Common Vulnerability Scoring System (CVSS) Is a framework that allows individuals or organisations to score their security vulnerabilities. The metrics consist of three groups Base, Temporal and Environmental. The scores range from 0.0 and 10.0 - 10.0, being the most severe.

Spring et al. (Spring et al. 2021) criticise that the calculation is unjustified, and the formula is not transparent. They further suggest that the framework is not a one size fits all. For example, they refer to data loss as more critical than the loss of control, which again depends on the nature of the business and the requirements.

As an organisation you would want to protect all your assets, not just one. The CVSS framework is a good starting point, but I agree with the comments to some extent. As stated by the CVSS Implementation Guidance, There are limitations with the model, which only looks at the vulnerability of that particular system and not the impact downstream of the system. (Franklin et al. 2014)

Spring et al. also discuss several alternatives to CVSS. One is SSVC Stakeholder-Specific Vulnerability, which is more transparent and looks at different stakeholders. SSVC implements decision trees to display all the vulnerabilities and all the potential outcomes, which allows organisations to have a holistic approach. (Spring et al. 2019)

References:

Bacon,M (2020) CVSS (Common Vulnerability Scoring System) Available From: https://www.techtarget.com/searchsecurity/definition/CVSS-Common-Vulnerability-Scoring-System [Accessed 29 September 2022]

Franklin, J.et al (2014) CVSS Implementation Guidance Available from : https://nvlpubs.nist.gov/nistpubs/ir/2014/nist.ir.7946.pdf

Spring, J.et al (2021). Time to Change the CVSS? Available From: https://ieeexplore-ieee-org.uniessexlib.idm.oclc.org/document/9382369 [Accessed 29 September 2022].

Spring, J et all (2019). A STAKEHOLDER-SPECIFIC VULNERABILITY CATEGORIZATION Available From: https://resources.sei.cmu.edu/asset_files/WhitePaper/2019_019_001_636391.pdf [Accessed 29 September 2022].