Global Advanced Research Journal of Educational Research and Reviews (ISSN: 2315-5132) Vol. 10(1) PP. 221-224, February 2023
Available online http://garj.org/garjerr

Review

Managing Cybersecurity Skill Shortage in the U.S

Osayuki E. Ehioghae

8000 Creekbend Drive Houston Texas 77406.
E-mail: yuki.ehio@yahoo.com

Accepted 23 February 2023

It is no news that technology companies struggle to find competent hands to hire especially in cybersecurity. This gaping chasm left unaddressed could offer bad guys a free run all day. Although attempts have been made to address these shortfalls, it seems to constantly grow larger by each sun rise. This paper attempts to address some observations about Cybersecurity skill gap and questions existing ways of viewing the problem in lieu of finding better solutions.

Keywords: Cybersecurity, Skill Shortage and Technology

INTRODUCTION

All over the world, there is a growing concern for companies and government agencies regarding a shortfall in technologically skilled personnel entering the job market. In the United States alone, The U.S. Bureau of Labour Statistics shows a huge gulf between available technology jobs and people qualified to execute these jobs. In Cybersecurity the chasm is even more evident. It is no doubt that technology has altered the way we learn and behave, however, it is important to discuss how these changes impact jobs in today's world.

> *"Employment of information security analysts is projected to grow 35 percent from 2021 to 2031, much faster than the average for all occupations. About 19,500 openings for information security analysts are projected each year, on average, over the decade. Many of those openings are expected to result from the need to replace workers who transfer to different occupations or exit the labour force, such as to retire." [(Bureau of Labour Statistics, U.S. Department of Labour, Occupational Outlook Handbook, Information Security Analysts, 2022)].*

This is a paper espousing some possible explanations for the chasm experienced in technical job markets and some changes that might have necessitated or influenced them. It is important to mention that these ideas are subjective and open to a quantitative study. This paper looks at the following in an attempt to explain the shortfall in the cybersecurity industry (skill gap).

The following areas are considered in an attempt to better understand the problem.

(1) Increase in demand for technology
(2) Existing Academic Structures
(3) Human capital vs Attention deficit
(4) Ever Changing Job Complexity and Requirements, in an attempt to find solutions to Cybersecurity personnel shortfall.

Increase in demand for Cyber Technology

It is no secret that the world has consistently experienced growth in the demand for technology related to the Internet. As the Risk VS reward quotient tilted increasingly in favour of reward, more people adopted cyber technology in different forms. Today its application is all-encompassing from medicine to agriculture, entertainment, and our everyday life. It is almost impossible for most people to go through their day without engaging one form of cyber technology. For instance, many people cannot imagine driving with printed paper maps, and the inefficiency associated with it, thanks to GPS navigation systems.

In addition to the growth experienced due to the efficiency of technology, recently, everyone in the world experienced a pandemic that required people to stay at home some people were required to work from home. Many Companies declared a work-from-home order necessitating a spike in streaming technology and overall data consumption. Companies that produced and supported streaming and video services, chat services experienced a boom, but these also increased the demand for devices and cyber technology experienced a surge. From children learning at home to holding board meetings and church services over the internet, more devices were required. Although the pandemic is over, many companies and sectors never regressed back to the old order, hybrid work situations and low in-person turnout in religious and business meetings have led to a sustained increase in the demand for cyber security professionals.

This surge in the adoption of cyber technology whether from its organic growth or the force majeure Occasioned by the COVID-19 pandemic has led to an increase in cyberattacks and left a gaping hole in the quest for more Cybersecurity personnel. In response to this golf, many programs have been put forward by the Government and private organizations towards encouraging more people to enter the cybersecurity field, but these initiatives seem slower to deliver results than the rate at which demand for cybersecurity personnel increases.

Existing Academic Structures

Academic institutions are generally set up to equip students with appreciable skills necessary for competing in the job market. The quality of skills gathered by students in relation to the level of skills required by most jobs is one argument for another day, but more importantly, the number of students being guided from high school into a Cybersecurity career path, the number of colleges with cybersecurity options, in relation to social science career paths with shrinking career opportunities is another area worth investigating.

On average, it takes a student 3-4 years to graduate from college. Students start out studying prerequisites and by the time they graduate a huge shift has been made in technology. Many institutions still uphold a result scale that lays emphasis on the final result and tests score more than the learning process.

