Guide to Cybersecurity Training Metrics

Improve how you measure the success of the training.

Table of Contents

Introduction

Since cybercrime has become a significant threat, regulators have stepped in to support organizations in reducing their cyber risks. As a result, security awareness training has become an essential component in achieving this. Organizations have been focusing on creating awareness around cyber threats, and they have been trying to measure the success of this training with tests, quizzes, or periodic phishing tests.

The main objective of awareness training has always been to reduce organizational risks related to employee actions. However, when employees complete the training, they may not necessarily know what to do with a real-life threat.

Employees are the prime targets for social engineering and phishing attacks. Employee actions and errors are still one of the primary causes of security breaches. Yet, awareness training may fail to prepare people for resisting social engineering attacks adequately.

Practical exercises that teach the correct security behavior are necessary to reduce these human risks and minimize the chance of an attack on the organization being successful. To determine whether the training positively impacts reducing risks, monitoring the right metrics for employee progress is necessary.

Behavior-changing training is a measurable way to make a positive impact on your defenses. This guide aims to explain some of the shortcomings of the more typical awareness training metrics for social engineering education and provide an alternative method for measuring behavior change. This method provides more descriptive and realistic metrics for measuring your company's security and risk level.

The shortcomings of security awareness training metrics

As part of awareness training, organizations may test people's knowledge and skills infrequently using phishing simulations. When performing these simulations infrequently, a lack of personalization on aspects such as difficulty, variety of content, or the individual point of view means that the results won't provide a realistic outlook on each employees' security skills. With infrequent, one-size-fits-all training, you can't track their real progress. You can't be sure if employees know how to recognize an actual cyber threat and react appropriately.

In the next sections, we will explain the pitfalls of the awareness training metrics that organizations frequently use to report for one-size-fits-all and infrequent employee phishing tests.

The failure rate per campaign

The failure rate is also known as the click rate; it measures how often an employee performs an unsafe action when they conduct a phishing testing campaign. Security awareness training and phishing tests use this metric to assess levels of success. The failure rate is a standard metric, and organizations may rely on it heavily. Many believe that the failure rate per campaign is the best metric to describe their organization's risk regarding phishing and social engineering attacks. However, the failure rate is not the best metric for assessing success when the simulations are infrequent and follow a one-size-fits-all strategy.

The common misconception is that the lower the failure rate, the better the training performance must be, but this is not true. A low failure rate does not necessarily tell you anything about the success of the training.

When only a small percentage of employees report the phishing simulation, the failure rate doesn't necessarily represent the majority's skills and success. You don't know how the other employees would react and, therefore, don't have metrics for how the organization would perform as a whole.

“

It’s a myth that the lower the failure rate, the better your employees perform in the training.

The failure rate also depends on the simulation's difficulty level and the employee's skill, knowledge, and experience level. It's a volatile metric because it's easy to fabricate low or high failure rates artificially. Do you want to lower the failure rate? Send out easier phishing simulations that even the least experienced employee can easily recognize. The moment you start sending out more difficult ones, the failure rate could jump up significantly.

With traditional awareness training, another issue is that some companies stop training those that reported the test successfully. They only train that part of the employee population who failed the test by clicking an email link, downloading a file, or giving away their credentials. The moment you stop training those that did not fail the test, the reporting rate only tells the story of those that failed. As they may attach negative feelings toward security training, they may stop reporting suspicious activity, lowering their engagement with their security responsibilities.

The failure rate can be a useful metric when the training is right. Each employee should receive frequent and personalized training in terms of content, difficulty, and individual points of view. We'll shortly explain when failure rates can provide useful and descriptive metrics.

The pass rate

The pass rate is a typical metric used for awareness training, but its basis may be on the employee not performing an unsafe action. For example, if an employee does not click on a test email link, they may be judged to automatically pass the training, even if they, for some reason, missed or ignored the training email. This approach means that you can't measure if they know how to identify the threat correctly.

When people ignore the test, the pass rate could be outstandingly high. It may look like your organization is in safe hands. In reality, employees may easily fall victim to an attack the next time a well-crafted spear-phishing email reaches their inboxes.

