FREE KIT · FOR FOUNDERS & TECH LEADS · 2026

Be breach-ready.

A security review checklist plus a 1-page incident response plan you can fill in today.

> **The wake-up call:** in October 2026, Binance said about **$6.3B** in assets was affected by a security incident. Blockchain analysts reported most of it left in **roughly 20 minutes**, after **36+ hours** of attacker preparation. Binance's first investigation pointed to a compromised engineer's laptop, and it later reported "additional points of breach." About $3B has been frozen so far. If a top exchange can be hit like this, any business that runs on software can.

Inside:

① Security review checklist: the 4 takeaways, turned into tasks
② 1-page incident response plan: who does what in the first 60 minutes
③ The questions to answer before you ever need them



Afeez Badmos
Principal Technical Lead · Global McLien Software Solutions

Incident figures are as reported in October 2026 (Binance; TRM Labs via Forbes and The Hacker News; Decrypt) and may change as the investigation continues. General guidance, not legal advice.

1 · Infrastructure gets continuous attention MONTHLY

- [ ] **Asset inventory:** every server, cloud account, domain, API key and third-party service has a named owner.
- [ ] **Patching cadence:** OS, runtime and container images are updated on a schedule, with critical fixes applied within days, not quarters.
- [ ] **Alerts that reach a human:** unusual logins, privilege changes, large outflows or exports, and new admin keys trigger a page, not just a log line.
- [ ] **MFA everywhere admin access exists:** cloud consoles, code host, CI/CD, DNS registrar and payment dashboards.

2 · Your codebase gets regular reviews EVERY RELEASE

- [ ] **Outdated dependencies:** turn on automated dependency alerts (e.g. Dependabot or `npm audit` in CI) and act on high/critical findings.
- [ ] **Exposed credentials:** run secret scanning on every repo and its history, keep secrets in a vault or env store (never in code), and rotate anything that has ever leaked.
- [ ] **Weak access controls:** review every quarter who and what can deploy, read production data or move money. Apply least privilege to people *and* service accounts.
- [ ] **Overlooked vulnerabilities:** do a security-focused code review on auth, payments and file upload, plus an external test before major launches.

3 · Your team is part of the strategy ONGOING

- [ ] **A no-blame channel to raise concerns:** "this key has too much access" should get a thank-you, not a debate.
- [ ] **Engineer devices are part of the attack surface:** device encryption, endpoint protection, screen lock and MFA, with no long-lived production secrets stored on laptops.
- [ ] **Phishing and social-engineering awareness** for anyone with production or financial access, refreshed at least yearly.

4 · Response plan: the kicker PAGE 3

Detecting a breach matters, but containing it fast is what limits the damage. Fill in the 1-page plan on the next page, print it, and run a 30-minute tabletop drill with your team this quarter.

Score yourself: 10–11 ✓ solid · 7–9 ✓ fix the gaps this month · under 7 ✓ book a review before your next launch.

Who's who FILL IN

Incident lead (decides):

Backup lead:

Technical lead (contains):

Comms lead (customers, staff):

Legal counsel / insurer:

Hosting / cloud support line:

Detect & confirm 0–15 MIN

- Confirm it's real: what was seen, where, and when? Open an incident log (time-stamped notes).
- Name the incident lead. Start a private war-room channel and keep it off any system that may be compromised.

Contain 15–60 MIN

- Revoke and rotate exposed keys, tokens and passwords. Disable compromised accounts and devices.
- Isolate affected systems, and pause risky operations (payouts, withdrawals, deploys, data exports) if needed.
- Preserve evidence: snapshot logs and disks *before* wiping anything.

Notify SAME DAY

- Brief legal counsel and your cyber insurer early. Notification deadlines vary by law and contract (for example, GDPR expects the regulator to be told within 72 hours of becoming aware of a personal-data breach, where it applies).
- Tell customers what happened, what you're doing, and what they should do. Keep it factual and avoid guessing.

Recover & learn DAYS 1–7

- Restore from known-good builds and backups, monitor closely for a return, and only then reopen paused operations.
- Hold a blameless review within a week: root cause, what slowed you down, and 3 fixes with owners and dates.

FIND THE WEAKNESSES BEFORE THEY'RE EXPENSIVE

Get an infrastructure + codebase security review.

Global McLien Software Solutions reviews web apps, mobile apps, SaaS platforms and cloud infrastructure, then helps you fix what it finds and write your response plan.

globalmcliensoftwaresolutions.com →

Sources: Binance incident reporting: forbes.com · thehackernews.com · decrypt.co · NIST SP 800-61 Rev. 3 (2025): csrc.nist.gov · GDPR Art. 33: gdpr-info.eu