Information Security Management Reflection

What?

To guide this reflection, I've followed the What? So What? Now What? Model, which encourages looking back, making sense of the experience, and thinking ahead (McLeod, 2024). I've also captured my journey in my e-portfolio, which serves as evidence of my progress and development. The Information Security Management module, my sixth at the University of Essex Online, really shifted how I think about organisational security. Looking back, it challenged me in ways I didn't expect, especially after a difficult time in the previous Network Security module. There was some overlap between the two, which made me feel a bit apprehensive at the start. I wasn't sure if I'd face the same struggles again.

I reviewed the final summative assessments during Unit 1 and noticed that the last unit, Unit 6, would involve building a Python application. I hadn't touched Python since Module 4 (Software Engineering Project Management), and I genuinely felt like I'd forgotten most of it. It had been a while since I'd done anything technical. I spent a lot of time in the early units just trying to get my head around what was expected and how the pieces connected. But at the same time, I saw it as a chance to rebuild my confidence and push myself back into more hands-on work.

So What?

Once I got over the initial hesitation, I decided to just go with the flow. I made a conscious effort to stay on track, I watched the lecturecasts regularly, completed the unit activities, participated in the forum discussion, and caught up on the seminar recordings. That steady engagement paid off. By the time I reached Unit 3, I felt much more confident tackling the first summative assessment, which involved writing a risk identification report for a small business. I found the threat modelling techniques I explored in Unit 2 particularly helpful here. My exploration gave me a structured way of thinking through potential vulnerabilities and helped me approach the assessment with a more analytical mindset.

Interestingly, it was only after completing the Unit 3 assessment that the final technical assessment in Unit 6 began to make sense. Before that, it had felt disconnected, but now I had the context. I could see how the technical elements were built on the risk concepts I had already explored. That clarity sparked my interest, and I ended up starting the technical work quite early, around Unit 4. For this assessment, we had to create an attack tree visualisation.

I hadn’t worked with Python in a while, and many of the libraries, like networkx and graphviz, were completely new to me. Rendering the tree in the terminal would have been the simpler option, and I kept that as a fallback just in case. But I was keen to challenge myself, so I dug into online documentation and tutorials to get the hang of it.

Despite starting early, I ended up spending far more time than I expected. Most of the actual coding didn't happen until Unit 6.

Now What?

Looking back, I wish there had been more engagement in the forum discussions. There was only one forum discussion, and unfortunately, only two of us, Hamdan Almheiri and I, participated. I had hoped for more interaction from peers, as exchanging ideas and viewpoints often helps deepen understanding. I suspect the limited engagement might have been down to the small number of students enrolled in this module compared to others. Still, it would've been great to have more perspectives shared.

One thing I've realised while writing this reflection is that I probably spent too much time on the Unit 6 technical assessment. I tend to follow an iterative approach in my work as a software engineer: start small, build gradually, and refine. But for some reason, I didn't apply that mindset here. I kept researching and exploring until the final unit instead of getting stuck earlier. In hindsight, if I'd started the coding in Unit 4 and built it up week by week, I could've managed my time better and reduced the last-minute rush. It's a good reminder for future modules: trust the process and apply what already works for me. I'll take a more agile approach going forward.

As for applying what I've learned to my professional role, well, that's still a bit uncertain. In my current work environment, I haven't yet come across anyone explicitly using threat modelling frameworks like the ones I studied. It's possible that security is handled

differently, or by a separate team altogether. Still, just knowing these approaches exist has broadened my understanding. Even if I don't use them directly, I now have a much stronger grasp of the principles behind secure design and risk awareness. The technical takeaway is also significant; getting hands-on with Python again and learning new libraries was rewarding. I wouldn't have picked those up on my own, so that in itself feels like a win.

References

McLeod, S. (2024) *What? So What? Now What? Critical Reflection Model*. Available at: https://www.simplypsychology.org/what-so-what-now-what.html (Accessed: 19 July 2025).