It might be of interest to know the number of high school counsellors and parents that can confidently tell their wards what cybersecurity is about and the classes /subjects of focus most beneficial to a cybersecurity career at the high school level. Most parents still carry the mindset of Psychology, Medicine, Law, Engineering, and Architecture as major areas of focus when guiding their children. At the high school level, many children are not adequately guided into subfields within cybersecurity thus leaving a bigger deficit.

Although the Cybersecurity industry has several subdomains like Application security, identity and access management, mobile security, cloud security, disaster recovery, and business continuity planning, it is interesting to measure how well our current education system equips students to take up roles in these subdomains in comparison to fields like Medicine and law that have been established for more than a century.

Ever changing Job complexity and skill requirements

From Century to century, the skill required to be productive and competitive in the workplace has varied in correlation with the technology tools invented/used and how society evolved. In previous centuries, it took several decades and generations for a tool to be perfected and ultimately affect the way work was done as seen in the development of electricity, telephone communication, the invention of automobiles and airplanes. Beyond requiring decades to perfect, in many cases, it took even more time to make those inventions directly beneficial to the middle- and lower-class population.

More than ever before, the invention of tools and platforms required for work has changed so rapidly that within five years of graduating from college with a degree, the knowledge gained can become obsolete and almost irrelevant in the Information Technology world. Between 2004 and 2009 Facebook and google completely revamped digital advertising thanks to social media advancements. Between 2011 and 2016 AWS and Docker completely revamped Website hosting and how digital businesses get launched.

Today many people can launch a multi-Billion Dollar organization from a single bedroom. The same thing is anticipated of Open A-I's Chat GPT.

These fast-changing technologies also present everyone with the need to constantly upscale knowledge in order to maintain relevance in the workplace. According to novoresume.com, citing the U.S. Department of Labour, (The average person will change careers 5-7 times during their working life. Approximately 30% of the total workforce will now change jobs every 12 months.) It is estimated that the average millennia and Gen-Z will be on the top end of this prediction in the course of a lifetime. This presents a challenge for closing the cybersecurity skill gulf. Where technology makes skill quickly obsolete, new attack opportunities like (zero-day conditions) will always be present. It is noteworthy to mention that Cybersecurity today requires you to understand the basic principle of security and familiarity with a wide range of tools. Because these tools quickly become inefficient, there is a constant need for re-tooling of skills to keep up, when compared to the 1970s and 1980s, the skills required to execute most factory jobs were learnt one

time, and very little subsequent additions were needed compared to the cybersecurity industry today. Conversely, in today's job market, one of the most important skills required to land jobs is a higher body of knowledge and the ability to continuously research. This makes it more difficult for people seeking to come through the door into the field.

Human Capacity Vs Attention Deficit.

In an extension of the previous point about changing job complexity, it is important to ask a few questions: Is the ability of the human brain to hold information depreciating? Does the use of technology like social media, spellcheckers, gaming platforms, and device addictions reduce the ability of new entrants to perform job functions? Why is there an increase in the number of employee burnout emotionally and mentally?

It is no secret that more than ever before, the records of teen suicide and other indices of population mental health suggest that we are almost in a crisis as touched on by (Amiri et al, 2020) it is important to correlate these findings with productivity in the Cybersecurity industry.

On one hand, it is undeniable that the work environment, people, and organizational culture is the biggest reasons given for employee burnout as mentioned by (Greg Ward, 2020) in his Forbes article titled "Organizational Culture In The Age Of Burnout: What Every Leader Should Know" However we have chosen to look critically at the impact of constant technology device engagement on the brain and its correlation to decrease in efficiency at the workplace.

This point is predicated on the knowledge espoused by (Dyer J, 2022) stating that technology is never neutral. In his book, he chronicles the example of adopting a project for a teen church to harmonize general reading of the bible and how that drastically discouraged teens from showing up with their own Bibles. Every technology reshapes its users.

Another area where this is visible is the use of spellcheckers and its impact on spelling comprehension as stated by (Rimbar 2017). The study concludes that whilst technology increased spelling accuracy on a surface level, spellcheckers did not help the student improve their spelling comprehension.

Although to my knowledge, there is no concrete research that measures the degree to which technology makes humans dumber, it will be interesting to research the degree to which this reduces effectiveness for jobs that require a great deal of thinking.

RECOMMENDATIONS

Firstly, it is important to mention that it is near impossible to completely solve the problems arising with technology because knowledge is progressive. However, we can reduce these problems and their impact drastically if the right approach is taken and good measures are implemented.