At Hoxhunt, we don't use the pass rate. The reporting rate replaces it entirely. Those people that did not report the test do not automatically pass the training. It means that if 70% of the population correctly reports, there are still 30% that are not actively learning. We include people that are not actively reporting in the miss rate.

The pass rate

“

A simple reporting process **is key to increasing the reporting rate.**

The reporting rate

Infrequent phishing simulations can also use the reporting rate. Ideally, the reporting rate is the primary metric to follow. It's an important metric as it tells you how many people engaged with the training. The goal should always be to engage as big a part of the population as possible so that you know that those people are actively shielding your organization and its assets from attacks.

For the reporting rate, a good quality reporting process is mandatory. With a simple process, people will encounter a lower barrier when it comes to reporting phishing emails. When people report, you know that they are engaged, learning, and acquiring the knowledge and skills to face actual threats.

When the reporting process is complicated or intrusive on their normal routine, such as calling the security team or finding the reporting email address and following the instructions on what to do, people may not report anything. You won't know whether they identified the threat, they didn't notice it, or they just by chance didn't interact with it.

Key takeaways awareness training metrics

The failure rate

• This is not the right metric for assessing success when the training is infrequent and same for all.

• A low failure rate does not tell about the success of the training.

• When you only train employees who failed, the reporting rate does not tell how the others perform.

The pass rate

• When people did not fail the training, they automatically pass it even if they missed or ignored the training.

• When people ignore the test, the pass rate can be high and it may look like your organization is in safe hands.

The reporting rate

• Security awareness training can also use the reporting rate. Ideally, this is the primary metric.

• When the reporting process is complicated, people may not report threats they see. You won't know whether they identified the threat if they decided to leave it alone.

“

Aim for at least

70%

reporting rate.

Measuring behavior-changing training

Security behavior change is measurable. With frequent training, it's possible to track the progress of individual employees and the company as a whole.

Security behavior means that people know how to spot and report threats because they learn the habit through frequent and personalized simulations. When people start correctly reporting both simulations and real threats, you will have guaranteed improvements compared to the results of traditional security awareness training. You will have more data points available to measure both people's training success and real threat reporting.

