WHEN HUMAN EYES STRAY FROM GLASS

SCENARIO:

A small company with a two-person IT team has not been using the purportedly automated cybersecurity solutions it had purchased nearly one year earlier. The lack of tuning and configuration of those solutions – and lack of 24/7 coverage on the attack environment – leaves the company vulnerable to malware that was executed on the company network nearly 10 months earlier.

BUSINESS IMPACT:

An unknown number of business records were exposed for months, since the average time to detect a data breach is 277 days. The company is forced to close for two days due to company-wide disruptions and concerns about a data breach.

- The company has an IT team and MSSP but there's no cohesion between the internal team and outsourced "experts."
- The incidents get logged but they're not discussed or remediated or correlated with related incidents.
- Each incident occurred in the early morning when neither IT director nor MSSP have "eyes on glass."
- The IT team – inundated with network and desktop responsibilities – was not reviewing the solutions, nor optimizing the technology the company had invested in.