1) The existing academic structures can be modified to cater to needs arising from niche areas like Cybersecurity. More colleges should be encouraged by Government mandates to offer stand-alone Cybersecurity programs with options that produce graduates along the existing Cybersecurity career paths mentioned above.

In addition, more students should be encouraged to participate in workforce programs. It is important to mention that Cybersecurity like most technology areas is largely hands-on, it is important for students to practice directly in the work environment. This will help create a link between academic knowledge and work environment requirements, thus creating a second-degree understanding.

2) To bridge the gap between the ever-increasing adoption of cyber technology and the shortfall in people required to work, drastic measures will be needed. In the United States of America for example, Cybersecurity is one of the areas with high-security clearance requirements for entry into the workforce. Although this is aimed at protecting the public, the reality is that external talent cannot be attracted. Whilst this is laudable, it is important that international graduates within the Cybersecurity field are not lost to other nations competing for talent. Figuratively, some of these students are extremely superior talent to everyday users of the web and can create endless opportunities and innovations in the future. On the other hand, they are now so knowledgeable about offensive security, the use of password-cracking tools, data encryption and decryption techniques, man in middle attacks; allowing these guys to return to any other part of the world exposes the United States security to more external threats. It might be possible to consider recruitment by private institutions and companies with conditions that limit their access to large-scale public data but allows them to contribute to the economy with their resource. For instance, small businesses struggle to compete with large organizations for cybersecurity talent. Many of these companies can be granted incentives like easier labour certifications, permanent residency pathways, and Work authorization conditions to hire foreign nationals in cybersecurity. Letting a trained cybersecurity Engineer return to their country of origin puts more burden on the cyber defence climate in the United States.

3) Cybersecurity Education awareness campaigns from middle to high school can help increase the number of people coming into the cybersecurity workforce. Field trips to cybersecurity departments and exposure to Security Operation Centre can be crucial in registering a grasp of what working in Cybersecurity industry entails.

Teachers and counsellors can help guide willing high school students into prerequisites for cybersecurity Courses at the College level, especially in public schools.

To combat the ever-changing job complexity and skill requirements, organizations and educational institutions would need to review curriculum more frequently. According to (Cyber Talent Network, 2019), cybersecurity practitioners should be encouraged to do the following in order to stay relevant:

A) Keep up with the news
B) Do some extra training
C)Attend Industry events.
D)Network with other practitioners

This leads me to the final point that can aid in closing the cybersecurity skill gap, “Mentorship”. It is a largely held understanding that mentorship helps to avoid unnecessary spelunking, creates focus, and leads to increased productivity along career lines (Venable, 2021).

Cybersecurity mentorship will help produce more-rounded graduates and fewer dropouts in cybersecurity.

Conclusively, the points put forward are not exhaustive of possible solutions for bridging the cybersecurity skill gap, but they will help reduce the deficit. It is believed that deploying artificial intelligence systems will help reduce the burden, but this is yet to play out significantly.

Hopefully, as we make these adjustments, we build a significantly safer Cyber-planet.

REFERENCES

Bureau of Labor Statistics (2022). U.S. Department of Labor, Occupational Outlook Handbook, Information Security Analysts, Bureau of labor Statistics, U.S. Department of Labor. [Online] Available at: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm [Accessed 18 01 2023].

Cyber Talent Network (2019). Cybertalentnetwork.org. [Online] Available at: https://cybertalentnetwork.org/2020/01/16/tips-to-keep-your-cybersecurity-skills-relevant/#:~:text=Be%20active%20on%20social%20media,sure%20to%20join%20the%20conversation. [Accessed 15 02 2023].

Dyer J (2022). From the Garden to the City: The Place of Technology in the Story of God. Revised edition ed. s.l.:Kregel Publications.

Kurtuy A (2023). novoresume.com. [Online] Available at: https://novoresume.com/career-blog/career-change-statistics#:~:text=Stats%20on%20Number%20of%20Jobs%20in%20a%20Lifetime,-The%20average%20person&text=The%20average%20person%20will%20change,the%20U.S.%20Department%20of%20Labo [Accessed 6 January 2023].

Venable DM (2021). bestcolleges.com. [Online] Available at: https://www.bestcolleges.com/blog/college-mentor-student-success/ [Accessed 15 02 2023].

Ward G (2020). Forbes Coaches Council. [Online]
Available at: https://www.forbes.com/sites/forbescoachescouncil/2020/01/16/organizational-culture-in-the-age-of-burnout-what-every-leader-should-know/?sh=36eac0b55b1b [Accessed 10 December 2022].