No Access Checklist

A secure software development checklist helps developers build more resilient systems against rising cyber threats as data breaches rise in cost and frequency.

STEP 1

Detection and Analysis

- [ ] Implement intrusion detection systems and monitor networks closely for potential breaches.
- [ ] Thoroughly investigate any anomalies and analyse log files to determine where, when, and how a breach may have occurred.
- [ ] Identify the types of data impacted and how many individuals may be affected.

STEP 2

Containment

- [ ] Isolate affected systems immediately and shut down access to block any further data loss.
- [ ] Remove compromised files or devices.
- [ ] Promptly reset passwords, encryption keys, API tokens, and other credentials.

STEP 3

Notification

- [ ] Transparently alert all individuals whose personal information may have been compromised, according to regulatory guidelines.
- [ ] Contact the appropriate legal authorities and partners that may be impacted.

STEP 4

Investigation

- [ ] Form an incident response team to thoroughly document the details of the breach and follow established procedures to determine the root cause.
- [ ] Secure evidence, logs, and system images for forensic analysis by internal staff or third-party experts.

STEP 5

Recovery

- [ ] After a root cause analysis, work diligently to restore and secure affected systems and data to their original state before the breach.
- [ ] Extensively test security before bringing systems back online.

STEP 6

Post-breach evaluation

- [ ] Conduct a breach debrief to closely assess your internal response and identify areas for improvement in policies, procedures, and systems.
- [ ] Implement changes to shore up vulnerabilities and prevent similar future data breaches.