Emily Vandalovsky

Strengthening Cybersecurity: Lessons Learned from Other Areas

8/21/2017

Dr. Carnahan

Summer 2017

The protection and securing of data have become of one of the foremost tasks of the digital age. A number of system security breaches per unit of time raises a great amount of concern among all users. The threat of unauthorized data access and leaking sensitive information is real (Robinson, Brown, & Green, 2010, pp. 56-58) and has become a frequent occurrence. With data, today's precious commodity, being exposed, jeopardized or stolen, providing adequate system security becomes critically important. The powerful and sustainable mechanisms are needed to withstand the existing threat.

In many ways the field of cybersecurity is similar to the field of medicine. (McGettrick, 2014). Both fields are focusing on protecting the common health. In one case, it is the human health that needs protection from illness, while in the other one, it is the health of electronic infrastructure that needs protection from potential threats. Both, the cybersecurity and the medicine, are extensive fields with the multiple areas of concentration and focus. Both require extensive amount of support from a number of related fields. The ground breaking research and forward thinking is moving both fields forward. Both fields include the private and public components, where a groups of trained professionals are responsible for the common well-being, while the public carries out the personal and social responsibility.

The span of cybersecurity is tremendous. It combines several technical fields with a number of non-technical ones. Cyber defense, network security, data assurance, computer forensics, cybercrime, hacking, data encryption are just several technical areas of focus within the field. Individuals pursuing careers in any one of these or related areas need formal education and extensive technical tanning. To continue the parallel with the field of medicine, the information security professionals may be considered the "physicians" of field. Their technical

knowledge along with the problem solving and critical thinking skills are providing for the adequate level of system protection, and, when needed, the necessary remedy or solution.

The army of cybersecurity professionals is immense. In 2016, there were nearly 750,000 employees in cybersecurity related jobs (CyberSeek, n.d.). However, there is a continued need for the trained professionals. Nearly 300,000 cybersecurity related positions were still unfilled between April 2016 and March 2017 (CyberSeek, n.d.).

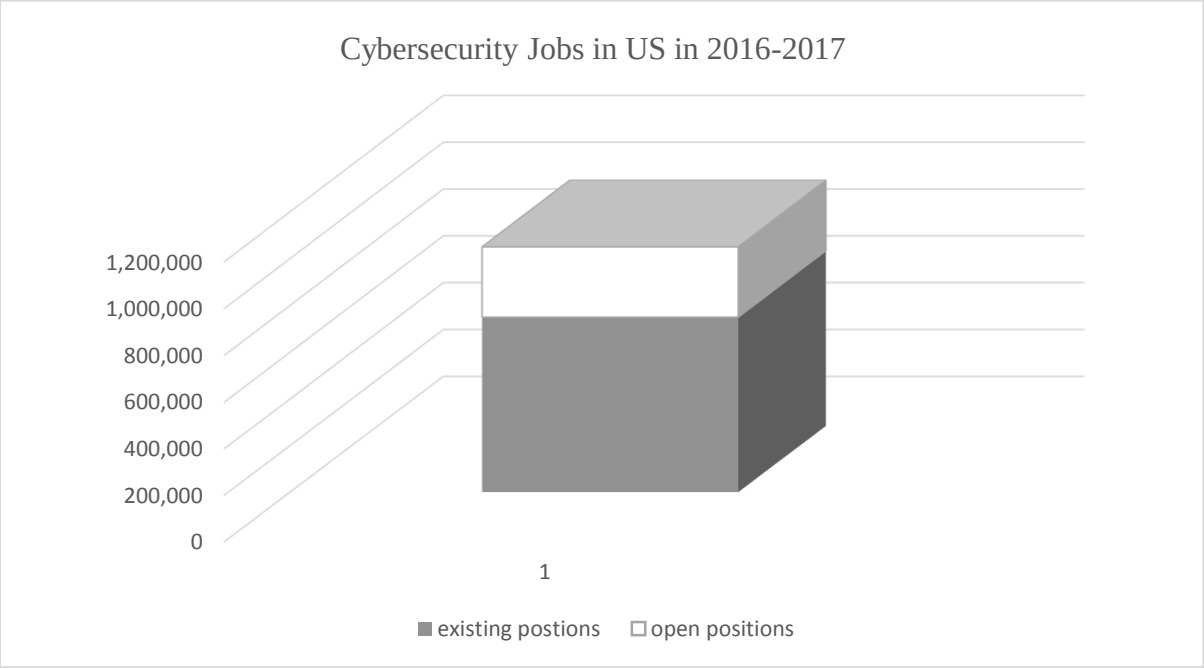

Figure 1-1: CyberSeek. (n.d.). Cybersecurity supply/demand heat map. Retrieved August 21, 2017, adapted from http://cyberseek.org/heatmap.html

The notable gap between the supply and the demand of cybersecurity related jobs suggests the following findings: colleges and universities do not award a sufficient number of degrees in the field and/or there is not enough interest in the area to attract more students, and therefore, create future employees.

