Initial Post:

Vulnerability assessment frameworks underpin modern cyber-risk management, yet their effectiveness depends on contextual adaptability and decision relevance. Spring et al. (2021) critique the Common Vulnerability Scoring System (CVSS) for its lack of contextualisation, arguing that the metric's linear scoring model oversimplifies complex interdependencies. I find this critique persuasive because CVSS emphasises numerical precision while ignoring operational urgency, business impact, and threat actor intent.

Jacobs (2020) further notes that static severity scores can mislead practitioners into over- or under-prioritising vulnerabilities, resulting in inefficient resource allocation. By contrast, the Stakeholder-Specific Vulnerability Categorisation (SSVC) proposed by Spring et al. (2021) introduces a decision-tree model incorporating exploitability, exposure, and mission impact. This approach enables organisations to derive risk decisions aligned with their operational goals rather than adhering to universal scores.

Almohri and Yao (2021) support this transition toward dynamic, context-driven frameworks, emphasising automation and data analytics in prioritising remediation. Similarly, Alahmari and Duncan (2020) highlight that small and medium-sized enterprises benefit from flexible models that reflect real-time resource constraints. Sarker (2022) also links such adaptability to resilience in digital-transformation contexts.

In summary, replacing or complementing CVSS with SSVC fosters risk decisions that are defensible, auditable, and mission-aligned—ultimately enhancing cybersecurity resilience.

References

1. Alahmari, F. and Duncan, B. (2020) 'Cyber risk assessment for SMEs: A practical approach', *Information & Computer Security*, 28(3), pp. 345–361. doi: 10.1108/ICS-04-2019-0058.
2. Almohri, H.M.J. and Yao, D. (2021) 'Prioritising software vulnerabilities: From CVSS to data-driven risk analytics', *Computers & Security*, 108, 102351. doi: 10.1016/j.cose.2021.102351.
3. Jacobs, J. (2020) 'Metrics that mislead: Revisiting vulnerability scoring', *Journal of Cybersecurity Metrics*, 6(2), pp. 59–72. doi: 10.1093/cybsec/taa028.
4. Sarker, I.H. (2022) 'Cybersecurity data science: An overview from machine learning perspective', *Journal of Big Data*, 9(1), 13. doi: 10.1186/s40537-022-00584-5.

5. 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. doi: 10.1109/MSEC.2021.3051234.

Peer reply:

I completely agree with your evaluation of Spring et al. (2021) and the advantages of SSVC in aligning risk decisions with mission objectives. However, one potential limitation worth noting is scalability. Implementing SSVC requires significant contextual input and human judgment, which may restrict its adoption in large or resource-limited organisations (Hausken, 2022). While automation tools could streamline decision-tree mapping, Almohri and Yao (2021) highlight that automated systems still rely on accurate contextual data, which many enterprises lack.

Furthermore, since CVSS remains embedded in compliance frameworks such as NIST SP 800-53 and ISO 27001 risk registers, replacing it entirely could create compatibility gaps. A hybrid approach—using SSVC to complement CVSS scoring rather than replace it—may therefore be more feasible. This integration would allow practitioners to retain standardised benchmarking while achieving contextual precision.

References

1. Almohri, H.M.J. and Yao, D. (2021) ‘Prioritising software vulnerabilities: From CVSS to data-driven risk analytics’, Computers & Security, 108, 102351. doi: 10.1016/j.cose.2021.102351.

2. Hausken, K. (2022) ‘Challenges in vulnerability assessment and mitigation prioritisation’, Journal of Cyber Policy, 7(1), pp. 98–113. doi: 10.1080/23738871.2022.2025551.

3. 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. doi: 10.1109/MSEC.2021.3051234.