The importance of a postgraduate degree in the Cyber Security field

Table of Contents

Introduction 2
Discussion 2
Reflection and observations 3
Conclusion 3
References 4

Introduction

Cyber Security is a vital part of any organisation as it enforces protection of data , software and hardware from damage and theft through processes and technologies. It includes sensitive and confidential security information, protected health data, personally identifiable information, military information and intellectual property data. Without the consideration of cyber-security measures, the organization cannot adequately defend and mitigate the risk of their information from being breached (Sherf, 2022). This essay is aiming to analyse the importance of a postgraduate degree in the cyber-security field along with reflecting on experiences and observations of this specific industry.

Discussion

A postgraduate degree in the cyber-security field is essential as it equips student with an overview to better manage and secure systems from both technical and strategic perspective. It provides a suitable opportunity for the students to strengthen their knowledge base, apply critical problem solving techniques and also inherently be equipped to design and implement security strategies. This field is underserved and there is demand for highly skilled specialist. (Collegeconsensus, 2022). Pursuant to the recent Covid pandemic there has been a sharp increase in digitalisation and the industry has been forced to quickly adopt and develop mitigating processes and technologies. The accelerated pace of digital automation and the industrial revolution brings with it risk issues as the manufacturing industry has a heavy reliance on computer operated machines.

There needs to be a paradigm shift in focus which will be brought about by more research orientated educational development. Historically there were no formal Cyber security qualifications and this area was predominantly served by computer scientists developers.

It is not known what the motivation is for some attacks which increases the emphasis of also understanding the human behaviour element. Undergraduate learning usually does not cover the human element of cybersecurity and hence limited specialist research available on

Most governments need to employ academic orientated pragmatic approaches to their strategies if they want a cyber resilient strategy. There is a growing need for research based strategies which can only be explored within an academic institution, specifically at post graduate level. The regulatory and legislative landscape needs to be aligned and integrated with technology advancements and critical assessment of safety and system integrity issues.

The increase in demand in the highly educated specialists is also partly due to cyber criminals constantly upgrading their knowledge base.

Reflections and observations

The postgraduate qualification provides a comprehensive overview and technical application of theoretical concepts in a real business context. This speciality is still in its new and therefore forcing business to reduce the skills shortages by investing in upskilling their employees. There are 3 key differences between certificates and postgraduate level cyber security study; namely

· Post graduates degrees do not require constant renewal or upgrading or qualification as seen with certification qualifications.

· The measure of competency is incrementally more in depth at post graduate level and requires a higher level of critical thinking and complex analysis, peer discussions and report writing.

· The objective of post graduate study is to continuously improve and expand knowledge and emphasis is put on individual thinking and unconventional solutions using proven concepts.

Conclusion

The primary focus to pursuing this qualification is to effect change. Its important to highlight how security breaches, threats and high-tech warfare waged, have caused financial damage, in some cases loss of lives and crippled governments. There are various opportunities to create employment as this specialist field is still in its infancy and not many educational institutions offer it. My objective is to unpack the legalities and governance issues. Change starts with improving policy so law enforcement organisations are able to promulgate additional laws using technical and practical understanding of the field. The South African Cybercrime Act only came to effect in December 2021. The act also criminalises the act of sharing messages which was not received well by the country as its seen as an infringement of a basic human rights which is freedom of speech. The promulgation has translated to some convictions.

References

Carrapico, H. and Barrinha, A., 2018. European Union cyber security as an emerging research and policy field. European Politics and Society, 19(3), pp.299-303.

Collegeconsensus, 2022. 10 Best Degrees for a Career in Cyber Security. [online] Collegeconsensus.com. Available at: <https://www.collegeconsensus.com/degrees/best-degrees-for-cyber-security/> [Accessed 5 June 2022].

Moore, M., 2022. 10 Reasons Why a Cyber Security Degree is Worth It. [online] University of San Diego Online Degrees. Available at: <https://onlinedegrees.sandiego.edu/10-reasons-to-get-your-masters-degree-in-cyber-security/> [Accessed 5 June 2022].

Sherf, E., 2022. The importance of cyber security in journalism. Network Security, 2022(4).

Tunggal, A., 2022. Why is Cybersecurity Important? | UpGuard. [online] Upguard.com. Available at: <https://www.upguard.com/blog/cybersecurity-important#toc-7> [Accessed 6 June 2022].

E. de Boer, D. Hernandex Diaz and H. Leurent (2018). The Fourth Industrial Revolution and the Factories of the Future. McKinsey & Company. Accessed 08 June 2022

Spidalieri, Francesca, and Jennifer McArdle. “Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The Role of Cybersecurity Education in US Service Academies.” The Cyber Defense Review, vol. 1, no. 1, 2016, pp. 141–64. JSTOR, http://www.jstor.org/stable/26267304. Accessed 9 Jun. 2022.

Drent, Margriet, et al. “Case Study Cyber Security.” Civil-Military Capacities for European Security, Clingendael Institute, 2013, pp. 53–63. JSTOR, http://www.jstor.org/stable/resrep05404.8. Accessed 9 Jun. 2022.