HOXHUNT

Security Engagement as a Service

Our objectives

Decrease your human asset risk

by delivering a spaced repetition learning program that makes your employees identify the attacks.

Increase your active protection levels

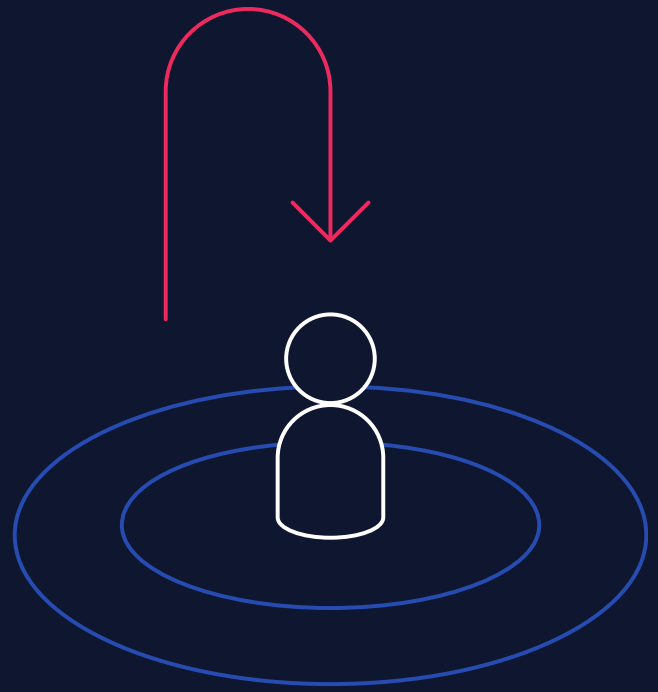
by reinforcing positive behavior of reporting possible attacks

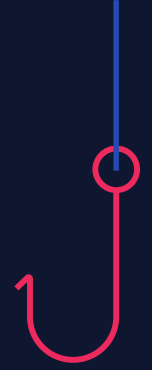
Change your cyber security culture

by creating engaging and lightweight training sessions with interactive content.

