CASE STUDY #3:

Is There a Cybersecurity Workforce Crisis in State Government?

DeBora King
CSIA 360 7980
Cybersecurity in Government Organizations (2172)
April 16, 2017

University of Maryland University College – Spring Semester, 2017

INTRODUCTION

According to the most recent Global Information Security Workforce study (GISWS), by 2022 there will be an estimated 1.8 million workforce shortage of cybersecurity professionals. In planning the one-day workshop on workforce development needs for cybersecurity workers, the question that must be addressed: Is there a cybersecurity workforce crisis in state governments or not? First, the word crisis must be defined to address this question. Are governments in a state emergency or disaster as a result of a shortage in cybersecurity workers? The answer is – that depends on a number of factors. This position paper will provide the workshop's coordinating committee addressing these factors which gives a perspective whether or not a crisis exists.

FACTORS AFFECTING POTENTIAL CYBERSECURITY WORKERS

The following factors must be considered to address the issues of the cybersecurity workforce in government. These factors include political, economic, and educational issues.

- **Political** – Along with major retailers, the government is also prey to increased security breaches. Ann Visalli, director of Delaware's Office of Management and Budget commented about the critical demand for data protection. "We house information for payroll purposes for people's health insurance. We are dealing with confidential legal information, confidential criminal information. We have an obligation to do everything in our power to protect all the data that the stat has in its possession," said Visalli (Stone, 2014).
- **Economic** – The U.S. Bureau of Labor and Statistics reports that the mean salary for a cybersecurity analyst in 2013 was $92,280 for a private-sector worker versus $72,210 for a public-sector worker (Trevorh, 2015).
- **Education** – Young Americans are lacking the foundation they need in early education to make college-ready choices involving a cybersecurity career. The Organization for Economic Cooperation conducted a student assessment which stated that U.S. students came in 27th in science and 36th in math out of 65 nations (NCI at Excelsior, 2015). In addition, out of 234,000 U.S. colleges graduates a year only 13% of undergraduate degrees include a concentration in science, technology, engineering or math.

GOVERNMENT CHALLENGES HIRING CYBERSECURITY WORKERS

After surveying IT chiefs from 48 states, the National Association of State Chief Information Officers (NASCIO) found the following hiring obstacles associated with hiring good cybersecurity staff (Bergal, 2015):

- Almost 92% of states said salary and pay grades are a challenge while trying to attract and retain employees.
- Problems with recruitment to fill vacant positions has increased. While 55% of states reported having issues with recruitment just four years ago, now 86% of states admit having these challenges.
- The length of time it takes to fill positions can be up to five months for senior level positions – this was reported by 45% of states.

The private sector has their fair share of challenges in hiring cybersecurity professionals. Tech Republic addresses five reasons why companies can't hire cybersecurity professionals as follows (DeNisco, 2017):

1. Demanding a vast amount of specialties that require more skills than candidates can produce. Requiring too much of candidates leaves a big gap in skill sets.
2. Poor compensation with qualifications not measuring up to pay grades.
3. Overlooking talent from within the company, new college graduates, veterans, and women (which make up only 11% of the cybersecurity workforce).
4. Poor work/life balance, as many cybersecurity workers do not have a 9-5 position because security alerts can pop up any time within a 24/7-time frame.
5. An inefficient and lengthy recruiting process can turn-off candidates and companies can be left with a scarce pool when choosing good potential employees.

NON-CYBERSECURITY REASONS FOR WORKFORCE SHORTAGE

Government agencies have stiff competition, in general, when it comes to hiring good staff because private sectors have the ability to hire candidates with greater pay. Unfortunately, states have issues with sufficient funding. They receive federal grants, but some expenses are earmarked as

"administrative costs" which are capped to save money. Mitch Herckis, Director of NASCIO, is hoping to raise awareness so that states can have enough funds to cover their IT costs.

The pay for government jobs is not the only one factor in the challenge for filling positions. According to Srini Subramania, a state cybersecurity principal at the consulting firm Deloitte & Touche LLP, the government lacks a clearly defined career path for upward mobility in state government (Bergal, 2015).

RECOMMENDATIONS FOR HIRING MARKETING/ACTIONS

State government agencies can do a number of things to improve the challenges hiring cybersecurity professionals. States can benefit from offering the following marketing/actions while being confined to budget constraints: 1) training (and cross-training) the staff they already have; 2) offering certificate programs to new hires; 3) providing flexibility/remote work to support work/life balance; and 4) collaborating with partnerships. For example, in order to raise awareness and promote cybersecurity in the workforce, Maryland's Howard Tech Council partners with Howard County Economic Development Authority and Innovation Catalyst provides a CISO-in-residence program (Stone, 2014). Jim Smith, CIO in the state of Maine's IT agency revamped their internship program by partnering with colleges in the state. The interns are selected by skill level, partnered with the right position and paired with a mentor (Bergal, 2015). Finally, incentives do not have to be monetary as the government can provide discounted programs that are offered to other government workers, such as teachers, firefighters and emergency medical technicians. Our government has overcome many obstacles obtaining good people in the workforce. There has been a demand from secretaries that know short-hand, to those that know the electronic typewriter; from keypunch operators to data entry workers on computer terminals. Now everyone has a personal computer, mobile or hand-held device, and many other positions from the past are now obsolete. In time, the market in America always adjusts and eventually prevails -- until the next wave of innovation.

References:

(ISC)^2 Blog. (2017, February 15). *Cyber security workforce shortage projected at 1.8 million by 2022*. Retrieved from http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html

Trevorh. (2015, November 3). *Choosing a career in cybersecurity: public sector or private sector?* Cybrary. Retrieved from https://www.cybrary.it/2015/11/choosing-a-career-in-cybersecurity-public-sector-or-private-sector/

Stone, A. (2014, October 3). *State and local governments try to fix the cybersecurity staff problem*. Government. Retrieved from http://www.governing.com/news/headlines/state-and-local-Governments-dont-have-the-cybersecurity-staff-they-want.html

Bergal, J. (2015, May 14). *States have trouble hiring good cybersecurity staff. Governing*. Retrieved from http://www.governing.com/topics/mgmt/states-have-trouble-hiring-good-cybersecurity-staff.html

DeNisco, A. (2017, March 29). *5 reasons your company can't hire a cybersecurity professional, and what you can do to fix it.* Tech Republic. Retrieved from http://www.techrepublic.com/article/5-reasons-your-company-cant-hire-a-cybersecurity-professional-and-what-you-can-do-to-fix-it/