Udaya Tejas Vijay Anand

Kara Parks Fontenot

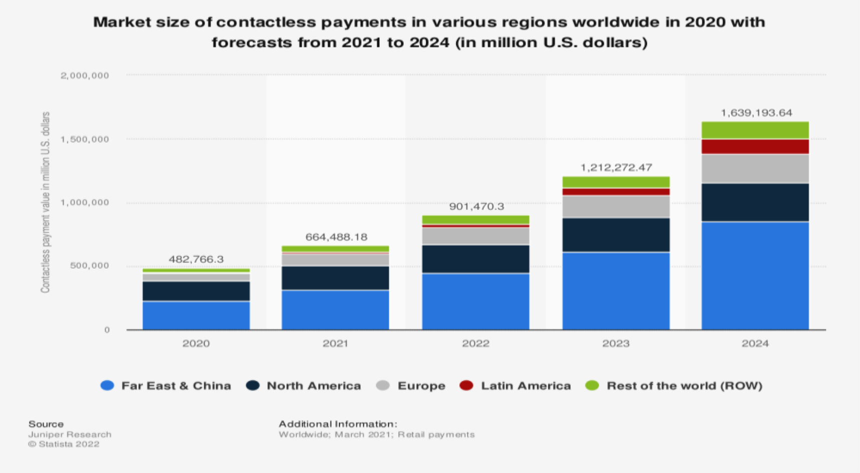
WR 1011

06 October 2022

Ethical Hacking: An Essential Course WPI Should Offer

With the advancement of the technology we possess, it has also come with a certain degree of drawbacks that every sector faces. Due to a lack of cybersecurity infrastructure, we can no longer prevent or stop cyber warfare attacks from hackers. Future information security professionals are adapted to have the same skill as attackers to adequately recognise and defend networks from intrusion. But when this comes to a profession – people tend to lean towards the safer side of the spectrum to get a safe and secure job. On the contrary, numerous institutions educate students on the fundamentals of Cybersecurity and how to protect themselves from an attacker but never really teach them the offensive side. Getting the students exposed to the hackers' perspective on how these attacks are performed could help them develop a much more innovative and efficient solution to such problems. Multiple articles discuss whether the adaptive process would be viable through research and have concluded their findings (Hartley (2015)).

Figure: 1



Market size of contactless payments in various regions worldwide in 2020 with forecasts from 2021 to 2024 (in million U.S. dollars)

Source
Juniper Research
© Statista 2022

Additional Information:
Worldwide; March 2021; Retail payments

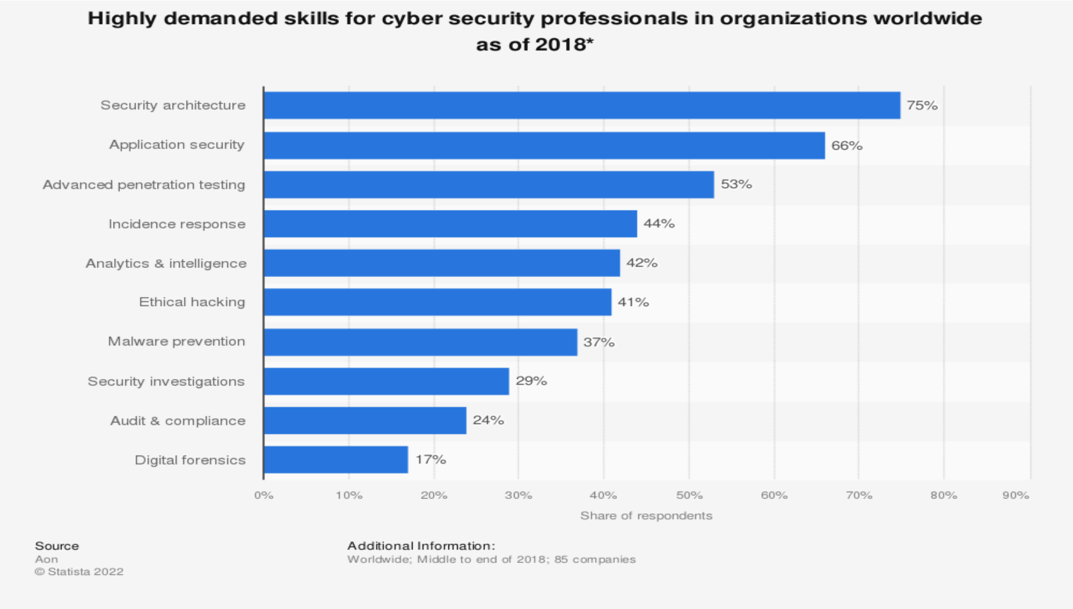
(https://www.statista.com/statistics/1227815/contactless-payments-worldwide-by-region/)

