

## Critically discuss the importance of being able to program competently in the cyber security environment

This essay will look into the importance of being able to program in the cyber security sphere. It will also look into the reasons for and against the importance of being able to competently program, if this is affected by GDPR and if it is, how it affects the need for programming competency. It will also look into the whether or not having the ability to program competently affects the chances of being employed in the cyber security field and also look at what companies that are currently hiring are looking for in their cyber security personnel.

The main argument for being able to program competently is that programming knowledge is “essential for analysing software for vulnerabilities, identifying malicious software, and other tasks required for cyber security analysts.” (Ruddy, 2015). Within (Ruddy 2015) it is argued that a knowledge of programming is essential for people working in cyber security as looking over and checking software for vulnerabilities and for malicious code needs a good understanding of programming to do. In (Singh, 2013) it is argued that programming argues that for web application security, software security, Malware analysis and Reverse engineering, Network security, Computer forensics. However, it goes onto say that not all realms of cyber security need the same level or programming competency. For example, with web application security a person working in that field would need to be competent in web languages such as PHP, JavaScript and database languages like SQL so that they can see the obvious and less obvious security flaws. For something such as software security, you also need to be competent in whatever language the program is coded in. If they work in the field of malware and virus analysis and reverse engineering, you would need to know basic assembly as well as how to use basic debuggers. For a network security engineer, you would have to be competent in the basic security protocols and how they work. However, for a field such as computer forensics needs minimum programming knowledge as well as knowing about file systems etc.

It is argued by (Ruddy, 2015) that the “ideal cyber security professional” possesses knowledge of basic, key computing fundamentals such as computer architecture, basic system’s administration as well as knowledge of a variety of operating systems. They also need to know some more advanced features, such as knowing how to set up networks, use virtualization software, configuration and manage firewalls, set up network load balancers, set up and maintain network routers and switches, and other pieces of network architecture this has been brought about since there has been a huge amount of data being produced over the last few years people have been looking to cloud storage to store all of their photos and other bits of data on networks and with the advent of cloud computing, Software-as-a-Service (SaaS), which can now be accessed through web browsers, mobile devices and even TV’s these now require a detailed understanding of security on this level. and other common tools used in commercial IT systems. While this cyber security professional may not be able to code as well as others if they have this comprehensive understanding of system architecture, it will allow them to have a greater understanding of the big picture view which in turn allows them to see where possible vulnerabilities lie and how to best protect from attacks.

As discussed in (Harrison, 2004) companies often hire what he calls “dilettantes”. These “dilettantes” are programmers who have had no formal education in programming such as doing a computer science degree but are people who have been taught by or are so called “end user” (Harrison, 2004) programmers. The problem is, is that a lot of companies especially in the 1980/90s hired people who

said that they could code or had coding experience, for them to work on things internally do they didn't have to hire people to make them programs. This has led to poorly trained and unqualified programmers working on software which had important information either stored on them or used by them. This was fairly ok in the 1980/90s as most things were local and therefore applications were fine. However now with nearly everyone online companies are still hiring these unqualified programmers which are leading to a lot of security implications. In the wake of GDPR this means that companies are going to be less likely to employ people simply because they can program. As GDPR comes into force companies are going to be a lot more careful with how they treat cybersecurity as "Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million." (EUGDPR.org, 2018)

After having a brief look online at what job opportunities exist for people looking to enter the cyber security field there seem to be mixed bag between jobs that want programming experience and those that don't care. Although that being said those job vacancies that care about programming experience were generally better paid than those which didn't care. (Job Search, 2018), (Job Search, 2018).

In conclusion, the importance of being able to program competently in the cyber security environment all depends on what you want to get out of the cyber security environment. For example, certain fields in cyber security such as reverse engineering malicious programs you need to be able to code competently, however if you're going to do high level things such as computer forensics, you don't really need to know how to code, just have an understanding about computers. This is generally reflected in the jobs, with the cyber security jobs requiring coding skill being the most competitive and having the highest salaries due to the increased work load involved with them. As well as this GDPR is causing companies to take cyber security very seriously as a result of this the amount of cyber security jobs has increased dramatically increased with about a 0.6% growth per year in terms of the percentage of IT jobs that are about cybersecurity, which it currently stands at "2.13%" (ITJobsWatch, 2018).

## References

EUGDPR.org. (2018). GDPR FAQs. [online] Available at: <https://www.eugdpr.org/gdpr-faqs.html> [Accessed 19 Jan. 2018].

Harrison, W. (2004). From the Editor: The Dangers of End-User Programming. *IEEE Software*, 21(4), pp.5-7.

ITJobsWatch. (2018). Cybersecurity UK. [online] Available at: <https://www.itjobswatch.co.uk/jobs/uk/cyber%20security.do> [Accessed 19 Jan. 2018].

Job Search. (2018). Airbus Group Network Security Operation/Technology Specialist. [online] Available at: [https://jobsearch.direct.gov.uk/GetJob.aspx?JobID=45184098&JobTitle=Network+Security+Operation%2fTechnology+Specialist+\(m%2ff\)&redirect=http%3a%2f%2fjobsearch.direct.gov.uk%2fhome.aspx&pp=25&pg=1&sort=rv.dt.di&re=134&q=Cyber+Security&AVSDM=2018-01-25T01%3a33%3a00-05%3a00](https://jobsearch.direct.gov.uk/GetJob.aspx?JobID=45184098&JobTitle=Network+Security+Operation%2fTechnology+Specialist+(m%2ff)&redirect=http%3a%2f%2fjobsearch.direct.gov.uk%2fhome.aspx&pp=25&pg=1&sort=rv.dt.di&re=134&q=Cyber+Security&AVSDM=2018-01-25T01%3a33%3a00-05%3a00) [Accessed 19 Jan. 2018].

Job Search. (2018). NHS Jobs IT Security Officer. [online] Available at: <https://jobsearch.direct.gov.uk/GetJob.aspx?JobID=45202790&JobTitle=IT+Security+Officer&redirect=http%3a%2f%2fjobsearch.direct.gov.uk%2fhome.aspx&pp=25&pg=1&sort=rv.dt.di&re=134&q=Cyber+Security&AVSDM=2018-01-26T03%3a33%3a00-05%3a00> [Accessed 19 Jan. 2018].

Ruddy, W. (2015). Do You Need Programming Skills for a Cyber Security Career?. [online] Phoenixts. Available at: <https://phoenixts.com/blog/do-you-need-programming-skills-for-a-cyber-security-career/> [Accessed 19 Jan. 2018].

Singh, A. (2013). Network Security: How much programming knowledge do you need to know to work as an infosec professional?. [online] Quora. Available at: <https://www.quora.com/Network-Security-How-much-programming-knowledge-do-you-need-to-know-to-work-as-an-infosec-professional?share=1> [Accessed 19 Jan. 2018].