How to measure the success of cyber security training in your business

One of the most widely used methods of evaluating the success of training is using the **Kirkpatrick Model**, offering a four-level approach (Reaction, Learning, Behaviour, and Results) to measure the effectiveness of training provided.

The Kirkpatrick Model, developed by Donald L. Kirkpatrick, is a widely used framework for evaluating training programs and assessing their effectiveness. The model consists of four levels, each representing a different aspect of evaluation. **These levels are:**

1 Level 1
Reaction

How did the participants react or respond to the training?
As communication is vital in a cyber culture, checking in with your team to uncover how they found the training is crucial. You want your team to feel that cyber security training is valuable. Measuring how engaged they were and how they reacted to the training helps you to understand how well they received it.

Gathering feedback through surveys or interviews allows you to better understand their satisfaction, engagement, and perception of the training.

Here are some important questions to ask your team:

- Did you feel that the training was worth your time?
- What were the biggest strengths and weaknesses of the training?
- Did you like the gamified element of learning?
- Was the platform engaging?
- What are the three most important things that you learned from this training?
- From what you learned, what do you plan to apply in your job?
- What support might you need to apply what you learned?

2 Level 2
Learning

What did participants learn from the training?

A great way of measuring learning is to initially create individual learning objectives with your team to accurately measure their progress to date and hold your team accountable. The TryHackMe management dashboard allows you to easily create branded learning paths aligned with skill requirements, to give your team personalised training.

We recommend conducting assessments or tests to measure the understanding of key concepts, best practices, and specific technical skills to allow learners to demonstrate their knowledge of cyber security principles and techniques.

3 Level 3
Behaviour

Did the trainees take what they learned and put it into practice on-the-job?

In a critical industry with an ever-increasing risk of cyber attacks, your team's behaviour and attitudes towards taking precautions is a crucial factor. Be sure to introduce processes that encourage, reinforce and reward positive behaviours.

Monitor behaviour changes by observing their adherence to security policies, their ability to identify and respond to threats, their implementation of secure coding practices, or their adoption of secure data handling procedures. You can gather feedback through observations, performance evaluations, or self-reporting mechanisms.

4 Level 4
Results

Did the training meet the stakeholders' expectations? What was the return on these expectations (ROE)?

Evaluate the effectiveness of the cyber security training by examining relevant metrics, such as the number of security incidents or breaches, the time taken to detect and respond to incidents, the reduction in security vulnerabilities, or the overall improvement in the organisation's security posture. By comparing pre-training and post-training data, you can determine the extent to which the training has influenced these outcomes.

TryHackMe features a management dashboard that allows progress monitoring across employees, to understand the results of internal training. This enables you to assess employee progression across cyber security skill sets.

TryHackMe upskills and arms teams with knowledge of tools and practices to mitigate cyber attacks, and can be a pillar to building cyber culture.

Reach out to our team today to *ingrain cyber security training* into your company culture!

tryhackme.com | *sales@tryhackme.com*