Julius Cloos
Module: Security and Risk Management
Tutor: Dr. Siddiqui
E-Portfolio: https://juliusneweportfoliouser.github.io/uoeoeportfolio/index.html

Reflective Piece

This reflective piece will follow the outline described by Rolfe et. al (2001). First, I will outline what happened in the module (What?), then I will analyze these events (So What?) and finally, I will describe what I learned from these events (Now What?).

What?

The module "Security and Risk Management" (SRM) focused on:

- Terminology
- Risk Management Standards (such as Open FAIR and OCTAVE)
- Qualitative and quantitative risk assessment types and approaches (such as Monte-Carlo Simulations for quantitative risk assessment)
- Threat modeling techniques (STRIDE, DREAD, MITRE ATT&CK etc.)
- Regulatory aspects (GDPR, PCI-DSS)
- Standards such Cobit, ITIL
- Business continuity (BC) and disaster recovery (DR) plans
- Impact of RPO and RTO on DR plans
- Advantages/disadvantages of Disaster-recovery-as-a-Service (DRaaS)
- Future trends

For assessment, the module contained 3 assessments:

- A risk identification report
- Execute Summary
- E-Portfolio

Furthermore, there were several opportunities for students to engage in seminars, debates and discussion forums.

Unfortunately, I didn't participate in the units due to health-related issues that come up in early February. When I was in Costa Rica in November 2023, I had contracted a severe food poisoning which caused diarrhea over the course of 14 days (2/3 of the total time in Costa Rica). In January, I had gotten a salmonella infection. In February, I started getting random fever spikes which I was afraid were symptoms of a serious illness, as various online sources regarding normal and abnormal fever curves indicate. It turned out to be harmless (cortisone medication for 3 months fixed it), but I didn't know that until mid-April. During that time, I couldn't sleep or focus properly, and coursework was not my main priority.

Therefore, I am now re-submitting risk identification report, the executive summary and this reflective piece.

While this means that I don't have any collaboration in my assessments (specifically the risk identification report), I tried my best to obtain feedback about my views regarding Industry 4.0 and CVSS as I wrote a discussion forum post for the first and second discussions. Amrol Miah kindly provided me feedback, adding more detail regarding IoT and Stuxnet to my post in the first discussion forum, and more detail on CVSS 4.0 on my post in the second

discussion forum. I have since responded to Amrol's posts in my summary posts. Furthermore, I completed the GDPR case study. As for the assessments, Dr. Siddiqui thankfully took the time outside the weeks during which the module officially ran to provide me an overview of the requirements and ideas to get started, especially regarding the fact that I should look for an approach to combine STRIDE/DREAD.

So what?

Knowledge gained throughout the module can be applied to my job working at a Security Operations Center (SOC) for a company in Wiesbaden, Germany. For example, when analyzing systems to then design detections for attacks (and prioritizing new detections to be designed), the STRIDE/DREAD approach I used in the risk identification report will be useful. This is due to my methodology of using MITRE ATT&CK coverage, finding areas which are not covered by our current detections and then seeing if I can design a detection to increase the coverage of our SOC's detections. Without a clear guide on how to prioritize these new detections, I usually end up picking a MITRE technique not yet covered based solely on my own subjective understanding of the problem and the infrastructure in which my detection will be used. With the approach from Dykstra et. al. (2023), I have a more objective way of identifying necessary detections. While the approach is inherently subjective due to how the values for DREAD are assigned, it's still more of a scientific approach than what I used before.

Also, my increased knowledge on GDPR will come in handy as it's an important part of the IT-field given the hefty fines one can incur when failing to comply with the regulations (InCountry, 2024).

Given one of my hobbies that I'm doing on the side is investing, Monte-Carlo Simulations will perhaps be useful, although I am not claiming I fully understand them. Many examples of Monte-Carlo Simulations I came across during my research involved stock market simulations as examples, such as Kenton (2024) and various papers, for example He (2022).