Free your resources

by automating everything in your awareness program





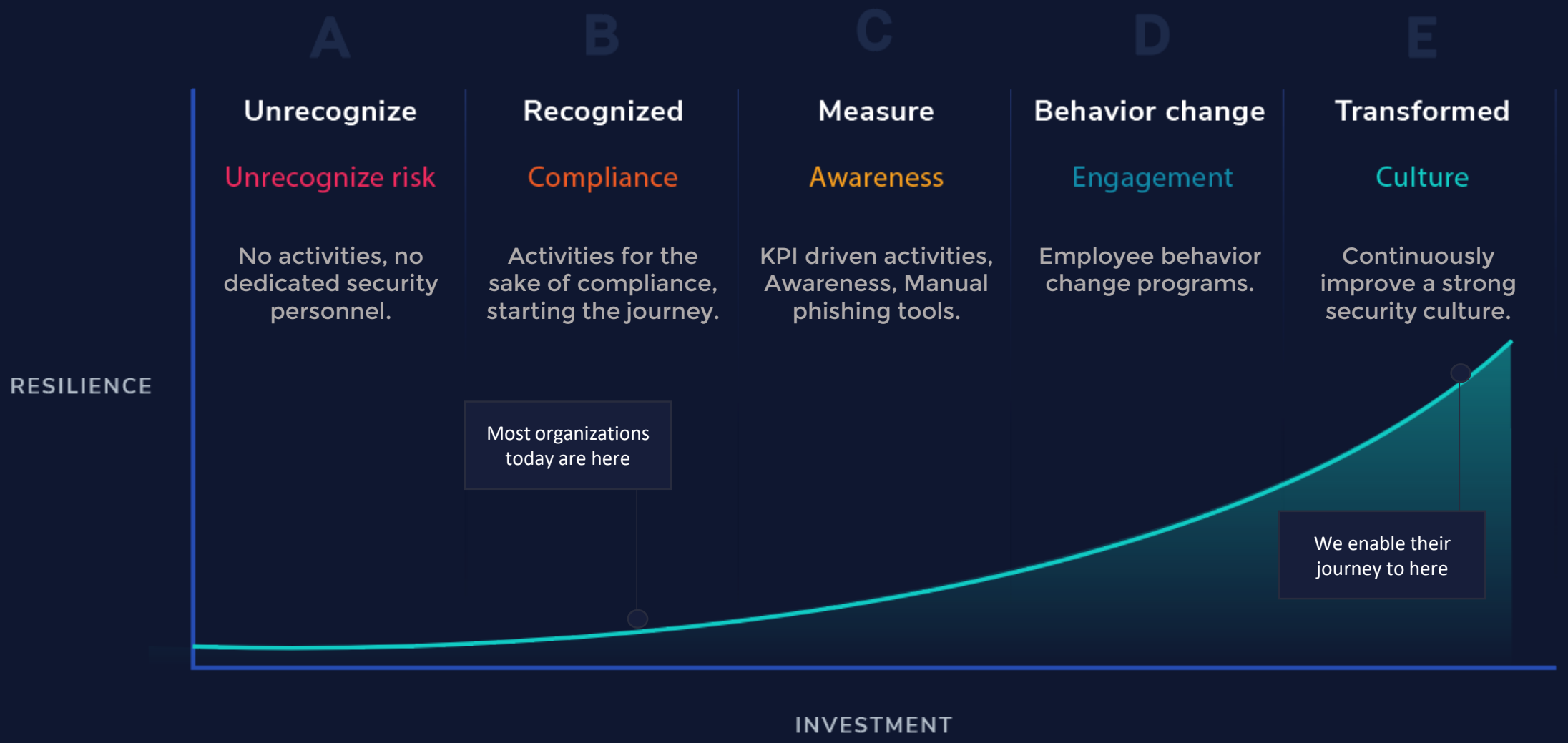
90%