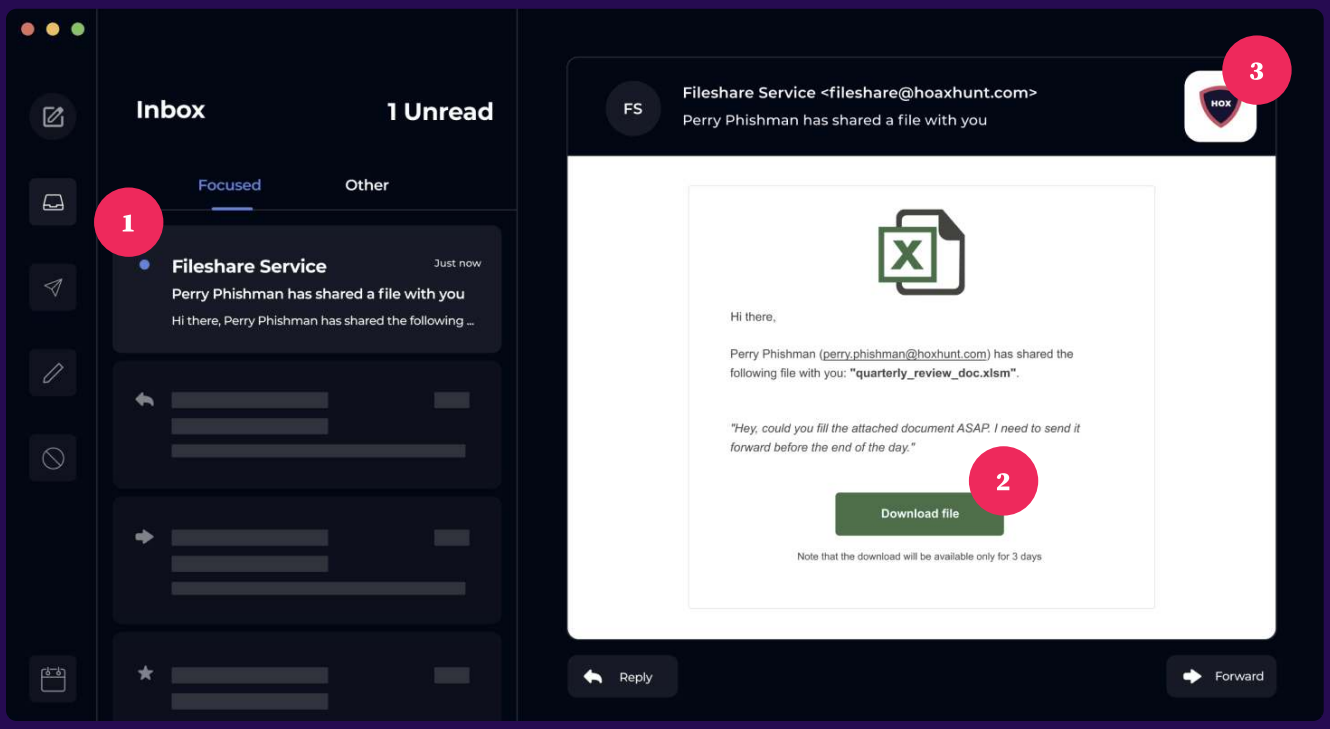
The measuring frequency

Frequent and practical training that reflects the sophisticated and ever-improving real-world threat landscape provides you with data on how your people regularly perform. Based on the results from a few simulations, it's hard to tell whether the training has been positively impacting people's behavior and reducing the cyber risks for your organization. With frequent training and measurement, you can follow how people react to the training and what it means in terms of the overall assessment of security risks.

Did you know?

A good reporting process is a must for improving the reporting rate of both simulations and real threats. When the process is simple, it is a lot easier to report phishing emails. It's common to overlook having a reporting button, but it's a simple solution for encouraging people to report threats.

Good reporting process



1

Open the email

The email could be an everyday email, a phishing simulation, or an actual phishing email. Always be mindful when you open an email.

2

Recognize the danger

Whenever you open an email, think critically before you click. Could it be a possible threat? Take the normal precautions before you click on links or attachments.

3

Report the email

If the email is suspicious, report it. If it's a simulation, you will get immediate feedback. If it's a real threat, you just saved the day!

The reporting rate

When the training focuses on behavior change, the reporting rate is the most important metric. The goal must be to engage as many of the employees as possible to obtain data on how people develop their threat recognizing and reporting skills, both in the simulations and real life.

Average simulation reporting rate per employee

Goal: Aim is for high engagement. When people correctly report, you will have data on their progress. It's vital to engage all employees, not only those that previously failed the test.

The average simulation reporting rate tells about how many people have engaged with the training. At Hoxhunt, we advise our clients to aim for at least an average 70% reporting rate. This is because when over 70% of employees keep reporting threats, you know that the chances of them making an error and falling for an attack are lower as they are adopting safe email practices.

The reporting rate is almost the only consistent metric. With people-first training, you keep educating all people regardless of if they've failed the simulation or not. This is why the reporting rate gives you a good indicator of the whole population's level over time.

The reporting rate tells you that people are actively learning, and you can be more confident that they will do the right thing when they face real threats.

The real threat reporting rate

Goal: Catch attacks faster and before an incident can happen by motivating your employees to report all the threats they encounter. They can become an additional defensive layer and help you prevent a breach from happening.

The training's ultimate goal is to teach people to recognize and report cyber threats, which can be invaluable for preventing a breach and gathering data on the attacks that get through your email filters.

The failure rate

A low failure rate is not always an indicator of successful training. The failure rate depends on factors such as difficulty level, variety of the content, individual points of view (also referred to as personalization), timing and frequency, and positive reinforcement and feedback. However, the failure rate can be a crucial metric if used in a meaningful way.

Difficulty level

People can have widely varying skills based on the time spent in training or any previous security education. When employees receive simulations that are too easy, it will likely lower the failure rate. They may also start developing negative feelings towards the training because it's not challenging enough for them, and they may not feel like it's worth their while engaging with it.

