Reflection

## Github Link: https://arashid99.github.io/e-portfolio/

Skills gained

By completing this module I achieved many skills in relation to Professional, Ethical, Legal, Social, Technical and Subject Application aspects. As for the professional skills I have gained , I am able to provide and express information to novice and expertise in the subject area, this can be proven through assignments, and discussion forums that I have completed. I also obtained skills in subject understanding which I previously did not have, as well as improved my critical thinking through completing tasks from the module. Additionally, I am more aware of the Ethical and Legal implications we need to consider as Cyber Security professionals, which I thoroughly enjoyed learning about such as the GDPR (GDPR.eu, 2021) and PCI DSS (PCI Quick Reference Guide, 2008), which we incorporated in our Unit 11 Assignment. Skills where I would like to improve myself are to participate in a professional organisation to gain commercial awareness and for the application of my knowledge.

These skills relate to all of the learning outcomes of the module particularly the fourth one.

For further details refer to the Professional Skills Matrix in the E-portfolio.

Team Work

As mentioned in the Professional Skills Matrix document, the social skills which I gained and improved were through the Team work in the module. We completed a project which had two parts Unit 6 and Unit 11, we were also asked to complete some seminar exercises together.

As for the team work we had regular meetings to discuss our thoughts and ideas. We planned everything thoroughly and decided to keep meeting notes and timeline of when we need to complete tasks and what our next steps are which showed our time management and organisational skills.

However, (Unit 11) did not run effectively as (Unit 6); Not every member of our group had the chance to showcase enough work due to certain members of the group feeling superior than others. Tasks to be completed were not fairly distributed as compared to the first assignment, and the tasks that I did complete were changed without me knowing. However, some members were more supportive than others from start of the module, explained new concepts and understood not everyone is on the same page of understanding and come from different educational and workplace backgrounds.

As for my individual contributions in meetings I noted that I was not contributing ideas enough, and rather was listening and respecting the ideas of others, so to improve myself I started to contribute ideas to the group more. Additionally, I attended meetings always prepared and demonstrated a cooperative and supportive attitude to my group members. Moreover, I tried my best to prepare all given tasks in a quality manner. On the other hand one aspect which I lacked in was not being confident enough to disagree with my peers’ opinion so in the future If I have a problem or an issue with an idea or a member I hope I am able to express myself clearly.

Legal, social, ethical and professional issues faced by information security professionals

As for the legal issues faced by Information security professionals, they need to ensure that the organisations are following the security standards such as PCI DSS, and GDPR as learnt in this module. Without following the standards it can lead to social and ethical issues as studied in the Case study in the discussion forum three, where a third party was informed of personal information of a lady as they were not compliant with the GDPR of keeping information up-to date and accurate which lead to a further noncompliance of the GDPR act 6. As mentioned in the Seminar exercises, where it is explained in an article of the data breach on Yahoo that caused a breach of 3 billion user account data which is a huge ethical and social issue. (Swinhoe, 2020).

However, the issue for organisations trying to be compliant with the GDPR is that it will cause financial loss, data shows that an organisation with around 500 employees would need to spend around 3 billion dollars in order to comply with the GDPR (Layton, 2019). This is a huge amount of money and can be an issue for small-medium organisations, however on the other hand for organisations that are global such as Facebook the cost would not affect them a lot as their networth is 528 billion dollars (Facebook Net Worth, 2021).

Nevertheless, Information security professionals need to ensure that organisations which deal with sensitive data comply with security standards such as GDPR otherwise if a data breach occurs it will cause major problems such as Garg et al (2003) analysed; a loss of reputation, losing customers, and a loss of stock market of 9.3 percent up to 14.9 percent in only 3 days of the data breach being announced. Although this study was carried out in 2003, it shows as a proof if more than 10 years ago this was the result of a data breach, then certainly the effects of it is much higher now.

It is required for information security professional to inform the organisations’ customers of the data breach for example to inform them if they need to change their password. However, a research conducted by Ponemon Institute LLC, (2012), found that over 36% of customers considered their breach notice letter to be junk mail, while 13% considered their breach notification email to be spam. This shows that customers do not pay attention to breach notifications. So, the question arises what should the information security professionals do in this case? What steps should be taken so that the customers are aware that their data is at risk? If the customer themselves do not take responsibility in changing their password whose fault will this be, the organisation/information security professionals’ or the customers?

Conclusion

Overall, the Network and Information Security Management System module was a enjoyable learning experience, I plan to improve myself in aspects where I lacked however, I also did gain many skills and knowledge which I will take onto the next modules.

References

Celebrity Net Worth. (2021). *Facebook Net Worth*. [online] Available at: <https://www.celebritynetworth.com/richest-businessmen/companies/facebook-net-worth/> [Accessed 23 July 2021].

Garg, A., Curtis, J. and Halper, H., (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, 11(2), pp.74-83.

GDPR.eu (2021). *What is GDPR, the EU’s new data protection law? - GDPR.eu*. [online] Available at: <https://gdpr.eu/what-is-gdpr/> [Accessed 18 July 2021].

Layton, R., (2019). *The 10 Problems of the GDPR*. [PDF] American Enterprise Institute. Available at:

My-course.co.uk (2021). *The Virtual Learning Environment: Log in to the site*. [online] Available at: <https://www.my-course.co.uk/course/view.php?id=6757&section=0> [Accessed 22 July 2021].

*PCI Quick Reference Guide* (2008) [PDF] PCI Security Standards Council. Available at: <https://www.pcisecuritystandards.org/pdfs/pci\_ssc\_quick\_guide.pdf> [Accessed 19 July 2021].

Ponemon Institute LLC, (2012). *Consumer Study on Data Breach Notification*. [PDF]. Available at: <https://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf> [Accessed 22 July 2021].

Swinhoe, D., 2020. The 15 Biggest Data Breaches Of The 21St Century. [online] CSO Online.