of security breaches involved a phishing element

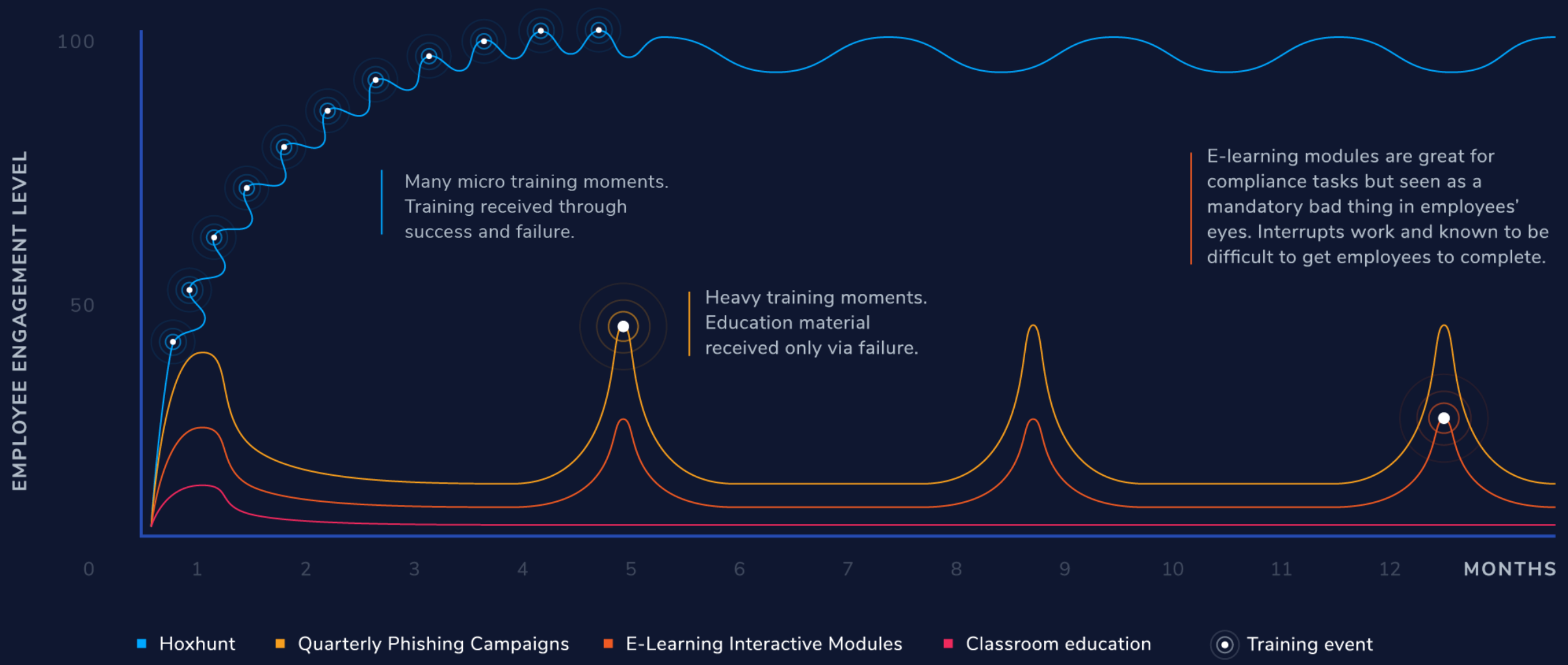
Verizon Data Breach Investigations Report 2017

