Mirza *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 2 April-June 2018

In-Demand Skillsets in Cybersecurity

Jawad Khalid Mirza[1], Zohaib Shahid[2]
Information Security Group
Allied Bank Limited Headquarters
jawad.khalid@abl.com[1],zshahid91@gmail.com[2]

Abstract:

In the recent years, a huge shift to digitization has been observed on a global level. Due to the advantage of having easy access and other benefits, digitization is being adopted fast. With digitization, the ever-growing threat of cyber-attacks increases. Thus, the need for cybersecurity professionals, with an excellent skillset, is on a rise. Alongside this, it is important to know the skillsets of cybersecurity, which are needed the most. This is also important because once an organization knows what skillsets, it requires the most, the spending of its resources will become efficient. As a result, the protection of its digital assets can be done properly. In developing countries, like Pakistan, organizations need to know what skillsets they require the most because many of them have limited resources. Considering this problem, this research makes an effort to list and describe the most in-demand skillsets of cybersecurity in the world. As the skillsets of cybersecurity increase in number and versatility, a good knowledge of what skillsets are required can prevent saturation in the job market. This research will also help people, who are amateurs in this field, understand the concept of cybersecurity and the knowledge required to excel in this field.

Keyword: Cybersecurity, Skillsets, Cyberattacks, Network Security, Cloud Security, Security Analyst, Penetration Testing

1. Introduction

In this fast-progressing digital age, when all kinds of assets and data is being shifted online, the need for qualified cybersecurity professionals is more than ever. It is a critical issue because in this current era of technology, where many advancements have taken place, a negative aspect named cyberwar has also evolved at an astonishing pace. The attackers of today need not plan airstrikes or send an army across a border when they can just reach the sensitive assets via the internet or related technology. With this grave danger in existence, there is still less awareness of cybersecurity and a deficit of qualified security professionals in the industry. Thus, an expert blackhat can break in and eavesdrop on sensitive communication and

steal sensitive data without being detected for months or even years. Even when a security breach is detected, it is not easy to trace expert hackers because they leave no footprints. So, as observed, digital assets are always at a huge risk because they can be affected negatively without any disturbance or noise.

With every passing year, the threats, to cybersecurity, and their sophistication escalates which makes the need for cybersecurity positions a priority within organizations, according to Alice Hill, Managing Director at Dice.com [1]. As the threats evolve, the skills gap becomes wider. According to 'Hacking the Skills Shortage' report by Intel, there will be 1-2 million unfilled cybersecurity jobs worldwide by 2020 [1]. According to [2], 32% of the enterprises report that the time to fill cybersecurity and information security positions is 6 months or more. The percentage of enterprises in USA, Europe and Asia, who are unable to fill open cybersecurity positions are given below [2]. The small percentage in Asia can also be attributed to the fact that in developing countries, like Pakistan, cybersecurity is still a budding field. Organizations are still working to incorporate proper measures of cybersecurity. As more organizations will enter the realm of cybersecurity, the need of cybersecurity professionals will increase and reach the level observed in USA and Europe.

Europe (30%)

USA (27%)

Asia (22%)

Also, 37% of the companies indicate that fewer than 1 in 4 candidates are qualified for such jobs. So it is clear that there is an acute shortage of cybersecurity professionals and skillsets in the industry. Considering that, it is important for one to know about the most in-demand cybersecurity skillsets to train in. The section, ahead, give the details of such skillsets.

2. Literature Review

After an extensive study, it was found out that there is a versatility in the skillsets found in cybersecurity. Every skillset has its own importance and contributes to the whole concept of cybersecurity in its own way. Concerning their requirement, a lot of other factors also come in play like the type of data to be protected, the location of the storage of sensitive data, the approach to cybersecurity (taken by the organization) etc. Some cybersecurity skillsets, which are in the most demand, are detailed below. The order, in which they have been set, does not mean that one skillset takes precedence over the other.

2.1 Network Security

As organizations move to virtualization and cloud technology, the demand for network security professionals has increased a lot [1]. Although network monitoring applications have taken care of a lot of the work like detecting suspicious behavior but an expert person has no substitute. When it comes to threat escalation and developing countermeasures against different types of malware, organizations need experienced employees with excellent knowledge of networks [1, 3]. With the presence of critical infrastructure in business networks and the success of current ransomware, security professionals need to find and repair the vulnerable points in their networks. This skill applies to a wide array of companies like technology firms, consulting companies, government, healthcare and retail [1]. So an up-to-date knowledge of network security is essential to save an organization from multiple

threats.

