Rahul Khurana
CST 300 Writing Lab
17 January 2020

Cybersecurity

Cybersecurity is one of the most fundamental and rapidly growing industries in the technology world right now. With technology companies becoming a fundamental part of global economies, and the world's transition to digital infrastructure, so too has the threat of cyberattack and hacking grown with it. This has by necessity required companies to invest in skilled personnel who can defend against these threats. As such, it is expected that by 2029, the number of information security analyst positions will grow by 31% from 2019 (Bureau of Labor Statistics, 2020).

Incidents of hacking and cyber intrusion have been on the rise for some time, and have only increased during the pandemic (Sheng, 2020). These attacks are costly and can cost companies affected in the area between hundreds of millions of dollars of losses, to billions. To counter these attacks, cybersecurity personnel are responsible for a variety of mitigation strategies to reduce the potential harm to companies. While application security professionals are involved in the software development process, operations security are responsible for the protection of datacenters and cloud environments, while those trained in governance, risk, and compliance focus on developing security awareness throughout the company, developing security policies, and ensuring alignment between a company's security strategy and its business priorities. In addition, penetration testers are trained to look at an environment in the same lens as a hacker, to best determine the vulnerabilities within a company's environment.

More and more companies are involved with recruiting these skilled individuals who have the appropriate knowledge to secure environments against cyber intrusion. In the wake of

the transition to cloud and app-based infrastructures, many companies such as Apple, Facebook, Salesforce, Box, and Microsoft are seeking more positions dedicated to information security. Of these, Microsoft is one that has undergone a significant transition from its inception. Microsoft was founded in 1975 by Bill Gates and Paul Allen as a software company focused on the Altair 8800, eventually making a deal to create the operating system for IBM's first personal computer (Microsoft, 2020). Eventually, Microsoft released the household name of Microsoft Windows, their flagship operating system that still runs most personal computers. For decades since, Microsoft was well known as primarily a software company, producing its flagship Windows operating system, as well as productivity software such as Microsoft Office.

Throughout the 1990s, Microsoft continued to gain influence and was considered one of the most successful software companies in the world. At the turn of the millennium, Microsoft was the subject of the infamous United States vs Microsoft Corporation antitrust lawsuit. While the case was eventually settled, it is considered to have contributed to decreasing Microsoft's stature and limiting them through the early 21st century. Since then, however, Microsoft has since ventured into other areas, with hardware such as the Microsoft Surface, gaming platforms such as the Xbox, and large online platforms such as Microsoft Teams and LinkedIn. However, one of the most strategically important has been Microsoft's cloud computing service in Microsoft Azure.

The current CEO of Microsoft, Satya Nadella, began his tenure as CEO in 2014, taking over from Steve Ballmer. Having worked at Microsoft since 1992, he was educated at Manipal Institute of Technology in India, and at University of Wisconsin – Milwaukee. He is widely considered to have successfully overhauled Microsoft's culture and guided it to a turnaround from a weak position at the turn of the millennium (Business Insider, 2020). Likewise, Bret

Arsenault is the Chief Information Security Office (CISO) at Microsoft. Having a degree from The College of Idaho, he has worked at Microsoft for over 30 years. Having led Microsoft's early network security strategy, building security products, and a variety of other tasks, Bret oversees information security for Microsoft across a large variety of its divisions, from Azure Cloud to its software development. (Krazit, 2020)

From a products perspective, the Azure Cloud Platform is one of Microsoft's most important assets. In recent years, Microsoft has gained an increased share of cloud computing market share, with a report in 2019 showing 29.4% of application workloads compared to 41.5% on the largest competitor, Amazon Web Services (McAfee Cloud BU, 2019). The Azure Cloud Platform hosts a tremendous number of large customers for Microsoft, and as such, protecting it from cyberattack is vitally important to preserve its reputation and data. Microsoft also needs to defend major online products such as Microsoft Teams, GitHub, LinkedIn, and others.

In addition, from a software perspective, Microsoft still develops the Windows operating system and needs to maintain its security – not just for its own sake, but since most personal computers on the Internet rely on Windows security. In addition, Microsoft maintains many of its original office productivity software that must be kept secure, including Microsoft Office, the Internet Explorer browser, and Skype. Microsoft also has to defend its hardware divisions from cyberattack, with both hardware products like Surface and gaming division products like Xbox representing a greater surface area and requiring commensurate protection.

Microsoft's current reputation in the industry is one of considerable respect. Microsoft, while having a rough patch in the early 21st century, has largely regained its reputation as an industry leader, and Microsoft Azure runs the backbone of 95% of Fortune 500 companies (Microsoft, n.d.). With over 160,000 employees, they have a strong base of talent to work with at

the company. Their cybersecurity is well lauded, and they have multiple certifications attesting to their strong cloud security. Furthermore, Microsoft has decades of experience with software development and security, which is a claim few other companies can hold.

Cybersecurity is a vast field, and its importance is only growing over the next few decades. The current environment shows that the demand for cybersecurity professionals exceeds supply, and that gap is only expected to widen over the next decade as the threats facing the corporate world continue to evolve. As such, gaining the skills required to successfully participate in this field is likely to prove very fruitful for individuals seeking employment in the tech industry.

I am currently employed as a cybersecurity professional, with my current position being an Information Security Manager at SAP, currently leading a Governance and Risk team. In order to continue my career, my aim is to reach higher for a Director position, or potentially a Cybersecurity Architect position at a major tech company focused on SaaS (Software as a Service) offerings. While I possess several skills in cybersecurity and risk management, including certifications in CompTIA Security+, ISC2's CISSP, and ISACA's CISM and CRISC, I believe I still can gather more skills to solidify my position and advance my career.

