**Security Risk Management**

**Individual Reflective Piece**

**By**

**Nkosana Mlambo**

[**https://nkosanamlambo.github.io/e-Portfolio/Module2.html**](https://nkosanamlambo.github.io/e-Portfolio/Module2.html)

‘It is not sufficient to have an experience in order to learn. Without reflecting on this experience, it may quickly be forgotten, or its learning potential lost.’ (Gibbs, 1988).

# **Security and Risk Management process**

The Security Risk Management (SRM) module has been quite an interesting journey throughout, it has brought a lot of insight and perspective when it comes to risks.

In this module, I have learned a lot of concepts with regards to SRM and there was a lot of reading to do. We had interesting discussions with my peers which included industry 4.0 and the risks that it presents, and these gave a lot of insight into Industry 4.0 risks, and how they can be tackled and the methods to use, e.g., RADi (Risk assessment for Digitalisation). Another interesting discussion was that of using a Common Vulnerability Scoring System (CVSS) and if it’s still relevant. There were quite interesting arguments pertaining to it and if it should be replaced. We also had interesting topics covered on our seminars and had interesting knowledge touching on security standards, threat modelling exercises, quantitative and qualitative risk modelling, Disaster Recovery (DR) solutions, and the future of SRM.

# **Individual Contributions and Team Activities**

# Part of the exciting tasks that were assigned to us as a team was to develop a risk identification report for a business transforming its operating model from a Bricks and Mortar Company to a Digital e-commerce business, we were tasked to formulate a risk assessment report, a threat modelling exercise, and recommendations and mitigation initiatives for the business.

This exercise was quite exiting and enjoyable in the process, as we tackled this report from a real-life problem perspective and scenario. Our team held weekly meetings to complete the report, and all agreed on tasks assigned to each individual team member and agreed deadlines in order to submit the assignment on time.

Part of my Individual contribution in the group included creating a WhatsApp group to use a communication platform that pertains to the assignment should we need to contact each other urgently and for short communications. In the Risk Identification report, I compiled a template/format for the assignment in which we all agreed on, and in order for us to be in sync and for the assignment to have a proper structure. Another task I was tasked with is the enumeration and risks that were faced by the business and the mitigation steps as well.

Other team activities that we worked together on included a second assignment, whereby we were tasked with developing a business executive summary for the business, formulating quality and supply chain risks and mitigation actions, using a quantitative risk modelling approach, and providing a Disaster Recover strategy. This assignment did bring challenges to the team, as we were somehow indecisive on which quantitative modelling approach we should use. We finally decided to use a 5x5 risk matrix as it was easy to use, concise and easily interpretable, as we were contemplating on using a monte Carlo simulation, but we decided that it was a bit complex and could take up too much time if we used that approach.

Part of my individual contributions was drafting the format of the report, drafting the introduction of the report, and compiling the list of quality risks and mitigation strategies. Other initiatives I undertook was to quality check the report once it was completed and submitting it. I have also assisted the team on attending seminars in order to acquire a better understanding on the report requirements, as some team members were unable to attend due to work commitments they had.

A final team exercise that we undertook was a presentation that we prepared for the last Seminar, entitled the great debate, the future of Security Risk Management. Were we compiled a presentation listing trends on Security risk, and we chose Artificial Intelligence and Machine Learning as a future trend. We all compiled the presentation and requested one of our team members to present it on our behalf at the last seminar.

The team worked well together, and the communication was very effective. The only issues we have was that we were at different time zones, and unfortunately the team could not always meet but we worked well around that as we communication through WhatsApp and always knew what was expected of us and by when.

# **Experiences**

Challenges on the module was perhaps an information overload with the amount of required reading to go through, as a working professional with competing priorities, it can be at times overwhelming and almost impossible to go through all the required reading and the formative tasks that are assigned in the module. Another challenge in the module was the word count limit given for each assignment which at first, I believed was a bit narrow to get your points across, but it has been a learning curve to help express views across in the most succinct way possible and eliminating unnecessary information.

# **Impact on Development**

As a Cyber Security manager and having to manage security risks at my workplace and a chair of vulnerability and risk remediation committee. This module proves to be amicably valuable in my development. Some of the Key knowledge areas that will help me make better decisions and change how I can sometimes do things for the betterment of providing sound knowledge on security risks include:

* Risk Management Processes and concepts
* Risk assessments and threat modelling techniques
* Disaster Recovery and Business Continuity strategies
* Risk Management standards and their importance and effects.

# **References**

Gibbs, G. (1988*) Learning by doing: a guide to teaching and learning methods*. Oxford: Further Education Unit, Oxford Polytechnic