Solving the Cybersecurity Workforce Crisis

Malintha Liyanage

School or Institution Name (University at Place or Town, State)

**Solving the Cybersecurity Workforce Crisis**

**Introduction:**

Information technologies play a central role in all the aspect of modern life. Information and communication technologies are being used by state departments as well as private organizations and businesses. State departments utilize information and communication technologies to process personally identifiable information of the citizens such as names, physical addresses, social security numbers, and passport information, etc. Processing personal information in such systems makes them the potential target of cyber-criminals. Headlines are filled with successful news of targeted attacks on both public and private sector organizations. Cyber-criminals are always developing sophisticated attacks to bypass existing security architecture of public sector organizations as well as leading state departments (Assante & Tobey, 2011). During the last decade, various state departments suffered sophisticated cyber-attacks such as the website of Oregon's state department of employment was breached. In another breach, hackers were able to breach millions of social security numbers form the state revenue department of Carolina. These events and many of the similar attacks on state departments emphasize the need for robust cyber security architecture for state departments.

Cybersecurity is the most important requirement of any state department in the modern world dominated by information and communication technologies. The building of strong security architecture to combat sophisticated cyber-attacks on critical information systems of the state departments a comprehensive amount of cyber security workforce is required such as malware analysts, network security experts, and ethical hackers. On the other hand, the situation of cyber security experts in state departments is not satisfactory to combat sophisticated attack weapons of modern cyber-criminals (Evans & Reeder, 2010). State departments suffered from various issues and challenges in hiring and retaining top cyber security professionals for the protection of the critical information assets of the nation. The paper discusses the challenges faced by the state governments and provides best practice recommendations to make information technology infrastructure more secure.

**Difficulties Faced by State Governments:**

State departments and governments deal with personal information of citizens using information technology systems. Having extensive amounts of valuable data in these systems make them a potential target of cybercriminals. These systems range from storing and processing health information by public health facilities to keeping records of criminal activities by the state police. Protection of such systems is to meet the basic security goals of confidentiality, integrity, availability, and non-repudiation of the data. To meet these goals, the extensive workforce is required by the state governments specializing in cyber security which is currently lacking due to various reasons (Fraley & Cannady, 2017). One of the most important reasons behind the lack of cyber security workforce in state departments is the lack of attractive salaries and pay grades. These are among the biggest challenges faced by the state departments in retaining and hiring the required talent for protection of critical infrastructure.

Private sector organizations have taken more serious approaches toward cyber security. Most of the developments made in cyber security are by private sector organizations. They have invested heavily in infrastructure development and hiring of top talent from educational institutions directly. They offered more attractive salaries than any of the state departments resulting in high turnover rates for them. There is another potential challenge that whenever a state hired a professional, then massive investments are made to train them up to the industry standard. After getting requisite training and experience from public sector organizations, the skilled persons are then recruited by private sector organizations offering better salaries. Eighty-six per cent of the states reported that they faced difficulties in hiring cyber security professionals for various vacant positions in state departments (Vogel, 2016). It was never so difficult a few years ago. As targeted attacks have increased exponentially on large-scale organizations, cyber security professionals are in high demand that have increased their values for both the private and public sectors.

Moreover, the private sector has developed more secure systems as compared to the systems owned by the state departments by employing top talent in the industry. The results are obvious that state departments have to rely on private sector organizations in order to protect critical information assets of the nation. The private sector has made marvelous achievements in halting cyber-attacks as compared to state departments. They have incorporated big data analytics along with machine learning capabilities to fight against sophisticated attacks. Their processes and algorithms are mature enough or continuously improving at such a pace that many vendors are claiming that their solutions can protect against never before seen attacks (Newhouse, Keith, Scribner, & Witte, 2017). Although it may not be the case as a recent wave of ransomware attacks both in private and public sectors caused a catastrophe. None of the available cyber security vendors was able to stop the attacks in first place. Lack of research facilities and modern algorithms in state departments provides a challenge in hiring and retaining cyber security talent as compared with the private sector.

**Non-Cybersecurity Reasons behind the Workforce Crisis:**

There is a plethora of technical issues results in a workforce crisis in the cyber domain. Along with many non-cyber security reasons as well such as salaries offered by the state departments. Most of the state departments have budgetary issues in offering attractive salaries as compared to the private sector organizations. The situation is not a result of a sudden increase in cyber-attacks on state departments. It is present due to a long-term lack of attention practiced by many state departments. It has been reported by ex-managers or project managers that it was difficult to convince governments to invest in a secondary system to protect an existing system when there were no obvious benefits to such investment (Jethwani, Memon, Seo, & Richer, 2017). The result of this lack of attention has resulted in the current situation where it is becoming more and more difficult for state departments to hire and retain cyber security professionals.

Moreover, state departments are still not willing to invest in youngsters to train them for the required processes. They are looking for candidates having requisite skills as they apply against vacant positions in various departments. On the other hand, private sector organizations took a completely opposite approach. They selected fresh graduates and trained them to the required level of skills in cyber security. The reason behind this situation is again the budgetary issues. It is not possible for state departments to fund such pieces of training and most of the departments do not have the training facilities as well. All the issues combined together have resulted in a more vulnerable information technology infrastructure used by the state departments. It can be improved with public-private partnerships to make information technology ecosystem more secure for the nation.

**Recommendations:**

There are several recommendations for state governments that can help them to compete with the private sector in terms of hiring and retaining cyber security talent without competing in terms of salaries. State governments must promote and articulate a culture of flexibility as practiced by private organizations. Flexibility in working hours and remote work locations will help state governments to retain talent. They have to consider cyber security as an industry side problem and formulate strategies to overcome the problem. Latest developments in cyber security such as deep learning neural networks to find malicious patterns in network traffic have made it an industry side technology problem (Newhouse et al., 2017). Training programs can be arranged in partnerships with private organizations to equip fresh graduates with the required skills. Policies in state departments that restrict the hiring of candidates lacing formal education must be revised for cyber security domain. As it is not necessary that an ethical hacker will have a graduate degree as well. Without having any formal graduate degree, an ethical hacker having concrete skills will prove to be an essential asset for state departments. It will help state departments to discover vulnerabilities in existing systems and will help in designing cure as well. The gap in the workforce for cyber security related positions in state departments can be filled by making the hiring process and working conditions more flexible.

**Summary:**

Cyber security professionals are in great demand as compared to any other skill. It is due to the exponential growth in a number of sophisticated cyber-attacks on information technology systems both in the public sector and the private sector. State governments are facing difficulties in hiring and retaining top talent in cyber security to protect critical information systems of the nation. However, it can be solved without competing on salaries by making the working conditions flexible. Perks introduced such as training and flexible work location benefits along with career advancement structure by the state governments will help solve the workforce crisis being experienced by the state government at present.

References

Assante, M. J., & Tobey, D. H. (2011). Enhancing the cybersecurity workforce. *IT Professional*, *13*(1), 12–15.

Evans, K., & Reeder, F. (2010). *A human capital crisis in cybersecurity: Technical proficiency matters*. CSIS.

Fraley, J. B., & Cannady, J. (2017). The promise of machine learning in cybersecurity. In *SoutheastCon 2017* (pp. 1–6). IEEE.

Jethwani, M. M., Memon, N., Seo, W., & Richer, A. (2017). “I Can Actually Be a Super Sleuth” Promising Practices for Engaging Adolescent Girls in Cybersecurity Education. *Journal of Educational Computing Research*, *55*(1), 3–25.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication*, *800*, 181.

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32.