WPI’s cybersecurity program has been ranked as one of the top five cybersecurity programs offered all across the United States, and it’s a relatively popular and well-opted course on a graduate level. When the institute covers the defensive side, covering the offensive side would make both programs equally engaging and competitive. This could offer a wide range of scope and further branch out into different areas of computer science to specialise in a particular component – like network or cloud administration, hardware handling, software support etc. But with digitalisation emerging as a phase – the economy and the way things operate around us – from self-driving cars to making the minor transaction at a grocery store are transitioning to depend more on technology. This has opened up a wide range of possibilities for hackers to exploit the vulnerabilities of emerging technology. We currently don’t have the resources, the skill, or the people to protect what’s around us. As shown in Figure 1, the amount of contactless payment, which is the most yet useful and most targeted platform, is yet to increase by over 150% in a course of two years.

The hacking skill is a potent tool and could get exploited if it gets into the wrong hands. Therefore, sources suggest selecting potential students during the probation period by evaluating and qualifying them on a survey basis to learn their true intention of the skills they’re going to pursue (Trabelsi, & McCoey). Therefore, the selection process of the candidates is crucial to prevent incidents at a much earlier stage. Even though it’s a contradicting claim to say that some knowledge is confined to a smaller audience group, it’s for the betterment of humanity.

Figure: 2

Demanded skills for cyber security professionals in Organizations worldwide



Source
Aon
© Statista 2022

Additional Information:
Worldwide; Middle to end of 2018; 85 companies

Note: This statistic shows the most highly demanded skills for cyber security professionals worldwide as of 2018. Around 75 per cent of respondents from AON Hewitt's Global Cyber Security Talent Survey stated that "security architecture" was the most in-demand skill for cyber security professionals in their organisation.

(https://www.statista.com/statistics/979499/worldwide-cyber-security-most-demanded-skills/)

Every sector will use ethical hacking as a profession for penetration testing and to check for vulnerabilities in their programs and firewall to develop solutions. This would be a space which would require constant development. To receive an Ethical Hacking degree, a candidate must have specialised in a particular area of computer science and should have learned the cybersecurity aspect of it to protect themselves from the existing threats. As shown in Figure 2, we can see how the inclusive of the following courses are not only primarily oriented towards hacking but also aspects of other areas and considering these are requirements for this course be beneficial for the candidate not only to get well exposed but to secure a high yielding job position. This entire process could take around seven years to complete to become an Ethical Hacker who could pursue his career. As time-consuming and effort-taking as this course can be, a career in this field would be highly demanded by the community and considerably well-paying and respected as time passes. This course has been taught at a graduate level across the world. There's even a cybersecurity concentration offered by WPI exclusively for Computer Science, Robotics Engineering, and Interactive Media Game Development majoring students, but with the benefits of how much this could help in favour of cybersecurity students for competitive learning and arising Ethical Hacking as a major could also be relatively more manageable for the university to get started with minimal resources.

Four Significant Assignments:

The increase in the number of research made in this field has given us more information on computer administrations and comparable knowledge and skills of the attackers. Therefore, it's crucial to determine the required skill sets and educate security professionals. (Hartley. (2015)) Moreover, the skills used in ethical hacking are considered reactive rather than proactive, meaning the action is taken by analysing the past to anticipate the future. Furthermore, educators tend to lean towards "offensive methods" to produce better security professionals than teaching "defensive techniques", which is the traditional way. This particular also suggests that candidates should receive to prepare them for intense research and development in their careers. *"One cannot perfectly design or build defences for attacks that one has not truly experienced, first-hand"* is a quote from this article which summarises the author's distinctive thoughts, which correlates with the framework of this article (Trabelsi, 2011).

