Self reflections on Security and Risk Management (SRM) Module.

Introduction:

This is a very comprehensive module that started with introduction of security risk management (SRM), user assessment and risk management, introduction and application of threat modelling techniques to industry standards governing the security risk, concept of Qualitative and Quantitative Risk Modelling, Business Continuity (BC) and Disaster Recovery (DR) plans and Debate on Future Trend of SRM. We had two projects using the qualitative methodology for security risk assessment and Business Impact Assessment for Pampered Pet (PP) enterprise with business model change to digitalization objective and a quantitative methodology using Monte Carlo Simulation to analyse risk management technique in the digitalization project of PP.

SRM is the process of identifying, assessing, and implementing plans to address the security risk to acceptable level and the risk is determined by the extent of potential threat, vulnerabilities, and the impact on valuable assets. The module taught me that SRM involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process (Stoneburner et al, 2002) and a regular evaluation, assessment, and review of SRM is crucial to survival of a business.

I got to understand that distinguishing threat and vulnerability is important in knowing the appropriate control measures to adopt. A vulnerability is flaw in code or design that creates a potential point of security compromise for an end or network, meaning that vulnerabilities create possible attack vectors (Tech-Target). While threat is any event with the potential to adversely impact organizational's operations, assets through unauthorized access, destruction, disclosure, modification of information, or denial of service (NIST SP 1800-15B).

Qualitative and Quantitative risk assessment methodology were explained with major difference being that qualitative uses less data while quantitative uses mathematics concept.

Threat Modelling frameworks assess security risk of an organisation and the techniques include STRIDE and DREAD, Attack Trees, PASTA, OWASP, CVSS, OCTAVE etc .The general step requires in threat Modelling are (Lecture-cast unit 3):

1. Asset identification (Web-site, Applications, Database, Employées).
2. Create an architecture overview of the system (dataflow, external factors & Boundaries etc).
3. Decompose the application (identify the vulnerabilities points).
4. Identification of Threat (using risk assessment frameworks like STRIDE).
5. Documentation of identified vulnerabilities and threats
6. Rate the Threats (Using DREAD assessment framework).
7. Implementation of countermeasures
8. Document Review

9. Communicate to end-users.
10. Revalidation

The above frameworks are mainly for qualitative methodology of risk assessment while the quantitative risk assessment method include Monte Carlo Simulation Analysis, Bayes' Theorem, and Multi-Criteria Decision Analysis.

During the module, we reviewed vendor lock-in concept and its impact on adoption of cloud computing by Opara-Martins et al (2014) and Morrow et al (2021). Cloud computing being delivery of computing services like servers, storage, databases, networking, software etc to facilitates innovation, flexible resources and economies of scale (Ranger.S,2022). Despite benefit of cloud computing services, organizations are slow in adapting the cloud servicing model due to the associated vendor lock-in challenges. Vendor lock-in is a situation where a customer cannot easily transit to cloud services of competitors (Hanna.k,2023).

The major challenge limiting the customer's choice of switching to other providers because of vendor lock-in issues are around integration complexity, configuration & customization, data and format locking .A further classified is lack of interoperability and portability where vendor uses licensed software application under exclusive condition to lock-in clients and lack of Standardization to address workload migration and data migration format which makes it difficult for data portability and interoperability.

The mitigation could be option of multi-cloud or hybrid strategy, Providers implementing standard-based solutions, reviewing Service Level Agreement (SLA) and confirm Data portability policy which is important factor in signing-on vendors.

In optimizing the benefit of digitalization based on decision outcome from Business Impact Analysis (BIA), SRM, cost effectiveness and efficiency in use cloud providers, it's important to ensure continuity of the business which is achieved by implementing BC and DR strategies. This is in-line with ISO 22301 recommendation of risk assessment, BIA creation of BC and DR strategies of a business. `

BC is the readiness to maintain critical function of an organization process after an emergency or disruption e.g. security breaches, natural disaster, equipment failures and sudden departure of employee (VmWare) while DR is a subset of a BC plan that deals with availability of IT infrastructure that supports the business and staff. DR targets are measured by Recovery Point Objective (RPO) and Recovery Time Objective (RTO) where RTO determines the maximum amount of time that passes before a system is disaster recovered, the RPO is the maximum amount of time acceptable for data loss after a disaster. The shorter RPO & RTO the more expensive the solution.

Summary of DR solutions

S/N	**DR Solution**	**DR Objective**
1	**Active -Active**	**RTO < 1hr : RPO < 1min**
2	**Cold Standy**	**RTO>12hrs : RPO>1hr**

3	**Backup Restore**	**RTO>48hrs : RPO>24hrs**
4	**Active -Passive**	**RTO>1hr : RPO>15mins**

The industry standards and regulatory governing any business module were also discussed examples; General Data Protection Regulation, Payment Card Industry - Data Security Standard for cards providers, International Organization for Standardization (ISO) 27000,27002 ,31000 for Information Security Management System, NIST 8000181 and SRM regulatory compliance. Understanding and implementing the standards are important to avoid penalties for non-compliance and loyalty and trusted secured system.

During the group's projects, I handled the pre-digitalization business assessment of Pampered pet where qualitative risk assessment methodology and BIA was applied while the second project on quantitative risk assessment, the BC & DR aspect of the project inclusive of DR solution design were assigned to me.

Working on the project rekindled my critical thinking and analysis skills while I also learnt to collaborate with the team produce quality output. It is also important to participate in all units' activities because it gives one a better understanding of the module to deliver on any project task.

The overall units of the module are useful and would assist me in understand the expected security risk management of a business project management especially the use monte carlo simulation technique for various managerial business decision .

.

References:

- Hanna.k,(2023).TechTarget. vendor lock-in. Available from: https://www.techtarget.com/searchdatacenter/definition/vendor-lock-in# [Accessed 30 October 2023].
- Morrow. el at (2021), Carnegie Mellon University Software Engineering Institute, Cloud Security Best Practices Derived from Mission Thread Analysis.Available from: https://apps.dtic.mil/sti/pdfs/AD1139951.pdf[Accessed 08 October 2023].
-
- Open Risk Manuel. Quantitative Risk Model. Available from : https://www.openriskmanual.org/wiki/Quantitative_Risk_Model#:[accessed [Accessed 21 September 2023].
- Opera-Martins et al (2014). International Conference on Information Society (i-Society 2014) Critical Review of Vendor Lock-in and Its Impact on Adoption of Cloud Computing.Available from:https://eprints.bournemouth.ac.uk/22467/1/Critical%20Review%20of%20Vendor%20Lock-in%20and%20Its%20Impact%20on%20Adoption%20of%20Cloud%20Computing.pdf [Accessed 04 October 2023]

- 08 October 2023].
- Ranger.S, (2022).Zdnet Innovation.What is cloud computing? Everything you need to know about the cloud explained. Available from: https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/ssed [Accessed 30 October 2023]

.