Insider Risk Resolution
Decision Tree

An incident has occurred → **The incident/actions**
- ✓ Do not violate internal policies
- ⚠ Violate internal policies
- ✕ Are illegal or criminal

Was it intentional?

YES ← → **NO**

YES branch

What was their motive?

Motive could help understand the situation.
Was the individual under pressure to complete a task?
Did they have financial incentives or revenge?

→ **Malicious**

Were there any suspicions?

YES

If co-workers/managers had suspicions were they reported?
If no, why not? If yes, was the individual on persons of interest list, or were concerns dismissed?
Are reporting forms confusing?

NO

What did they do to avoid suspicion?
Were there signs that were ignored by co-workers and/or managers?

This is an opportunity to educate employees on common indicators.

NO branch

Avoid harshly punishing individuals for unintentional actions, instead revisit training.
If the individual was outsmarted e.g., by a phishing email, investigate if anyone else has been targeted.

→ **Non-malicious**

Is it a common behavior in the organiztation?
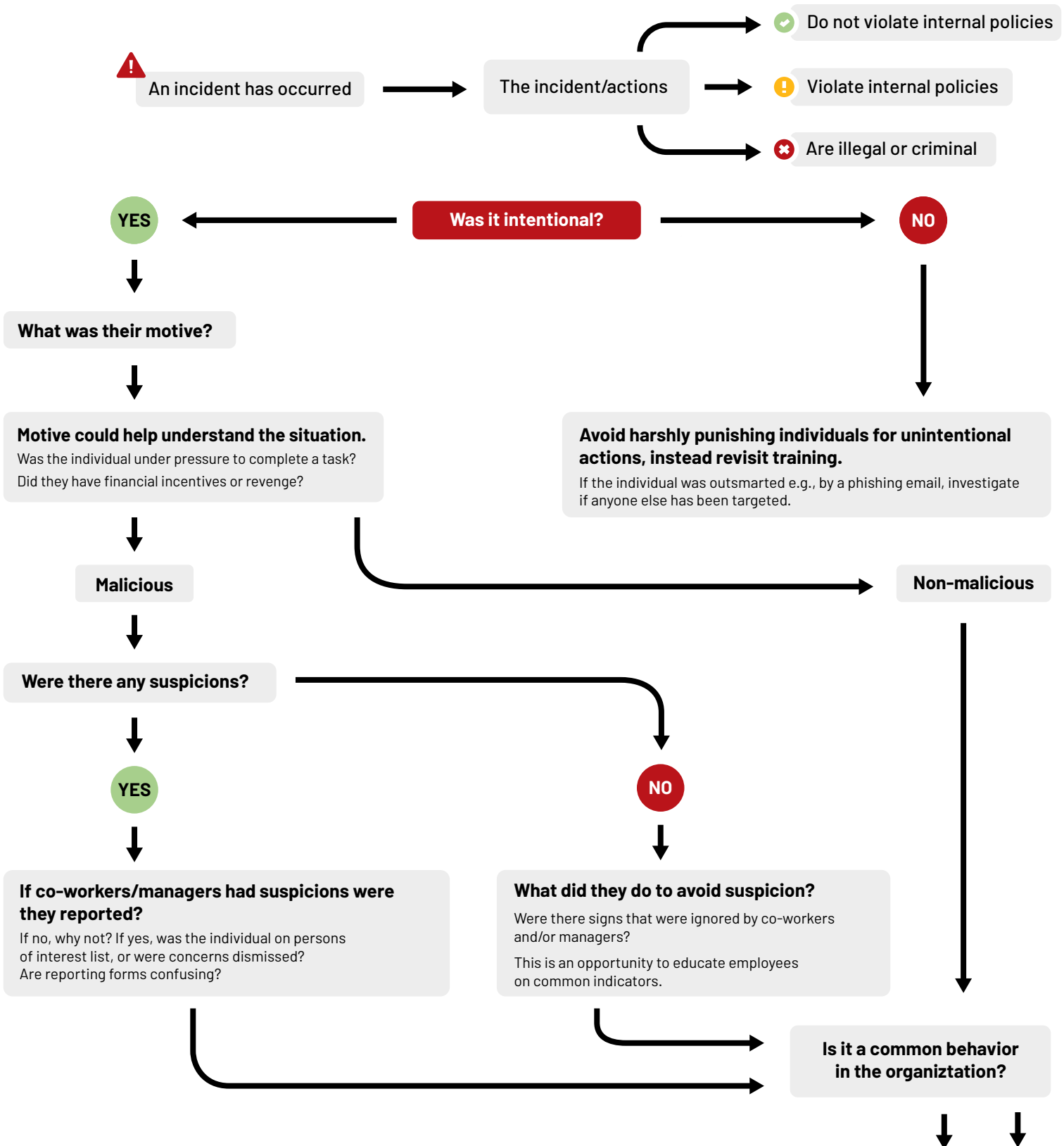
If actions are common, you shouldn't be focusing on one individual, instead look at changing the culture, reminding people of current policies or implementing new ones, and blocking access to sites/applications you do not want employees using.

YES → **NO**

Did internal systems/protocols raise the individual as a risk?

YES → **NO**

Was the individual on a persons of interest list?
Look at what was done well and what could be done better for future incidents.

Be mindful about avoiding targeted investigations. If someone is unfairly targeted this could lead to legal action for wrongful dismissal or disciplinary action.
Conversely, if the individual was showing signs of disgruntlement and/or malicious behavior and they were not viewed as a higher risk, why?

Yes, a third party ← **Were other people involved?** → **NO**

Who is it? What is their motive? Are they a competitor? Is a legal response warranted?

Yes, other workforce member/s

How did they avoid suspicion? Were tasks split? Was one individual the leader?

Did they experience any challenges?

YES → **NO**

Were there any security measures that acted as a deterrent?
Were there moments that they thought they would not go through with the attack? When the roadblocks that an individual faced are known, this could help in the mitigation of future incidents.

What challenges should they have experienced?
Are security measures working effectively or easily worked around? What would have stopped the individual from causing an incident?

Finalize investigation