https://www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/

Cyber Security People Maturity Model



High Engagement – High Reward

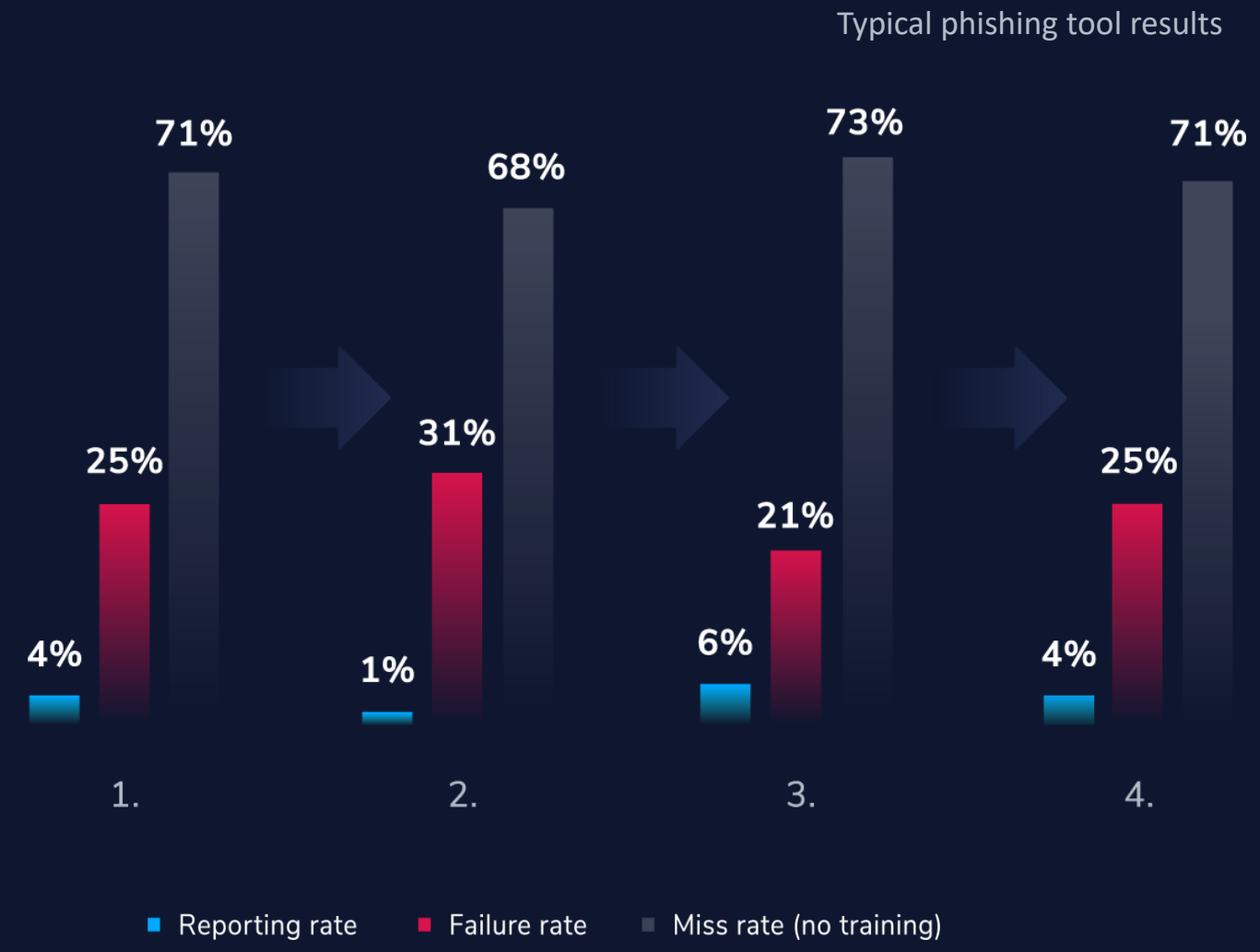


Manual phishing tools do not impact human asset risk

”We are using a lot of time in crafting phishing testsand then sending them to the organization. However,our failure rates vary from test to test. The only way toproduce less failure is to send our employees easiertests”

Manual phishing tools:

- Unable to reduce risk.
- Take a lot of time to operate.
- Engage employees to training only via failure, creating negative cultural effects.

