22 agencies. And, if you look at the black agencies -- such as the CIA and FBI -- unless the candidate has done work on that side of the government, or has sold into that space recently, they're not going to understand how the federal government actually buys products, and who pays for those products. It's all *political*. Unless you've lived that, either by being a federal employee or selling into it for a number of years, you won't recognize the buying signals. That's the biggest problem companies have. They have a lot of good meetings with government agencies, which are very receptive to their technology, but those meetings don't end up turning into contracts.

Q When you say, "it's all political," are you suggesting that the best product or best service won't necessarily win the contract?

A That's exactly what I'm suggesting. The best technology really never won. It's always the relationships, getting to the right people, putting together the right deal, particularly in the federal government.

You need to understand what everyone's motivations are at various levels of the government. The senators and congressmen have one motivation; the technology folks have different motivations. Unless you recognize what drives them, you're not going to recognize who's going to buy your technology. So the best technology

Evan Scott, the president of **Evan Scott Group International**, an executive recruitment firm based in Plymouth Meeting, PA, near Philadelphia, has been focused in recent years on the red hot government security sector. He took a breather recently to fill in *GSN's* Jacob Goodwin on current opportunities for federal government employees with the technology companies targeting this marketplace. And he outlined what new C-level employees -- and new board members -- might expect to be paid for their labors.

isn't what it's all about. It's about the best relationships, especially personal relationships here in Washington.

Q What types of government employees are commercial companies seeking these days?

A The federal government has terrific systems people. You look at the CIA, FBI, aviation. They have individuals that run their systems and technologies, and they're experts at the business. Those folks now are very attractive to commercial companies, companies trying to sell into the agencies. So we've been asked to recruit CIOs and heads of technology from these various agencies. No. 1, they understand how they bought technology. No. 2, they understand the technology itself. No. 3, many of them, candidly, have felt underpaid for so many years and see that the commercial private sector is paying much more money. There are many examples of individuals that have left big jobs on the federal side to move onto the commercial side, with very, very big pay packages.

Q Can you provide a few examples.

A An individual who was running one of the black agencies, one of the intelligence agencies, as the CIO, just left to join a major integrator. His job is now to be responsible for selling integrated services into the federal government and being the screen for new technologies.

Q How has his compensation changed?

A He'll almost triple his compensation, including base and bonus. This individual's total base and bonuses are going to be somewhere around \$300,000. He wasn't earning anywhere near that in the federal government, certainly not with the bonus opportunities.

Q Do you have another example?

A This is an individual who came out of one of the military branches, laying down all of that service's systems globally. He's very sophisticated, understood technology, understood how this particular agency bought the technology. He said to me in an interview, "It's time for me to catch up financially, and I see what's going on in the private sector." So he left and went to work for a biometric company. His salary has tripled, with the potential for more, plus equity, which continues to be more valuable. You can't get equity from the federal government. A lot of these biometric companies are offering equity. And the ones that hit can be a great wealth-building opportunity for folks.

Q Typically, what would be the elements of a compensation package you would help negotiate for a C-level candidate for a major government security company?

A The elements would be base compensation, "On Target Earnings," which we call OTE; a set objectives for revenue; and MBO's, or "Management By Objectives," which may include hiring and firing people. Then we talk about equity, or the percentage of the outstanding shares that they would get. Then we talk about how they could exceed the bonuses; we call them "Accelerators." If you hit your OTE, what kind of accelerators or cash and/or stock can you earn by exceeding those objectives? Those are the major elements of a compensation package.

Q Does your company negotiate on behalf of the candidate? Or the employer? Or both?

A That's the art of our business. The good recruiters recognize that in order to create a win-win. The candidate has to feel that we negotiated on their behalf. And the client, of course, expects us to negotiate on its behalf. So, having been at this for 26 years, we understand how to strike a balance on

what's fair, and we always keep that in mind -- what's fair based on the market and based on what the individual is bringing. We are intimately involved. We don't allow our clients to negotiate directly with candidates. Candidates don't want to negotiate with clients. They look to us to be the sounding board.

Q How is your search firm compensated?

A We've created a new paradigm in fees with our clients. We work with small companies where the typical search fee in this industry is one-third of first year's cash compensation. However, we're very sensitive about a company's cash flow.

We're very interested in taking stock as part of our compensation. So we negotiate a fee that's fair for us, fair for the result, and fair of our client based on the stage they're in. We tie our fees very much into our deliverables, where the first retainer will be paid in the beginning of the assignment, when the job is put together, helping to develop the strategy. The second retainer is due upon delivery of a slate of candidates and the final payment is due when the search is completed.

Q Give me a feel for the compensation that a typical CEO candidate would get, and the compensation that you would get as the executive search firm that placed him or her.

A The CEO position pays, let's say, \$300,000; the search firm will be one-third of that, so our fee will be \$100,000 paid in three installments. It's tied directly into the base comp, and sometimes the bonus. But the bonus would have to be a fair estimated bonus because it's really tough to identify. In the past, we've billed on the base salary, and after 12 months, we billed the balance on the actual bonus earned.

Q Are you also involved in searches for members of a company's board of directors?

More on Page 34

A We do a lot of board searches. I'm seeing many, many companies in different industries -- companies that want to deal with the federal government -- are coming to us and saying, "We need someone on our board that understands how Washington works."

The talent pool is huge. We have many individuals that we know who have a wealth of contacts, that lived in Washington, that worked on the federal side, who would love to serve on a public board. It's a great pool of talent that is not being utilized by public companies. And we have several public companies right now that have asked us to find board members with federal contacts.

Q What kind of compensation can these former government employees expect if they join the board of a public company?

