A Companion To The Oversight Checklist

What a Good Answer Sounds Like

You don't need to be a technologist to tell a strong answer from a weak one. For four of the questions on the checklist, here is the difference between an answer that should reassure you and one that should prompt a follow-up.

When someone clicks a bad link, what happens next?

A WEAK ANSWER

"We note it in the employee's record and assign them extra training. Repeat offenders get written up."

A STRONG ANSWER

"We thank them for flagging it, then we ask how it got past our filters and what we can fix. People aren't afraid to tell us."

How do you measure whether security training is working?

A WEAK ANSWER

"Everyone completed the annual training. We're at 100 percent, and we keep the certificates on file."

A STRONG ANSWER

"Completion is our floor. What we watch is the phishing reporting rate, how fast people report, and whether repeat clicks are going down over time."

Where does security sit, and does it have your attention?

A WEAK ANSWER

"IT handles security. They bring us an update once a year, and we approve the policy."

A STRONG ANSWER

"Our security lead briefs us regularly and can reach the board directly. Security is part of how we set executive goals, not a once-a-year item."

Your phishing test came back with very few clicks. Good news?

A WEAK ANSWER

"Yes. Click rates were low, so our people are clearly careful. We're in good shape."

A STRONG ANSWER

"Low clicks are fine, but the number we care about is the reporting rate. Did people report the test email? Silence worries us more than a click."

The pattern to listen for: Weak answers tend to be about paperwork and blame. Strong answers are about what people actually do, what gets measured, and whether staff feel safe speaking up. When in doubt, ask the same question two different ways and see if the story holds.