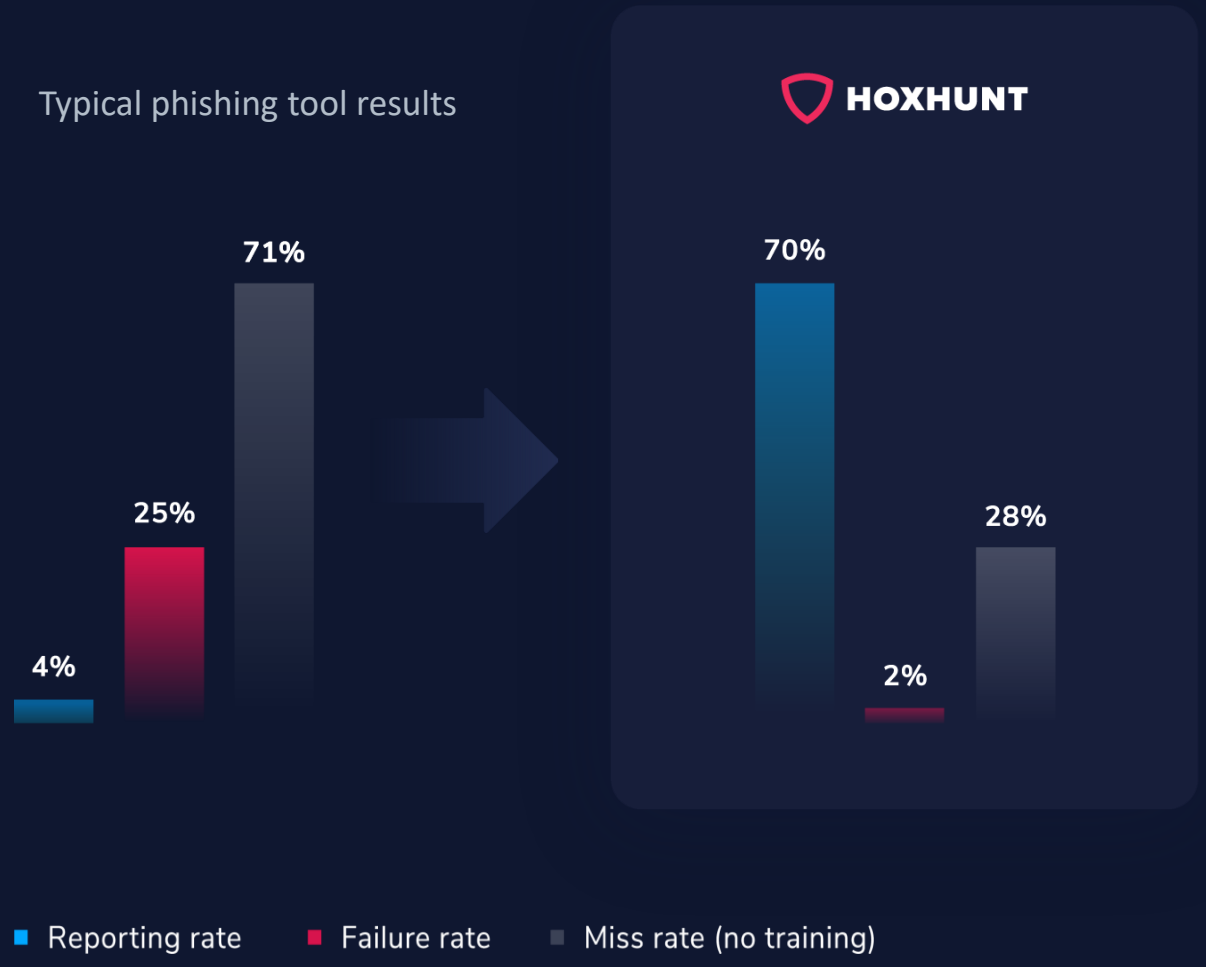


How to reduce human asset risk with behavior conditioning?

- Human mind searches for active behaviors.
- Telling employees **not to click**, is not an active behavior
- Therefore, in order to reduce click-rates, we need to provide an alternative behavior pattern that supersedes the behavior of clicking emails.
- This superseding behavior is the click of the Hoxhunt add-in. The Hoxhunt game engine reinforces the behavior pattern with rewarding for that behavior.

In class organisations are able to transfer to:

> **Low failure rate** (high human asset risk)
>
> **High report rate** (low active protection)
>
> **Low miss rate** (low training impact)



Why companies choose Hoxhunt?

1 – Risk reduction

Conditioning the human mind to an active behavior of attacks in return for rewards leads to:

- Decrease in phishing failure rate.
- Increase in phishing reporting rate.

2 – Automation

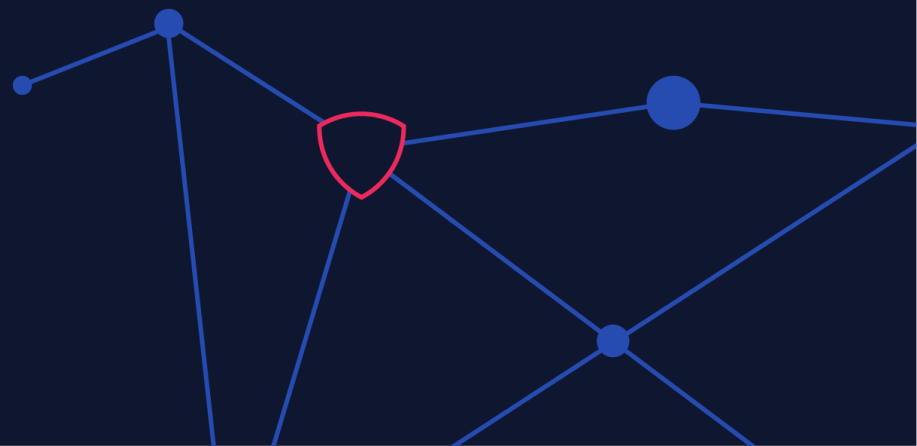
Automating the behavior change program leads to:

- Less time and money spent in thinking about how to train certain roles and user groups.
- Higher quality training by taking advantage of machine learning.

