Does Cyber Crucible have an incident response and breach-notification process?

Short answer: Yes. A documented data-breach response process defines the roles and steps for responding to a suspected theft, breach, or exposure of protected data, including customer notification. A committed notification timeframe can be set by contract for regulated customers.

The response process

A suspected incident is reported immediately through internal channels monitored by the Information Security function. On identification, access to the affected resource is removed and an incident response team chaired by executive management is convened. Forensic investigators and experts, provided through Cyber Crucible's cyber and technology insurance, determine how the incident occurred, the data involved, the parties affected, and the root cause. A communication plan is developed with Legal, Communications, and Human Resources to notify staff, the public, and affected parties as appropriate — including customer notification through a mutually agreed channel — followed by a post-incident review.

Support response and notification

Customer-facing incidents are tracked against the published SLA severity tiers (SEV1 through SEV4), and a breach or incident notification timeframe can be committed contractually for regulated customers.

Framework alignment and the honest boundary

The process aligns to NIST SP 800-61 and ISO/IEC 27001:2022 A.5.24–A.5.26. No certification is claimed. The full incident-response and breach-notification procedure is provided to reviewers under NDA.

Revision #1
Created 2026-07-24 23:08:43 UTC by Dennis Underwood
Updated 2026-07-24 23:08:43 UTC by Dennis Underwood