2.2 Cloud Security

As mentioned before, all organizations have to handle very large amounts of data and need more infrastructure so the use of cloud solutions is on a boom. Although there are a lot of security benefits of this technology but improper use leads to increased data breaches, weak identity management and denial of service [1]. The main issue is that there is a deficiency of personnel with adequate knowledge of cloud security. In a recent Intel security report, almost half of the surveyed organizations indicated that the lack of cloud security skills discourages adoption or usage of cloud services [1]. In a research report by ESG/ISSA, 22% of the respondents said that their organization suffered from an acute shortage of cloud security skills [4]. Thus, the demand for cloud security professionals is only going to increase in the coming time. Coming to the other side of the picture, that is, the cloud service vendors, secure and proper cloud data management is also a top priority. Overall productivity is increased as a result of good cloud data management [3]. As hackers target cloud servers too, cyber security professionals, well-rehearsed in the knowledge of cloud security, are needed by vendors too.

2.3 Data Security

Data security is concerned with the protection of digital data, kept in databases or related locations, from unauthorized users like cybercriminals. The techniques of data protection include data encryption, regular backups, data masking and data erasure [5]. Concerning the ever-increasing amount of data handled by all kinds of organizations, skilled professionals are needed to analyze the need of data security and protect the data accordingly. According to [1], over half of C-level executives said that data security is among the top three business priorities in 2017. Also, the average cost of a data breach is a major concern as it is $5.28 million or 20 percent of the revenue [1]. This is without the consideration of lasting brand damage. Many operations are linked with the data, handled by an organization, so an expert data security professional can help a lot.

Organizations are getting very concerned about data security because of the increasing events of data breaches like the attack on Yahoo in 2016, which compromised 1 billion accounts [1]. In 2017, two largest data breaches, of their kind, took place and did a lot in moving data security to the top of the list of concerns of major organizations. On July 29th, 2017, Equifax, which offers credit monitoring and ID theft solutions, revealed that the data of 143 million US citizens (almost half of the country) had been exposed [6]. The stolen data included the names of the consumers, social security numbers, birth dates and addresses. Driving license and credit card numbers of about 209000 citizens were also stolen. It was later revealed that the sensitive data of 2.5 million additional US consumers had also been stolen [7]. Thus, the number of total US consumers affected, by this massive data breach, went up to a shocking 145.5 million. One of the world's "big four" accountancy firms, named Deloitte, discovered in March 2017 that it had been the target of a major data breach [8]. Lots of conditional information, including the private emails and documents of the clients, was stolen. In both cases, it was found out that the data breach had been occurring for quite some time (months) before it was discovered. As discussed before, this is one of the foremost concerns because a lot of irreversible damage has been done before the discovery.

2.4 Security Analyst

Also known as, SOC (Security Operations Center) Analyst, a security analyst with good investigation skills and experience can save an organization from many threats before they cause lasting damage. According to [4], 33% of the respondents, surveyed by ESG/ISSA, revealed that their organization has an acute shortage of investigation skills and security analysis. Another main issue is that this skillset takes years to develop so organizations usually benefit by luring security analysts from other organizations [4]. Nonetheless, harvesting good security analysts is a need of time and can benefit an organization a lot in the long term. By analyzing the network traffic, an expert security analyst can identify threats properly and can help mitigate them timely.

2.5 Penetration Testing

Through proper work done by penetration testers and ethical hackers, a company can know about the security flaws in its services and applications well before time. A well-trained pentester can identify zero-day vulnerabilities which are the ultimate targets of cybercriminals. Such vulnerabilities allow them to exfiltrate data for months or even years without the organization knowing anything [1]. In the ESG/ISSA report, 20% of cybersecurity professionals said that their organization has an acute shortage of pentesters [4]. Keeping this figure in mind, it cannot be ignored that a comprehensive security policy is only made when extensive penetration testing has been done [1].

2.6 Application Security

Cybercriminals are able to carry out successful attacks due to less awareness and implementation of secure coding. 32% of the cybersecurity professionals, in the ESG/ISSA research report, revealed that their organization suffered from a deficit of good application security skills [4]. For our own ease and usability, secure coding practices are neglected. When software is not patched properly and there are flaws in the code, data breaches become successful [1]. Thus, a professional, trained well in application security, will produce secure software, which will, in turn, protect employees from typical security threats and increase productivity [3]. Also, any secure software should be able to blend with other security measures in the organization [3]. They are not usually convenient but they can keep employees and information safe. Intensive secure code development and quality analysis will cost a lot in short term but as the probability of breaches will decrease, a long term benefit is surely present.

2.7 Risk Management/Evaluation

Excellent risk management is crucial for any organization to protect itself from cyberattacks. By gauging the importance of different assets and services of an organization, the measures for protection can be managed properly. Finding out about the risk, faced by cyberattacks, is a first step towards stopping most threats [3]. Thus, a professional with good risk management skills can save a company a lot of cost in protection of its digital assets through adequate analysis of the risks involved. Also, risk management plays a huge role in internet governance. This is because through the discovery of emerging risks, the norms, shared principles and related elements of the internet are altered which affects its evolution and way of use.

3. Analysis

Concerning the lack of cybersecurity professionals with the required skillsets, there

is a dire need to work on this vector. This is because cyberattacks are increasing exponentially and without trained professionals, they will get out of control easily. In many countries like US, UK, Singapore, India and Australia, the development of cybersecurity professionals has caught a fast pace but Pakistan still lingers behind. Although Pakistan may not have entered the digital age completely but its organizations are affected a lot by cyberattacks.

