Cybersecurity Staffing Shortages Make Safeguarding Data a Challenge

Posted At : October 1, 2013 2:41 PM | Posted By : John Slye
Related Categories: Critical Infrastructure Protection, Information Security, Cloud Computing, IT Workforce, Big Data/Analytics, Cybersecurity

What do you get when you cross exploding data stores concentrated together by technical efficiencies with a shortage of IT security staff to secure that data? You get the potential for huge data breaches. And from the looks of several recent surveys in the news this cybersecurity staffing issue is causing some insomnia among IT managers.

Several years of budget pressure has pushed federal IT managers to look for ways to cut their IT spending and increase efficiencies while the demands placed on IT through big data, mobility and the like continue to increase. At the same time we see more reports of how the current budget environment may impact the size of the federal workforce – either through retirements or reductions. Even IT staffing does not appear to be immune as agencies look for savings through approaches like cloud computing, virtualization, and IT-as-a-service. But could the combined effect of technology efficiencies mixed with growing data stores and a shortage of information security staff be setting agencies up for potential trouble. Several recent surveys suggest that is a possibility.

A recent Federal Times report included interviews from those inside and outside the federal government that said IT staffs would almost surely shrink across most areas due to trends like cloud computing, program consolidation and (of course) sequestration and budget cuts. The only likely safe area seems to be cybersecurity. But budget reductions may not be the biggest staffing issue facing federal cybersecurity departments. Their challenge seems to be finding enough people with the right skills.

Staffing Shortages, Big Data and the Insider Threat

Nextgov has reported that it is security concerns IT staffing shortages that keep IT workers up at night. The article references a survey by security company EiQ Networks of more than 250 IT decision makers in industries including government and 2/3 say their IT security department is understaffed and that their largest security concern (34%) is an external data breach for financial gain. By comparison, 22% said loss of intellectual property was their greatest concern and 9% responded that they feared a trusted 3rd-party contractor exposing their organization.

In the wake of the Snowden exfiltration case and others, organizations have come to recognize their data is one of their most valuable assets and that has agencies more aware of how the manage and protect it. Another recent article cites a study that federal cybersecurity pros are worried about the glut of data clogging their networks, with more than half (55%) of the 203 survey respondents saying agency networks cannot keep up with the current data loads and nearly 20% saying that their network and security monitoring capacity are insufficient to the task.

A fourth survey reported by Federal Computer Week of more than 700 IT professionals and business managers in civilian, defense and intelligence agencies and across large public sector organizations suggests that insider threats are more concerning than ever. Of the respondents 63% feel vulnerable to abuse of privileged user access rights by employees of the organization and 58% feel vulnerable to abuse of access rights by contractors of the organization.

So we have ever-burgeoning data assets that are increasing in value to agencies being concentrated in fewer places through the drive for technology efficiencies and that are straining existing networks. At the same time we have an ongoing shortage of skilled cybersecurity personnel – both in- and outside government – necessary to protect those data assets. Could this be the potential makings of another high-profile news story? Hopefully not.

Implications

Competition for IT staff with up-to-date security skills will continue to be hot and the growing emphasis on critical infrastructure protection by the White House, Congress and others will only fan the flames. Federal agencies face strong competition from private companies in the energy, financial, and transportation sectors as well as industries supporting government missions. This shortage will likely take years to overcome.

Training of federal IT staffers with adjacent skill sets will be a way to bridge part of the gap, so training companies may have some business opportunities, even though training is often the first place agencies look when trying to obtain immediate budget cuts. But much of the high-demand skills only come from years of varied experience, making these folks particularly hot commodities.

Since the cost and steep learning curve exacerbate the people problem technologies have been cropping up to help fill the void, reduce cost and help leverage the security staff that agencies do have on board. Technologies that increase efficiencies – analytics and advanced monitoring tools, etc. – will continue to be in demand.

Like so many things, the final solution will be a combination of people and technology to effectively secure valuable data. Both elements have a ways to go before IT managers will sleep better.

---
*Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about **GovWin FIA**. Follow me on Twitter **@GovWinSlye**.*