Although my work isn't focused on Risk Management, ideas from standards such as OCTAVE do apply, specifically the importance of user involvement (Gunawan, 2011). From my own experience, projects can go wrong quickly when the end users aren't involved enough in the process.

Now what?

Given I have limited experiences with mathematical concepts, the Monte-Carlo Simulation has been difficult for me. However, I believe I eventually understood the concept of it. Therefore, this course helped me improve my mathematical skills. Also, my knowledge on Microsoft Excel deepened, thanks to tutorials such as Chiddarwar (2020).

Especially the stress in the final 2 weeks of the resubmission period could have been avoided with better time management skills. I will need to continue to improve on these skills in the future.

During the next modules, I will need to work on my team working skills, as I didn't get any team working experience during this module. Especially in cyber security, collaboration is

important given organizations (and therefore people) need to work together to combat cyber attacks (Acris et. al., 2023).

In the coming weeks, I plan on looking more into cloud security, as this is a topic that I have no real experience in (compared to other security-related topics where I do have at least some limited practical experience, such as network security and web application security). According to Mordor Intelligence (2024), cloud computing is expected to grow significantly in the coming years. This means knowledge on cloud security will become even more sought-after. The research into the technical aspects of Azure Site Recovery (despite me not including it as a part of the executive summary due to word count constraints), provided insights into this topic.

Speaking of word counts, I would have liked to include more ideas for mitigations in the risk identification report. It's obvious that most security risks plaguing companies are not fixed by the simple mitigations I provided. While I ended up focusing mostly on the executive summary after Dr. Siddiqui provided me positive feedback on the risk identification report, I believe that I delivered solid pieces of work in all the assessments, my discussion forum posts and the GDPR case study.

Julius Cloos
Module: Security and Risk Management
Tutor: Dr. Siddiqui

References

Acris, J., Atherton, L., Clark, P., Crooks, D., Cutrina, P., Jordan, D., McKee, S., Vâlsan, L. (2023) 'Collaborative Operational Security: The future of Cybersecurity for Research and Education', 26th *International Conference on Computing in High Energy and Nuclear Physics (CHEP 2023).* Norfolk, United States of America, 8-12 May.

Chiddarwar, K. (2020) Monte Carlo Technique: How to perform Business Simulations & Assess Projects Profitability | Excel. Available from: https://www.youtube.com/watch?v=gGE6pByReAc [Accessed 29 July 2024].

Dykstra, J., Lander, T. E., Mittal, S., Rastogi, N., Reece, M., Sampson, A. & Stoffolano, M. (2023) Systemic Risk and Vulnerability Analysis of Multi-cloud Environments. Available from: https://arxiv.org/pdf/2306.01862 [Accessed 01 August 2024]

Gunawan, B., Merry, M., Nelly, N. (2011) Information Technology Risk Assessment: Octave-S Approach. *CommIT Journal* 5(1): 1-4. DOI: https://doi.org/10.21512/commit.v5i1.549

He (2022) Sensitivity estimation of conditional value at risk using randomized quasi-Monte Carlo. *European Journal of Operational Research* 298(1): 229-242. DOI: https://doi.org/10.1016/j.ejor.2021.11.013

InCountry (2024) Navigating GDPR data sovereignty requirements. Available from: https://incountry.com/blog/navigating-gdpr-data-sovereignty-requirements/ [Accessed 28 July 2024].

Kenton, W. (2024) Monte Carlo Simulation: What It Is, How It Works, History, 4 Key Steps. Available from: https://www.investopedia.com/terms/m/montecarlosimulation.asp [Accessed 01 August 2024].

Mordor Intelligence (2024) Cloud Computing Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029). Available from: https://www.mordorintelligence.com/industry-reports/cloud-computing-market [Accessed 02 August 2024].

Rolfe, G., Freshwater, D. & Jasper, M. (2001). *Critical reflection in nursing and the helping professions: a user's guide.* Basingstoke: Palgrave Macmillan.