Security Fears Drive Jobs Back to US, But Nearshore Can Benefit

Are security fears driving jobs back to the US? Maybe, but while demand for cybersecurity specialists in the US is increasing exponentially, potential skills gaps could mean significant opportunities for nearshore providers. Barriers remain, however.

By Bianca Wright August 18, 2015

Cybersecurity is increasingly a critical issue and recent threats are translating into more jobs in the US for specialists in this area. “Over the last five years, there’s been a 90 percent increase in demand for cybersecurity professionals,” Matthew Sigelman, CEO of Burning Glass Technologies, which analyzes jobs data, told CNBC recently. “That’s three times the growth that we’ve seen for IT jobs overall.” This kind of growth has other implications, as it points to increased focus on US-based security solutions, in-house teams and a move towards onshoring.

While statistics on reshoring — the practice of bringing previously outsourced functions back to the country or company — are in short supply, there have been indications of growing interest in moving IT back to the organisation or at least closer to home, with large companies like General Motors and AstraZeneca leading the way. Although security fears have not been chief among reasons cited for these moves, the need for greater control over data has been mentioned. Increased risk of cyberthreats could reasonably account for reticence towards outsourcing of any kind.

Graham Speake, vice president and chief product architect at NexDefense, explained that the proliferation of the cybersecurity threat landscape has caused the corporate governance of industrial organizations to rethink their strategies for combatting unprecedented levels of risk. "Whereas the opportunity-cost of outsourcing many cybersecurity jobs was once favorable, the 'new normal' that is comprised of frequent and sophisticated attacks has all but mandated the need for in-house experts capable of responding to events 24/7," he said.

Keeping It Close to Home

It makes sense in this context to keep the cybersecurity specialists close, and to ensure greater control over data. Cyber threats are likely to increase, and the need for secure solutions is unlikely to diminish.

Speake said that there are two main drivers of the jobs moving back to the US:

- The proliferation of the threat landscape: Today's cyber threats are advanced and sophisticated; and defending proprietary assets requires highly-skilled workers and innovative technologies.
- CEOs and board members are beginning to see the financial impacts of not investing in cybersecurity in the past, so they are allocating larger budgets to boost their mitigation and response strategies.

Alan Berman, President of DRI International (Disaster Recovery Institute), added: "With the proliferation of high visibility cyber security breaches, it is no wonder that the demand in the market place for trained cyber security professionals is increasing at an unprecedented rate."

He explained that the demand is expected to increase the number of personnel to 6 million in the next three to four years. Organizations are expecting that there will be a shortfall of more than one million cyberwarriors to meet this demand.

This is backed up by Burning Glass Technologies' survey, which found that the fastest increases in demand for cybersecurity workers "are in industries managing increasing volumes of consumer data such as Finance (+137% over the last five years), Health Care (+121%), and Retail Trade (+89%)."

"With regulations now requiring that organizations not only

demonstrate their own cyber security capabilities, but extending their responsibility to their vendors and suppliers, cybersecurity is a mandated requirement," Berman warned. "Without this demonstrated protection, companies will find that they will not be considered for lucrative government and private sector contracts."

US Skills Gap Means Opportunity For Nearshore

So where to look for that much-needed skill set? Dr. Rhonda Chicone, an expert in the IT security and software industry and faculty member at Kaplan University School of Business and Information Technology, explained that many organizations are starting to take a hard look at building their internal cybersecurity team/department due to all the highly publicized incidents.

"These incidents have made organizations aware of the cyber risks," she said. While this is a positive thing, Chicone warned that the highest bidders (companies with a big security budget) are snatching the best and the brightest up. "We simply need more talent. I'm sure cyber security outsourcers are having a hard time finding the talent as well. It goes back to education and training," she said.

It is not all bad news, though. While demand for cybersecurity professionals in the US is increasing, the

nearshore can benefit from that increased demand as well. Chicone said that the serious skills gap problem when it comes to cybersecurity talent in the US could represent an opportunity to nearshore providers.

"The talent is very hard to find. Many organizations may be forced to outsource in the nearshore. Also, the cyber security outsourcers could capitalize on some cyber security challenges or opportunities," she said, explaining that an example could be work force development by helping organizations with employee awareness and training programs. Another opportunity lies in helping firms lay the foundation for building an internal cyber security team/department.

Perceptions Need Changing

Being in a similar time zone to the US, closer than rivals in India, China and the Philippines, and with greater cultural affinity, the nearshore is positioned to potentially address the demand for cybersecurity professionals. There are barriers, however.

Perceptions of unpreparedness in terms of the reality of cybersecurity issues could mean that US companies are not willing to risk outsourcing to the region. In a recent post, Scott Sweeney, an attorney at Wilson Elser with experience in Latin America, wrote: "Most Latin American countries have done little in the way of enacting laws to dissuade cybercrime

either through governing and reporting requirements for those in possession of sensitive data or through more severe penalties for corresponding loss."

Vendors, therefore, need to work with clients to assure them of the rigorous security measures in place and to minimize potential risk.

Domain knowledge combined with cybersecurity skills will increasingly be in demand. The Burning Glass Technologies report found that "the hardest-to-fill cybersecurity jobs call for financial skills, such as Accounting or knowledge of regulations associated with the Sarbanes-Oxley Act, alongside traditional networking and IT security skills. Because finance and IT skills are rarely trained for together, there is a skills gap for workers who meet the requirements of the 'hybrid jobs'."

Countries like Uruguay and Colombia, which are positioning themselves in terms of their Finance and Accounting Outsourcing offerings could leverage this demand by upskilling candidates to meet the hybrid needs. Certification at the standard demanded by the US market will be required.

So while cybersecurity jobs are on the rise in the US, it does not necessarily translate into fewer opportunities in the nearshore – if the core barriers can be addressed and savvy vendors invest in the needed skills to meet growing demand.

Tags

Analysis | Colombia | cybersecurity jobs | cybersecurity specialists | cyberthreats | Uruguay

Bianca Wright

NSAM Managing Editor Bianca Wright has been published in a variety of magazines and online publications in the UK, the US and South Africa, including Global Telecoms Business, Office.com, SA Computer Magazine, M-Business, Discovery.com, Business Start-ups, Cosmopolitan and ComputorEdge. She holds a MPhil degree in Journalism from the University

c

of Stellenbosch and a DPhil in Media Studies from Nelson Mandela Metropolitan University.