

Trends In The Cyber-Security Industry

Posted on January 23, 2020

Introduction

Cybersecurity is an industry that has developed due to the introduction of technology. The improvement of technology occurring each year has led to an increase in the requirement for cyber security measures and personnel. The market is destined to grow to \$231.94 billion in 2022 from \$137.85 billion in 2017 (Zadelhoff, 2017, para 3). The major target audiences in the cyber security market are consulting firms, system integrators, IT security agencies, government agencies, and managed security service providers. According to Gartner, the cyber security industry had a turnover of 62540 million euros in 2015 at the global level. The industry has changed over the years, and trends keep on arising due to the customer demands and levels of technology within the industry (Rafferty, 2016, 12). The paper will focus on addressing three top trends within the cybersecurity industry. It will also focus on an important issue in one of the trends in the industry. The major trends include cyber education, change of organization and skills for cyber security, and prioritization of cloud security.

Top Trends In The Cybersecurity Industry

Cybersecurity Education

There has been an upsurge of media reports about businesses having their data centers damaged or stolen, which show the acts occurring within the cybersecurity industry. Firms have realized the need to update their employees with the latest technology hacks and crimes to minimize cybercrime. Enterprise security teams spend their resources to improve the skills of cyber security staff on how to respond to contemporary security issues (Disparte & Furlow, 2017, para 6).

Education institutions are also working towards improving the skills of the students who are joining the job market by focusing on incorporating recent technology and how to handle cyber-attacks. The need to ensure that employees and students acquire training over time is because of the high rates of cyber crimes, which have made firms to be cautious about damage or loss of data by having personnel with cyber security readiness tips (Vogel, 2016, 32). Normal employees are also engaged in training to make them aware of the risk of logging into some websites using a firm's computer. Hackers can use the information on leaves on the site to hack into the company's computers and manipulate any data within the system for their benefit.

Change of Organization and Skills in Cybersecurity

The unemployment rate in the cybersecurity industry is zero. There is a deficiency of enough personnel who can adequately meet the needs of many firms in the industry. The change in technology has made some of the security skills some experts had outdated, hence the need for them to improve them (Caldwell, 2013, 7). Every year, the industry evolves in data governance and data classes. The changes keep the cyber security experts on their toes as they have to stay updated with upcoming and recent technologies to remain relevant in the industry.

In the past years, organizations focused on dealing with botnets, spear-phishing attacks, and DDOS, among other attack vectors. The skills required to handle each of them today have worsened due to an increase in serious cyber-attacks (Assante & Tobey, 2011, 13). They need to know how to mitigate attacks, detect intrusions and develop secure software. The industry, therefore, needs well-skilled and trained cybersecurity professionals to meet the standards in the industry, such as having white hat hacking techniques.

Preference for Cloud Security

Most firms today rely on cloud security due to factors such as increased comfort with the cost and security. About 70% of businesses prefer cloud security platforms instead of legacy systems according to a new survey from Clutch. The cloud service providers have high-end security features such as redundant power sources, surveillance cameras, biometric identifications, and concrete walls, which make the cloud sites better and more secure than a customized security system for any business (Rabai et al., 2013, 64).

Younger people have grown up using cloud solutions such as Gmail and Skype, thus their preference over other systems. The average cost of additional security measures for half of the business's cloud services is \$100,000 annually; however, the price varies with the size of the firm (Sutter, 2012, para 4). Despite the efforts of cloud providers to protect their clients' data, one cannot fully protect and be liable to clients who share their passwords freely with anyone. There are various cloud-safety tips that are used within the cybersecurity industry. Information is backed up in the cloud as well as in real-life hard drives for maximum protection. Hundreds of hard-to-guess passwords are also developed and stored in devices for future reference. One is also advised to avoid linking accounts together as well as using two-factor authentication for personal accounts.

Issue

Inadequacy of Cybersecurity Experts

The changes in skills and organization of cyber security have led to less skilled people in the industry. Front & Sullivan's report found that the cyber security workforce globally will have more than 1.5 million vacancies by 2020 (Zadelhoff, 2017, para 3). There are some reasons leading to the growing shortage of cybersecurity talent in the industry. Security businesses are looking for candidates who have technology credentials that are traditional. Some of them do not fit into the current market hence making them irrelevant to work effectively today.

Some of the college degrees in the technology field, for instance, are based on theories from books and focus slightly on contemporary issues, which makes the students who enter the industry for jobs less skilled in working on complex tasks. Security students from post-secondary schools and colleges fail to handle complicated security tasks such as spear phishing and spam, which make them lack jobs, hence creating vacancies.

Crimeware kits and malware-as-a-service operations are some of the tools that have heightened the rates of hack attacks as they have made it easy for low-tech criminals to get into hacking (Kawamoto, 2017, para 2). It has led to the rise of cybercrime. The increase of high and complex with few people ready to develop new ways to stop the attacks has also led to the increased shortage of workers. The cyber security experts spend more time handling current attacks and later encounter hardships when more cyber-attacks are introduced hence making them overwhelmed with their workload. Huge workloads make some of the experts lack time to keep up with the latest technologies in the industry, hence the lack of information to handle new forms of attacks (Barrett, 2017, para 3).

There are people who disregard the jobs due to their demands. One has to receive certification and training to develop skills in the industry. One also requires various IT skills which means most people who are not taking IT cannot handle the job. Some firms have, however, lacked the job applicants' way of testing their competence, which makes them leave out potential employees in search of new staff. Lack of staff in firms costs the loss and damage of data and finances as some hackers go to the extent of stealing finances.

Conclusion

The cyber security industry has various trends due to the ever-changing technology. There are skills and organizational changes in the industry, there is an increase in the use of cloud security, and cyber security education is often being implemented to improve the skills of the existing cyber security experts. Changes in skills and the increase in cyber crimes have led to a shortage of workers hence costing most firms loss and damage of data or finances. Firms need to have competent cybersecurity employees to ensure that they minimize their chances of receiving cybersecurity attacks.

References

- Assante, M. J., & Tobey, D. H. (2011). Enhancing the cybersecurity workforce. *IT professional*, 13(1), 12-15.
- Barrett, R. (2017). *Digital organizations face a huge cybersecurity skills gap*. *VentureBeat*. Retrieved from <https://venturebeat.com/2017/06/18/digital-organizations-face-a-huge-cybersecurity-skills-gap/>
- Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, 2013(7), 5-10.
- Disparte, D., & Furlow, C. (2017). *The Best Cybersecurity Investment You Can Make Is Better Training*. *Harvard Business Review*. Retrieved from <https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training>
- Kawamoto, D. (2017). *Cybersecurity Faces 1.8 Million Worker Shortfall By 2022*. *Dark Reading*. Retrieved from <https://www.darkreading.com/careers-and-people/cybersecurity-faces-18-million-worker-shortfall-by-2022/d/d-id/1329084>
- Rabai, L. B. A., Jouini, M., Aissa, A. B., & Mili, A. (2013). A cybersecurity model in cloud computing environments. *Journal of King Saud University-Computer and Information Sciences*, 25(1), 63-75.
- Rafferty, B. (2016). Dangerous skills gap leaves organizations vulnerable. *Network Security*, 2016(8), 11-13.
- Sutter, J. (2012). *How to protect your cloud data from hacks – CNN.com*. *CNN*. Retrieved from <https://edition.cnn.com/2012/08/09/tech/web/cloud-security-tips/index.html>
- Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, 4(2), 32.
- Zadelhoff, M. (2017). *Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It*. *Harvard Business Review*. Retrieved from <https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it>