While my background in the Governance and Risk Management fields of cybersecurity is strong, my background in application security is less strong, which I need to strengthen to successfully meet the criteria for cybersecurity architecture knowledge. To gain this experience, my courses as CSUMB will enhance my knowledge of different programming languages and allow me to understand more about different attack techniques in practice, including buffer overflow attacks and other OWASP (Open Web Application Security Project) Top 10 attacks. In addition, CSUMB has courses that focus on operating systems and databases, both of which will

greatly aid my technical knowledge when it comes to application security and development security techniques (Microsoft, n.d.). A deeper understanding of operating systems will allow me to better understand techniques such as virtual machine escape, privilege escalation attacks, and a better understanding of databases (relational and non-relational) will allow me to comprehend the variety of defensive techniques such as field level encryption that can be utilized at the database level.

In addition to my courses, there are additional things I plan to do to aid my career growth. While I am already familiar with the basics of penetration testing, if aiming for a Director of Information Security position or a Cybersecurity Architect position, I should have additional knowledge in that field. Kali Linux, one of the most well-respected operating systems among penetration testers, is created by the Offensive Security group, who also offers the OSCP certification. This certification involves an extended training course in the usage of Kali Linux and its associated tools like Burp Suite, bash attacks, evading antivirus, Metasploit, and is followed up by a real-world 24-hour examination during which participants engage in a proctored hands-on penetration test of a simulated environment.

There are also several skills I need to gain in management and leadership. Udemy hosts several popular courses focused on practical leadership skills and management skills that I plan to complete over the next few years. Furthermore, there are excellent books that cover the topic that I have been recommended from friends and coworkers that I intend to read and learn from.

There are several industry conferences that I intend to attend to gain more knowledge from peers at other companies such as RSA, Black Hat, and DEFCON. Participation at these forums helps to ensure that one does not fall behind in a field as fast paced and complex as cybersecurity, and features professionals from across the industry. As soon as these conferences

reconvene in a post-pandemic world, I intend to attend these regularly to stay up to date with my peers at other organizations.

Lastly, while I possess strong knowledge in Governance and Risk Management, I could stand to improve on my knowledge of the compliance sphere, specifically on the NIST cybersecurity framework and the ISO framework. The NIST framework is run by the National Institute of Standards and Technology, a subdivision of the US Department of Commerce, and is a publicly available that covers a broad region of cybersecurity activities and outcomes that companies can adopt. Similarly, ISO (International Organization for Standardization) is an independent nongovernmental organization based out of Switzerland that also offers a framework for organizations to organize their cybersecurity activities and outcomes. To further my knowledge and understanding in this sphere, I intend to review and understand these frameworks and their associated activities and controls to best guide my knowledge of how these frameworks intersect with real-world activities that the organizations I work with perform.

These skills that I intend to gain will prepare me for the challenges ahead as I intend to gain additional expertise that will enhance my credibility and ability to execute on cybersecurity initiatives at my current organization and any further organizations I am employed at. Combined with my academic learnings at CSUMB, I have every confidence that my career will continue to progress in the direction I desire.

The field of cybersecurity is vast and is expected to grow and adapt even further into new fields and areas such as artificial intelligence and cloud computing. Presently, the industry suffers from a burgeoning skill gap in terms of available professionals, and there is significant current and expected future demand from organizations that require these skills. Many organizations such as Microsoft have multiple divisions that must respond to the challenges in

the cybersecurity sphere. As such it is worth investing in skills and knowledge that allow one to enter or continue in this career. While I already am in this sphere, I can improve on my skills and progress in my career towards promising positions such as Director level position by advancing my skills and knowledge further with academic progress, additional certifications, industry participation, and self-study.

References

Microsoft. (2020, September 15). About Microsoft. *News*. Retrieved January 10, 2021, from https://news.microsoft.com/about/

McAfee Cloud BU. (2019). Cloud Market Share 2019: AWS vs Azure vs Google – Who's Winning? *Cloud Security*. from https://www.mcafee.com/blogs/enterprise/cloud-security/microsoft-azure-closes-iaas-adoption-gap-with-amazon-aws/

Sheng, E. (2020). Cybercrime ramps up amid coronavirus chaos, costing companies billions. *CNBC*. Retrieved January 17, 2021, from https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html

Microsoft. (n.d.). Facts about Microsoft. *News*. Retrieved January 10, 2021, from https://news.microsoft.com/facts-about-microsoft/

Bureau of Labor Statistics. (2020). Information Security Analysts. *Occupational Outlook Handbook*. Retrieved January 17, 2021, from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

Business Insider. (2020). Satya Nadella employed a 'growth mindset' to overhaul Microsoft's cutthroat culture and turn it into a trillion-dollar company — here's how he did it. *Strategy*. Retrieved January 17, 2021, from https://www.businessinsider.com/microsoft-ceo-satya-nadella-company-culture-shift-growth-mindset-2020-3.

Krazit, T. (2020, June 9). The most interesting man at Microsoft. *Protocol*. Retrieved from https://www.protocol.com/bret-arensault-microsoft-ciso-profile

Microsoft. (n.d.). What is Azure-Microsoft Cloud Services: Microsoft Azure. Retrieved January 17, 2021, from https://azure.microsoft.com/en-us/overview/what-is-azure/