The cyberwellness of Pakistan can be judged by the fact that it ranks 67th on Global Cybersecurity Index [9]. This means that there is still a long way to go. Cyber legislation, in Pakistan, is still in its infancy but the neighbor, India, got this legislation in 2000 and has been developing quite fast in the field of cybersecurity [10]. Cybersecurity or information security is still a new subject in Pakistan. Only a few academic institutes like National University of Science and Technology (NUST) and Center for Advanced Studies in Engineering (CASE) have introduced Masters degrees and are doing good research work. NUST has also built its own Cyber Emergency Response Team (CERT). Such developments can only be quickened if academia, industry and government work jointly to build a cybersecurity strategy so the country can face the increasing threat of cyberwarfare. There is a need to introduce cybersecurity as a subject in Bachelors Degrees of engineering field so students can realize its requirement in the world of today. Also, it has been observed that students of cybersecurity put in a lot of effort in good research but that research seldom targets problems in the industry. The gap between the academia and industry should be bridged. Students should be given projects or research work, based on the problems of cybersecurity, faced by the industry. Such research will not only solve the issues of the industry but will also be very beneficial for the student's career. In this way, they will have a better idea of the issues to tackle once they start their jobs. Also, organizations, in Pakistan, should start spending more on cybersecurity as it has become the staple need, of today, quite rapidly. As a common man, in Pakistan, is still unaware of the dangers he or she faces online, cybersecurity awareness should be a principal target of every major organization like banks and organizations in the government sector. As observed, Pakistan might be far behind in cybersecurity, as compared to other countries, but the efforts being made, no matter how small they are, will help in catching up with others soon.

4. Conclusion

As observed during this research, the knowledge, required to understand cybersecurity, cannot be attached to something specific. The skillsets, described in this paper, not only require one to understand cybersecurity properly but also have thorough knowledge of computer systems, networks and related entities. These skillsets also show that people from other lines of career like business studies can play an important part too. For example, in the case of risk management/evaluation, professionals, from the field of business studies, can help produce appropriate policies and frameworks once they are trained in the basics of cybersecurity. Overall, for the proper progress and awareness of cybersecurity, it is important for technical and non-technical people, in an organization, to work together to implement it. For any novice in cybersecurity, this research work can help the person catch up quickly on cybersecurity and choose a path to build his or her career. Organizations, especially in

Pakistan, should understand that if they hurry in adopting cybersecurity measures and employ and train cybersecurity professionals properly, they will be able to survive and grow in this era properly.

It should be understood that cyber threats are more of a reality now. They can only be avoided by promoting cybersecurity, as a career, in educational institutes and training interested students or professionals, right from the beginning. If the concept of cybersecurity is introduced this early, it will be very easy to fill the shortage of professionals and skills, faced by the industry. Also, Pakistani organizations should consider spending proper resources on cybersecurity for the development of this field and encouragement of people so they may excel in it.

5. References

[1] A. Bennett, "These Are the Most In-Demand Cyber Security Skills for 2017," 28 February 2017. [Online]. Available: https://techspective.net/2017/02/28/demand-cyber-security-skills-2017/.

[2] ISACA, "State of Cyber Security 2017," 2017. [Online]. Available: https://cybersecurity.isaca.org/info/cyber-aware/images/Cybersecurity-Skills-Gap-2017-1500.jpg.

[3] J. Buntinx, "Top 5 Cyber Security Job Skills In High Demand for 2017 and Beyond," 26 February 2017. [Online]. Available: https://themerkle.com/top-5-cyber-security-job-skills-in-high-demand-for-2017-and-beyond/.

[4] J. Oltsik, "High-demand cybersecurity skills in 2017," 20 December 2016. [Online]. Available: https://www.csoonline.com/article/3152023/security/high-demand-cybersecurity-skills-in-2017.html.

[5] Wikipedia, "Data security," February 2012. [Online]. Available: https://en.wikipedia.org/wiki/Data_security.

[6] M. Kumar, "Equifax Hack Exposes Personal Info of 143 Million US Consumers," 7 September 2017. [Online]. Available: https://thehackernews.com/2017/09/equifax-credit-report-hack.html.

[7] S. Khandelwal, "Whoops, Turns Out 2.5 Million More Americans Were Affected By Equifax Breach," 2 October 2017. [Online]. Available: https://thehackernews.com/2017/10/equifax-credit-security-breach.html.

[8] M. Kumar, "Deloitte Hacked - Cyber Attack Exposes Client's Emails," 25 September 2017. [Online]. Available: https://thehackernews.com/2017/09/deloitte-hack.html.

[9] ITU, "Global Cybersecurity Index (GCI) 2017," International Telecommunication Union, 32017.

[10] A. Raza, Securing Cyberspace For Pakistan, Lahore, Punjab: Information Technology University, 2016.