3 – Cultural transformation

Making the employee experience as engaging and enjoyable as possible leads to:

- Change of employees' attitudes towards cyber security.
- Change in employees' attitudes leads to them thinking about cyber security in various situations, enabling cultural change.

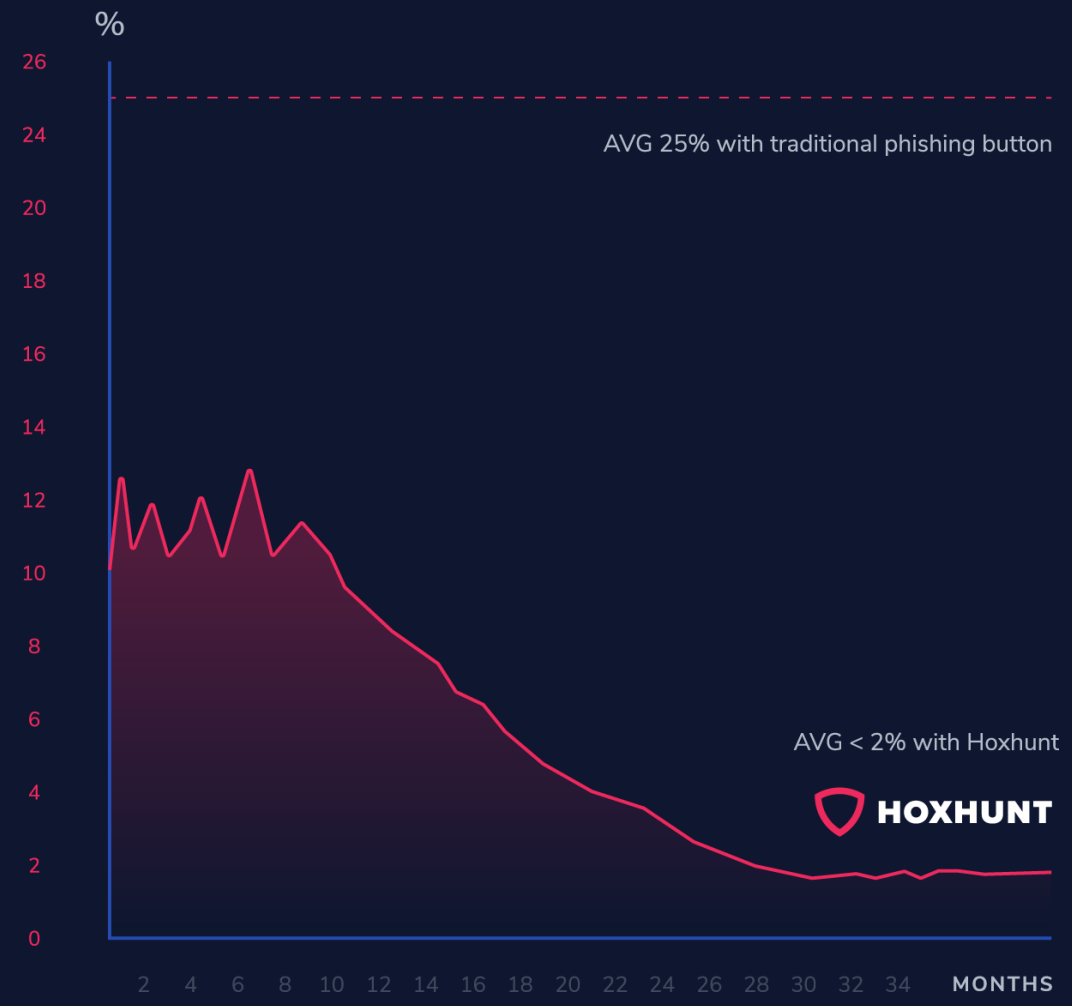


Global average reporting rate

The longer you have been in the training the higher your ability to react to attack is.

Global average penetration rate

The longer you have been in the training the less you have human asset risk.




HOXHUNT