When you adjust the simulations' difficulty level for each individual, the average failure rate will become a far more useful metric.

Variety of content

In another of our guides, we've written in-depth about why the test emails' content is so important. It's not useful to send the same content to everybody for two main reasons.

First, people with different backgrounds and roles need different content tailored to their experience. For example, content should vary based on who they typically interact with or what tools and software they use.

Second, attackers are quickly coming up with new attack vectors. When people don't frequently see relevant and up-to-date simulations, they are more likely to fail the test or not interact with the test at all.

An individual point of view

Every employee has a different background and a psychological profile. This means that people are prone to different types of social engineering. For instance, someone might be naturally very curious, while someone might react very strongly to fear-based attacks. Thus the failure rate is always individualistic. One attack type might work better for others based on their psychological profile and their skills, and the same attack could never make someone else fail.

Thus, measuring the failure rate with a benchmark does not tell about your organization's overall risk profile. An individual user's failure rate and the reporting rate will vastly vary user by user based on attack theme and difficulty.

An advanced targeted attack exploiting the individual's weaknesses might have a 100% failure rate for a person who has been participating in the training for a short while. For another user who has been taking the simulations for a longer time, the failure rate can be much lower.

This is why the average failure rate doesn't provide insights into learning and risk reduction progression. Measuring failure based on cohorts created by users' performance level, on the other hand, gives insights about the risk.

The failure rate with people-first security awareness training

<table>
<tr><th colspan="2">TRAINING EVERYBODY</th></tr>
<tr><td>FREQUENT TRAINING</td><td>VARYING DIFFICULTY LEVEL</td></tr>
<tr><td>VARIETY OF CONTENT</td><td>INDIVIDUAL POINT OF VIEW</td></tr>
<tr><td colspan="2">THE FAILURE RATE</td></tr>
</table>

Descriptive to the organization’s risk level

Jane

Advanced

LOCATION: USA

LANGUAGE: English

DEPARTMENT: Marketing

Enrolled to Hoxhunt: February 2019

Simulations received: 56

Reporting rate: 53/56

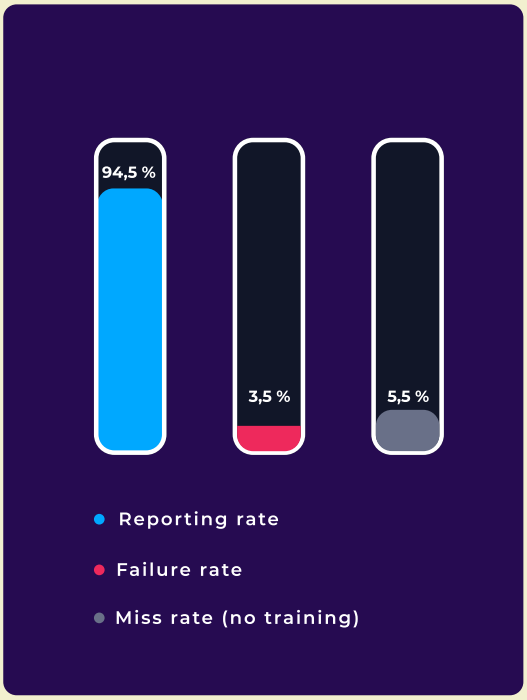
Failure rate: 2/56

Miss rate: 3/56

Simulation types: Common phishing, targeted spear phishing, targeted co-worker phishing

