

Wiki Entry: Risk Information Misrepresentation

Risk Information Misrepresentation discusses the problem of how risk information can be displayed without the influence of personal biases and prior knowledge. Furthermore, uncertainties have to be accurately represented and accounted for in a transparent way that properly justifies confidence in the results.

An example of how to do so would be the use of vulnerability databases such as the Common Vulnerabilities and Exposures database (CVE) maintained by Mitre, or the National Vulnerability Database (NVD) maintained by the American NIST. These databases are important resources that list publicly disclosed vulnerabilities and exposures. The CVE and the NVD are fully synchronized and contain the same list of vulnerabilities across both databases (Mitre, 2020). The vulnerabilities listed within contain a description of how the vulnerabilities can be exploited and have a CVSS score attached. The Common Vulnerability Scoring System (CVSS) is a system widely used in vulnerability management programs. CVSS indicates the severity of an information security vulnerability and is an integral component of many vulnerability scanning tools (Balbix, N.D.).

Having a reputable source confirm the existence and magnitude of an identified risk helps to prevent misrepresentation and justifies confidence. Furthermore, having a tangible score attached to highlighted risks helps communicate the severity of impact to the business in a way that management understands and can act upon.

Reference List

Balbix (N.D.) What are CVSS Scores. Available from:
<https://www.balbix.com/insights/understanding-cvss-scores/> [Accessed 5 March 2021].

Mitre (2020) CVE and NVD Relationship. Available from:
https://cve.mitre.org/about/cve_and_nvd_relationship.html [Accessed 5 March 2021].