Clarification w.r.t. information on data breach incidents reported in BRSR-2022

This clarification is made to a disclosure in the Business Responsibility and Sustainability Reporting (BRSR) section of our Annual Report 2021-22. The need for such a clarification arises because there was no definition provided as part BRSR guidance document as what qualifies as a data breach incident. Aligning to the general trend that is emerging in the sector of reporting only material and substantiated incidents, we are giving this clarification.

This clarification is related to the BRSR disclosure on Principle 9, Leadership Indicator number 5, reported in page 223 of our Annual Report 2021-22. (https://www.hcltech.com/sites/default/files/documents/investor-reports/AnnualReport2022.pdf)

===

In the Annual Report 2021-22, page 76, section 'Information and Cybersecurity Risks' entails the conclusion of all the incidents reported and investigated along with more information on our Cyber Security posture. We have not experienced any material data breaches that impacted HCL or any stakeholders.

The elucidation to page 223 - point 5: Provide the following information relating to data breaches:

a) The intent of information disclosure relating to data breaches in our latest annual report is not restricted to the number of incident(s) concluded as material breach but includes the entries received in our internal incident management portal via the employee self-service portal or automated IT incident reporting systems. These include the entries,

    - raised by employees or customers as prima facie or at the pretext of a potential data security related event anticipated or observed,
    - the cases raised by the automated IT system deployed to detect / prevent potential data loss events,
    - by others that required further analysis.

b) 158 such entries were received in our internal incident management portal via the employee self-service portal or automated IT incident reporting systems. All entries are treated as incidents until thoroughly investigated by our Cyber Incident Response Team (CIRT).

c) A comprehensive analysis was/is conducted to remediate any issues, identify information about trends, to remain vigilant for emerging issues, and to prioritize implementing preventive and proactive initiatives.

    The top key themes emerged from analysis of initial entries received in our incident system were related to - process deviations in data uploads to cloud storage; false positives and non-data loss related incidents; web app security related; use of external media or USB; GitHub Repository related; and email system usage. These incidents don't represent any incident which led to a material data breach.