Ethical Dilemma Response

Scenario: Ignoring a Junior Team Member's Report of a Breach

Issue Description: An IT support technician claims to have noticed abnormal access to the data, which may indicate a breach of internal data. Given that the supervisor is feeling the pressure of meeting the project's deadline, the temptation to delay action until more substantial evidence materializes is a possibility. Failing to address the report might compromise customer records and go against organizational standards and guidelines, and doing so hastily might end up causing panic and hindering the process of work.

Decision and Action: There is a need to act as soon as possible. This report should be officially recorded, and an initial triage into the investigation according to the incident response policy of the organization should be delivered. Although discretion is important, escalation to the Security Analyst at the right time is crucial so that verification with the corresponding expertise is initiated.

Ethical Principle: Fairness: In this judgement, fairness has been exercised so that each member of the team, irrespective of seniority, should have a voice and his/her struggles verified. Ethical leadership also demands that every employee is equally important in reporting potential threats, particularly in cases involving the organization's information (Al Halbusi et al., 2021).

Justification as a Leader: The desire to protect the integrity of data/organizational security is based on the principles of leadership methods. Tempo. If there is no instant copy answer, there is a risk of exposure, the internal culture of whistleblowing will also suffer, and it is an indicator that junior voices do not count. This undermines trust in teams and raises the long-term organizational risk.

Real-World Examples

Target had a serious data breach in 2013, where the personal data and payment card information of more than 41 million customers were compromised. The hack first occurred through phishing the third-party vendor, which allowed the hackers to install malware on the point-of-sale systems of Target (Wu & Zha, 2022). Even though the internal security tools identified an unusual operation, the supervisors overlooked the alerts raised by junior analysts, which delayed the response, thus exacerbating the breach. Equifax was the victim of a terrible hack in 2017 because its software engineers had failed to patch a known weakness in Apache Struts software. It was known to be a problem by the internal staff, and there were miscommunication and prioritization problems that needed to be addressed promptly. The result of this was that data regarding more than 140 million Americans, including Social Security numbers and information on credits, got compromised (Thiyagarajan et al., 2025). The event generated consumer backlash, executive dismissals, a government investigation, and a loss of reputation.

References

Al Halbusi, H., Williams, K. A., Ramayah, T., Aldieri, L., & Vinci, C. P. (2021). Linking ethical leadership and ethical climate to employees' ethical behavior: the moderating role of person–organization fit. *Personnel Review*, *50*(1), 159-185. https://www.emerald.com/insight/content/doi/10.1108/PR-09-2019-0522/full/html

Thiyagarajan, G., Bist, V., & Nayak, P. (2025). The Hidden Dangers of Outdated Software: A Cyber Security Perspective. *arXiv preprint arXiv:2505.13922*. https://arxiv.org/abs/2505.13922

Wu, J., & Zha, P. (2022). A data security model for altering data ecosystem and affirmatively prevent mass data breaches. https://osf.io/preprints/d479z/