A In a public company, we're probably talking about cash compensation between \$25,000 and \$35,000; stock options in the company, certain retainers per meeting -- typically there are four meetings per year. If they head up a compensation or strategy committee, they'd probably get a little more compensation or stock for that.

Q How do your firm's fees differ for a board search versus placing a CEO?

A We typically charge a fixed-fee between \$35,000 and \$45,000 to do those board searches. And we discount if it's for multiple seats.

Q Are we in a "buyer's market" or a "seller's market" for talented employees in the government security sector right now?

A It's a candidates' market. There isn't enough good talent to go around. The companies are scrambling to recruit talent. Major integrators have huge recruiting staffs, and they can't find enough people. It's very much like the Internet Age, back in the late 1990s, where companies had visions and were creating these new positions. Because there wasn't enough talent around, they came to the search firms. It's very similar to that today.

Q After the boom in the Internet and telecom sectors, there was a huge bust.

from the Internet until they achieved a more rigorous level of information security.

Throughout the lifecycle of vulnerability management technologies, federal agencies have been far from silent investors. These agencies have actively guided the development of such key features as vulnerability and asset prioritization, metrics and scorecards, and support for sophisticated, hierarchical organizations.

In the early days of vulnerability assessments, it was commonplace for vendors to load up their vulnerability scanning tools to examine a network for every possible security flaw in order to demonstrate how poor the customer

organization's security posture truly was. The vendors hoped to inspire the system or network administrators into action with a report that made an audible thud when dropped on a conference room table. As time passed, the federal government was one of the first customers to recognize that success in vulnerability management didn't lie in the number of vulnerabilities you identified, but in your ability to locate and eliminate the most grievous security gaps within your infrastructure.

Shortly thereafter, it became clear that when dealing with large networks in sprawling federal agencies, prioritization of remediation actions according to the importance of the vulnerabilities was a

good start, but not sufficient. Differences in the value of the assets could also be used to prioritize fix activities, based on the notion that not all machines are created (or valued) equal.

For example, if a devastating cyber worm is on the loose, it makes more sense to fix your high-value payroll and production systems than to spend scarce resources locking down lower-value test servers and staff desktops.

Concrete metrics for gauging progress in vulnerability management was also popularized by the federal government. For example, the "vulnerability per host" (VPH) metric, which is used by one of Foundstone's large federal customers, measures the VPH across that customer's networks and enables the agency to determine whether or not its security posture is improving. Metrics like VPH succeed where traditional measurements of the gross number of vulnerabilities fall short because VPH is easy to understand and accommodates the dynamic, complex nature of modern networks.

Useful metrics progressed logically into executive dashboard functionality where these vital security statistics could be understood at a glance and tracked over time. Federal customers' requests for at-a-glance reporting were heard loud and clear in industry. Federal IT officials insisted vendors must make it easy to grasp the big picture.

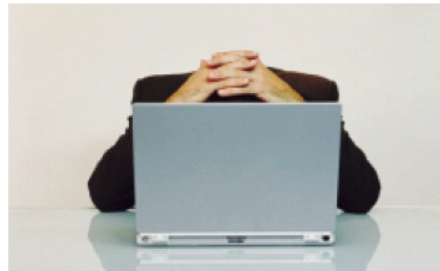
Perhaps the areas where the government has wielded its greatest influence are user account systems and flexibility of vulnerability management products. Simply put, the complex hierarchy and sophisticated reporting requirements of the federal government have stretched vendors well beyond the requirements of the commercial sector. For example, while each department in an agency may require its own separate deployment of a VM system, each of those systems is expected to report back to the global-repository for the entire agency.

For example, Foundstone introduced a specialized module that allowed trending and complex searches to be performed not just across organizations inside a single database, but also across multiple databases so that each department could maintain its independence while the agency's centralized security team still received the "roll-up" information it needed to monitor overall security health.

As the VM technology market hits its stride, it continues to be heavily influenced by the government sector with frequent announcements of vendors, commitments to supporting the Defense Department's Information Assurance Vulnerability Alerts (IAVA), Section 508 compliance, and Common Criteria certification. The collaborative relationship between the government and vulnerability management solution providers is likely to continue as long as features tailored to federal requirements are rewarded with new purchase orders and the commercial sector follows the government's lead. ■

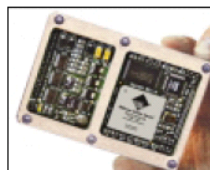


Don't lose your head over how to protect your sensitive data



Hardware Security Is The Only Solution

Every year thousands of notebooks and portable computers go missing, most are never recovered. Many of them in embarrassing situations involving the loss of sensitive or highly secret organizational and personal information. The Silicon Data Vault (SDV*) from Secure Systems is the only hardware encryption device that ensures your most valuable asset never falls into the wrong hands.



Easy installation for total sensitive data security

- 128 bit AES hardware encryption
- Pre boot authentication
- Multiple secure user profiles using advanced partitioning control
- Operating system independent
- Any laptop or desktop computer
- Set and forget - no ongoing costs

Contact Secure Systems for a demonstration of the Silicon Data Vault (SDV*) and rest easy knowing that while others around you are losing their heads your secrets are secure.

Secure Systems
www.securesystems.com.au

Secure Systems
Alexandria, VA
703-535-7999



For more information click on www.info.ims.ca/3390-680

What do you see as the similarities and the differences between those sectors and government security?

A The market of the late 1990's was driven by venture capital firms. Taxpayers are driving this government security market today. The federal government is going to be held accountable

to make sure that our citizens are protected. We will be looking for results; the protection of our airports, protection of the Internet, protection of our networks. That's the difference. This is a real business, and it's a long-term business, which will take years to perfect. It's not pie-in-the-sky. There will be accountability, and the federal government is in the hot seat to make sure that these safety measures are put in the place. ■