- ***Labs – Discussion:*** Contributed lab sessions are proven ways to enhance new techniques to protect ourselves from hackers (Hartley. (2017)). The author's argument is to expose graduate students to a broader range of interdisciplinary viewpoints – may be the key to nurturing creative and digital capabilities. The article suggests that creative hacking and multidisciplinary collaboration will allow the participants to draw their resources – to provide innovative solutions that can significantly impact the profession (Kessel. (2019)).

- ***Hackathons:*** These competitions have different characteristics, configurations, and goals yearly to live security exercises involving dozens of universities worldwide. Two other competitions (Treasure Hunt and a Bot-net-inspired competition) serve as the most extensive security exercises ever attempted. Hundreds of people have come to participate in these competitions. They've devised a structured guideline to make the competitions fair for the other educators and students who pursue the same interest, thus making the course work practical and engaging.
- ***Competing with Cybersecurity:*** With what's being learned theoretically, these techniques could be in the sequel with the cybersecurity students. With a simulated lab, the Hacking students can apply their offensive tools while the Cybersecurity students can practice defending against these attacks. This benefits both ends, thus also making the learning process competitive and engaging for both majors. As controversial as it could sound, nothing but a practical approach could teach the students about what they're learning in class and where it could get applied.
- ***Hands-on Approach and Soft Skills:*** Articles suggest that book and lecture-based learnings are not always as practical as demonstrating concepts through a hands-on experience (Logan and Clarkson (2005)). Supporting the same claim made by another article states that "hands-on security should be provided in all core classes" (Weiss and Mache (2011)). Therefore, taking a practical approach would help the students learn

effectively. Therefore, connecting the learnings with case studies could help the students connect and relate to real-life instances.

Similar to the other research, this article aligns with the methodologies' ideologies and practices. It will justify the need for an Ethical Hacking program as a part of the WPI curriculum. With a considerable amount of ethical considerations, it might lead to scrutinising the *Computer Use Policy* should keep that in check. But the key to the course would be to keep the students engaging with their course work in different forms but not to provide the same kind of work and overload them to the extent that could put them under significant stress. This balance would ideally provide top-tier security professionals to the society.

References

"Global Cyber Security Survey." *Www.aon.com*, www.aon.com/germany/human-capital-consulting/talentengagement/global_cybersecurity_talentand_compensation_survey_2018.jsp. Accessed 10 Oct. 2022.

Childers, N. *et al.* (2010). Organizing Large Scale Hacking Competitions. In: Kreibich, C., Jahnke, M. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2010. Lecture Notes in Computer Science, vol 6201. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-14215-4_8

Hartley, R., Medlin, D., & Houlik, Z. (2017). Ethical hacking: Educating future cybersecurity professionals. In *Proceedings of the EDSIG Conference ISSN* (Vol. 2473, p. 3857).

Hartley. (2015). Ethical hacking pedagogy: An analysis and overview of teaching students to hack. Journal of International Technology and Information Management, 24(4), 95–. http://proc.iscap.info/2017/pdf/4341.pdf

Kessel. (2019). Pracademic collaboration: Hacking into the future of legal education. Alternative Law Journal, 44(1), 73–75. https://doi.org/10.1177/1037969X18814980

Logan, P., & Clarkson, A. (2005). Teaching students to hack. SIGCSE Bull. ACM SIGCSE Bulletin, 157-157.

Trabelsi, Z. (2011). Hands-on lab exercises implementation of DoS and MiM attacks using ARP cache poisoning. Proceedings of the 2011 Information Security Curriculum Development Conference on - InfoSecCD '11

Weiss, R., & Mache, J. (2011). Teaching security labs with web applications, buffer overflows and firewall configurations. Journal of Computing Sciences in Colleges, 27(1), 163-170.