

THE HEIST CONTROL CHECKLIST **INSIDER EDITION**

The most dangerous person in any system is the one trusted to protect it. Twelve questions that check whether anyone at your company could do quietly what the lottery's security director did. Answer them about your own team, or about a vendor you're about to trust.

1 NOBODY AUDITS THE AUDITOR

who checks the person who checks?

- ☐ **Can one person write a change, deploy it, and sign off that it's safe?** If one name appears in all three places, that's the finding.
- ☐ **Who reviews the security team's own access and changes?** It must be someone outside that team's reporting line.
- ☐ **Is there a written list of duties that must never sit with one person?** Examples: requesting access and approving it, paying a vendor and adding the vendor.

3 NOBODY IS ALONE WITH THE MACHINE

who can touch it unwatched?

- ☐ **Does any critical system or room allow access by one person alone?** A two-person rule ends most insider stories.
- ☐ **Are USB drives and other removable media blocked on critical machines?**
- ☐ **Do the cameras and logs capture enough to reconstruct what happened?** A system that records one second per minute isn't recording.

2 SOMEONE ELSE READS THE CODE

is what's running what was approved?

- ☐ **Does every production change get reviewed by someone other than its author?** A trusted senior engineer still needs a reviewer.
- ☐ **Can you prove the file running today matches the version that was reviewed?** Look for a build record, a checksum, or a signed release.
- ☐ **Would an unexplained condition in critical code get questioned?** An example is logic that behaves differently on certain dates. Someone has to be reading closely enough to ask.

4 WATCH THE OUTPUTS, NOT JUST THE LOGS

would anyone notice a wrong result?

- ☐ **Does anyone review results for patterns, not just alerts?** Look at who keeps winning, which approvals cluster on one person, and which dates repeat.
- ☐ **Are the people who benefit from an outcome checked against the people who control it?** That means relatives, former colleagues and shell companies.
- ☐ **Does a large payout or transfer require a verified human name before it goes out?**

SCORING **10-12** Your controls would have caught him before the second jackpot. · **6-9** The gaps are in review and detection, which is where insiders hide for years. · **0-5** Start with question 1. Separating duties is the cheapest control on this page.

Cyber Heists: how the big breaches actually happened, and what was missing.

New episode weekly. Reply with the case you want next.