Triggers: Fear

Geography & Culture: North America



Bob

Beginner

LOCATION: Germany

LANGUAGE: German

DEPARTMENT: Finance

Enrolled to Hoxhunt: April 2020

Simulations received: 12

Reporting rate: 12/12

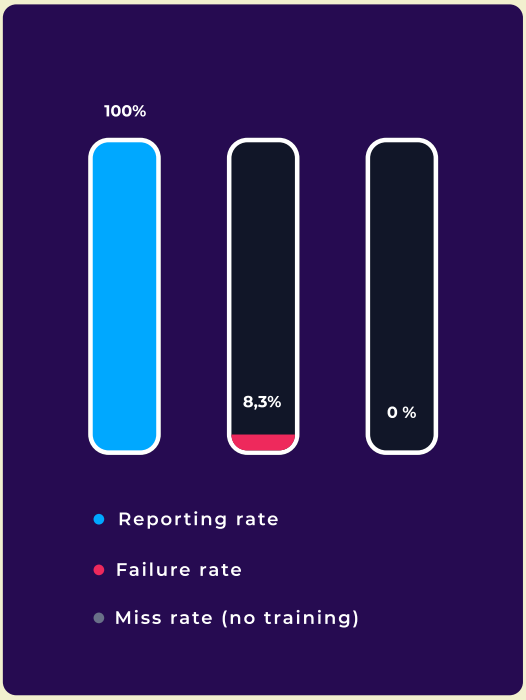
Failure rate: 1/12

Miss rate: 0/12

Simulation types: Common phishing, targeted spear phishing, targeted co-worker phishing, finance-related vectors

Triggers: Curiosity

Geography & Culture: Germany



Timing and cadence

When you send out the phishing test for the whole company at the same time, the word may get around fast to watch out for a phishing email. These warnings will likely lead to an artificially lower failure rate.

When the simulations' frequency is as often as once every ten days, you can follow the failure rate's progress. It will provide a better indication of how the organization is progressing. Attacks also arrive randomly: the test gives the most realistic result in terms of failure rate metrics when it appears realistic and catches people off-guard, for example, during a stressful day.

Positive reinforcement and feedback

Using positive reinforcement and giving people feedback can have a significant beneficial impact, whether they fail or not.

People will understand that it's okay to fail a simulation because they will know that they can do it without consequences; instead, they will be encouraged to try harder to succeed the next time.

Don't aim for a zero failure rate

It may sound like a good idea to aim for a zero failure rate, but that shouldn't be your goal. When people fail a simulation, it's not the end of the world. When the process is reasonable and provides feedback or micro training, they can better learn from their mistakes.

You will also have more visibility into how your organization performs or which attack vectors are leaving your organization more vulnerable. When you know that you can provide more training on those specific topics.

Failing a test shouldn't be a negative experience. It should be a means of teaching everyone how to defend the organization better together. After all, the individual's improvement and dedication to participating in the training are more important than lowering the failure rate.

Cybersecurity sentiment

Even when you focus on behavior change and risk reduction, measuring cybersecurity sentiment with qualitative and quantitative surveys can be useful. You want to know how people feel about the training, their attitude, or their motivation to participate. Do they understand that it's important? Do they find it interesting? Is the service delivery good?

Don't create a survey just for the sake of gathering insights. Make sure when you ask for feedback on something, it's actionable, so you can react and improve the experience for the employees if necessary.

The miss rate

The miss rate is the percentage of users who did not click or report the simulation within a set period from receiving it. Typically we use a period of four days.

People may be out of the office for many reasons such as annual leave, sick leave, or traveling, so having a miss rate is natural. The miss rate is problematic because you don't get data, don't know whether people are learning, and report a real threat.

You still want to monitor this metric because you want to make sure that people did not stop engaging with the training. Comparing the miss rate with absenteeism rates will indicate this. If they do stop engaging, it's good to plan how you will reconnect with them.

Outcomes of people-first security awareness training

Increase

- Increase number of simulations sent
- Increase the number of reporting rate
- Increase number of reported simulations
- Increase number of reported threats

Decrease

- Decrease failure rate
- Decrease risk

Behavior change and measuring risk

Methodologies broadly vary on how you assess organizational cyber risk. If you want a quantifiable approach to human risk, measuring behavior change helps with that. Using metrics is essential to identify whether your employees may jeopardize security.

Engaging people is essential. People need to participate in training to track how they are performing. Employees need to continually learn to develop the right skills and knowledge to defend the organization from attacks.

Through constant improvement of the reporting rate and creating an environment where it’s acceptable to fail the simulations, you can develop a security culture where people feel motivated to be active participants of your layered security defenses.

When people get into the habit of reporting real threats, you will lower the risk of them clicking on malicious links and attachments or giving away credentials. You will also collect invaluable data from the threat reports for use in improving your incident response.


HOXHUNT