Both causes have one common root, which is the magnitude of the field. Potential students may not always know what kind of work is included in the field of cybersecurity. They

may not be aware about existing open positions available. Currently, the sample list of available job openings includes: cybersecurity specialist/technician, cyber crime analyst / investigator, incident analyst / responder, IT auditor, cybersecurity analyst, cybersecurity consultant, prevention & vulnerability tester, cybersecurity engineer, cybersecurity architect (CyberSeek, n.d.). Moreover, it may not be clear to potential students what do professionals in these occupations do and what kind of skills do they need to be successful. The unknown or little known nature of the field may create a negative impression, and therefore potential lack of interest.

Moreover, the interest to the field may be planted earlier than college, during K-12 years. A number of subject related competitions and hackathons already exist, but the common curriculum still needs to be more focused on the area. The field is still unknown and unclear to younger students. Many of them are probably not dreaming of becoming an "IT auditor" or "prevention & vulnerability tester", as much as they may dream of becoming a doctor. Although it appears challenging, but making the field personal and approachable is long-term solution to the existing gap in supply and ever-growing demand.

Continuing with the theme of the similarities between the fields of medicine and cybersecurity, the protection of cyberspace can no longer be the prerogative of a group of professionals, regardless of highly trained they are. It should become everyone's personal and civil responsibility. The end-user mentality has to change, which is a lengthy process (Robinson, Brown, & Green, 2010, pp. 66), as many modern day technology users are savvy enough to incorporate the secure computing into every-day tasks.

The public health standards are introduced early in childhood and are encouraged throughout the lifetime. Following public health standards allows for preventive measures to

work and not to get ill. On many occasions, a generally educated individual may resolve some of their own health related issues of the common nature. Similarly, when the healthy computing habits are introduced early on, a generally educated individual may be able to recognize the signs of system ill or peculiar behavior bound by personal and social responsibility (McGettrick, en al, 2014). The public nature of cybersecurity resembles the concept of public health. (Mulligan, D. K., & Schneider, F. B. 2011).

Cyber attacks are the form of terrorism, and should be treated accordingly. In post 9-11 New York City, the following slogan became important and appropriate, "If you see something, say something". It was calling all New Yorkers to unite again suspicions behaviors and assist law enforcement officers with the anti-terrorism behaviors. The slogan made the city security everybody's business. Similarly, the cybersecurity should become everybody's business and the similar motivation for reporting suspicious or unauthorized behavior should be promoted (Marx, 2013).

The examples of community-based righteous behaviors in cyberspace already exist, such as reporting spam, or deleting phishing emails, but these examples are not frequent. Public digital hygiene is a strong mechanism against malicious behaviors (Paulsen, et al, 2012).

In conclusion, the field of cybersecurity is similar to the field of medicine in many ways, such as the size of magnitude, the level of professional training required, the promoting of healthy behaviors, and the use of prevention mechanisms. The main lesson that the cybersecurity field needs to learn from the field of medicine is the further involvement of the general public and incorporating digital health standards from the early age.

References:

CyberSeek. (n.d.). Cybersecurity career pathway. Retrieved August 21, 2017, from http://cyberseek.org/pathway.html

CyberSeek. (n.d.). Cybersecurity supply/demand heat map. Retrieved August 21, 2017, from http://cyberseek.org/heatmap.html

Marx, G. T. (2013). The public as partner? Technology can make us auxiliaries as well as vigilantes. *IEEE Security & Privacy*, *11*(5), 56-61

McGettrick, A., Cassel, L. N., Dark, M., Hawthorne, E. K., & Impagliazzo, J. (2014, March). Toward curricular guidelines for cybersecurity. In *Proceedings of the 45th ACM technical symposium on Computer science education* (pp. 81-82). ACM.

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus*, *140*(4), 70-92.

Paulsen, C., McDuffie, E. L., Newhouse, W. D., & Toth, P. R. (2012). NICE: Creating a Cybersecurity Workforce and Aware Public. *IEEE Security & Privacy*, *10*(3).

Robinson, L. K., Brown, A. H., & Green, T. D. (2010). *Security vs. access* (1. ed. ed.). Eugene, OR [u.a.]: International Society for Technology in Education.

.