

AWARENESS AND HUMAN RISK

Security awareness that changes the work

Use evidence and real working practices to design targeted security awareness, better processes and meaningful follow-up.

By Haroon Mahmood

A training dashboard can tell you who completed a course. It cannot, on its own, tell you whether a payment change is checked properly, whether staff can share sensitive files safely or whether someone will report a mistake in time for the organisation to respond.

If you are responsible for awareness, start with the work you want to make safer. This guide explains how to use evidence, conversations and a small practical intervention to improve a particular task. It is aimed at security leads, HR partners and managers who want useful results from the time people spend on security.

Start with a task people recognise

In previous in-house work on awareness and human risk, I combined information from security tools, incidents and threat intelligence with evidence about how people carry out tasks. I used that evidence to focus awareness activity and worked with process owners when it pointed to weaknesses in how work was organised.

That experience informs a simple starting point: choose a business task and ask what could go wrong. Examples include changing supplier bank details, granting access to a contractor, sharing an employee report or responding to an unexpected request for a password reset.

Write down the desired action in terms someone can demonstrate. “Be more vigilant” is difficult to test. “Check a request to change payment details through the approved verification route before updating the supplier record” gives the person a clear action, provided that route exists and is usable.

NIST's [guidance on cybersecurity and privacy learning programmes](#) supports tailoring learning to organisational needs and evaluating it as those needs change. The practical implication is to define the task and its intended result before choosing the training format.

Gather enough evidence to understand the problem

Look at more than one source. Incident records may show what happened; support requests may reveal what was confusing; process owners may explain why people took a shortcut. Technical data can show where suspicious messages or risky sharing settings are appearing. None of those sources tells the whole story alone.

Ask a few people to talk you through the task. Where do they find instructions? What happens when the usual approver is away? Does the secure option work on the device they use? Is there pressure

to finish before a deadline? These questions can expose an obstacle that another awareness email would leave untouched.

Define the limits of the analysis before combining datasets. Agree its purpose, access and retention with the appropriate HR, privacy and security colleagues. Use aggregated information where it answers the question. Keep identifiable data restricted to a justified need, explain the activity appropriately and avoid building individual risk rankings from noisy indicators.

A high count of reported messages may mean a team encounters more attacks or is more willing to report. It is not, by itself, evidence that the team behaves less securely. Record the size of the population, exposure and any changes in the reporting process before comparing results.

Choose the intervention that fits the cause

The response may include learning, but it may also require a process or technical change. If employees keep sending sensitive attachments because approved sharing is inaccessible to their recipients, demonstrate a workable route and fix the access problem. If a payment check relies on one person, define cover and authority for absence.

A useful change has a business owner, a specific behaviour or control to improve, a delivery date and a way to observe whether it works. Keep the initial change small enough to learn from. You might combine a short team discussion, an instruction placed beside the task and a change to the approval workflow.

The NCSC's [phishing guidance](#) recommends layered protection, including technical controls and response arrangements. It also cautions against expecting staff to identify every malicious message. Learning should support those protections, with a route for people to ask for help when they are unsure.

A worked example - changing supplier payment details

This is an illustrative example of how to apply the method, rather than a claim about a past client engagement.

A finance team receives legitimate bank-detail changes by email. Staff know fraud is a concern, but the verification instructions do not explain what to do when the supplier's usual contact is unavailable. An urgent payment can therefore create pressure to improvise.

First, the finance owner checks how requests are handled in practice. The team agrees a verification route using contact details already held in an approved record, rather than details supplied in the change request. It also defines who can resolve exceptions, how a change is authorised and where the check is recorded.

Next, the team walks through a realistic request together. Staff practise finding the approved contact, recording the check and escalating an unresolved request. The process owner confirms that those steps fit the team's workload and that there is cover for absence. Access to amend supplier records and any additional approval controls are reviewed alongside the learning.

The follow-up checks a sample of actual change records for the required evidence. If records are missing, the team asks why: unclear instructions, a workflow limitation, an unavailable approver or an

action not taken. The next intervention follows that finding. Course completion remains useful administration, but the check is tied to the task that matters.

Measure carefully and make reporting worthwhile

Choose measures before the pilot, and note what each one can and cannot show. Useful questions include whether people can find the instruction, carry out the action, obtain help and recover when something goes wrong. Include feedback from the people doing the work alongside operational evidence.

If you use phishing simulations, be clear about the purpose and agree the approach with relevant internal stakeholders. Consider message difficulty, audience and exposure when comparing click rates; [NIST's Phish Scale research](#) explains the influence of message difficulty and work context. A simulation is a limited observation, not a measure of an individual's trustworthiness or proof that the organisation is protected.

Thank people for early reports, including reports made after they have clicked or shared something. Give them a clear next step and close the loop where possible. Avoid public rankings and blame. The NCSC's [security culture principles](#) emphasise the importance of leadership, trust and an environment that supports secure behaviour.

Look for evidence of the desired change over a sensible period. A short pilot with few events may not support a meaningful numerical conclusion. Record that uncertainty, keep checking and avoid attributing a change in incident numbers to training alone when technical controls or attack volumes have also changed.

A one-page intervention brief

Use these prompts with the process owner before commissioning content or buying another tool:

- **Task and consequence:** What are people doing, and what could go wrong?
- **Evidence:** What have you observed, from which sources, and what is uncertain?
- **Desired action:** What should someone be able to do in the real workflow?
- **Obstacle:** What makes that action difficult, unclear or easy to bypass?
- **Changes:** What will the process, technology and learning owners each deliver?
- **Support:** Where can someone ask for help or report a mistake?
- **Evaluation:** What will you check before and after, and what would justify changing the approach?
- **Data handling:** What information is necessary, who may see it and when will it be removed?

Start with one consequential workflow. If the result is useful, adapt the method to the next area rather than assuming every team needs the same intervention.

Kurosec's [security programme development](#) includes awareness and human risk, with an emphasis on practical controls and how people work. [Contact us](#) to discuss a focused improvement to your programme.