Task ‘Security and Risk Management’ Unit 7

Collaborative Learning Discussion 2 – Summary

The discussion around the topic of Common Vulnerability Scoring System CVSS highlighted a noteworthy challenge consistency and practical utility. CVSS scores often lack inter-rater reliability, with evaluators frequently assigning divergent values to core metrics for instance, attack vector, scope, and user Interaction.
(Wunder et al. 2024)

In my initial post, I acknowledged few of these limitations to some degree, stating that although CVSS aims to facilitate vulnerability prioritization, its scores are often misinterpreted and used as direct risk indicators despite explicit guidance against such practice.
(Spring et al., 2021).

Peer contributions enriched the discussion by exploring alternative and complementary approaches. some had highlighted, again, the point the Exploit Prediction Scoring System (EPSS), which uses empirical, data-driven modeling to estimate the likelihood of exploitation and unlike CVSS, EPSS outputs probabilistic scores suitable for dynamic risk analyses.
(Jacobs et al., 2023)

Some comments have rightly emphasized that effective risk management would require integrating CVSS with contextual asset and business information to guide mitigation strategies meaningfully, demonstrating that hybrid approaches may be required in order to provide a more comprehensive risk assessment
(Hughes, Robinson, 2024).

The discussion reinforced several key insights. First, the Common Vulnerability Scoring System (CVSS) has value as a descriptive and preliminary assessment tool; however, it should not be used in isolation for decision-making, particularly in cases where risk practitioners rely only on their own expertise and contextual judgment.
(Thekdi et al., 2025).

In addition, hybrid approaches could help mitigate CVSS limitations by incorporating real-world exploitability and contextual factors. Risk can only benefit from effective characterization and adoption of hybrid risk methods, reflecting uncertainty and knowledge gaps which can be common in subjective security assessments.

In summary, this interaction had enhanced my knowledge about vulnerability assessment methods, underscoring the significance of supplementing from different sources of empirical data and contextual judgment. This exchange also reinforced the notion that a well-informed and integrated approach could

yield better more actionable outcomes, demonstrating the value of collaborative discussion.

References

- Hughes, C. & Robinson, N. (2024) Effective Vulnerability Management : Managing Risk in the Vulnerable Digital Ecosystem. 1st ed. Newark: John Wiley & Sons, Incorporated.

- Jacobs, J. et al. (2023) Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights. arXiv.org. Available at: https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_proquest_journals_2781017466 [Accessed 18 December 2025]
- Spring, J., Hatleback, E., Householder, A., Manion, A. and Shick, D., (2021). Time to Change the CVSS? IEEE Security & Privacy, 19(2), pp.74-78

- Thekdi, S. & Aven, T. (2025) Evaluating risk analyst views on uncertainty and knowledge aspects for risk characterization approaches. Journal of risk research. [Online] 28 (8), 912–928. Available at: https://**********.com/permalink/44UOES_INST/o3t9un/cdi_informaworld_taylorfrancis_310_1080_13669877_2025_2553847 [Accessed 18 December 2025]

- Wunder, J. et al. (2024) Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities. arXiv.org. Available at: https://**********.com/permalink/44UOES_INST/o3t9un/cdi_proquest_journals_2858809873 [Accessed 18 December 2025]