

KnowBe4

## KnowBe4 Security Awareness Training and Simulated Phishing Platform — Cyber Catalyst Designation

KnowBe4's Security Awareness Training and Simulated Phishing Platform has been designated a 2019 Cyber Catalyst solution. It is designed to help organizations manage the ongoing problem of social engineering attacks by improving their last line of defense: the human firewall. Employees are often the weakest link in an organization's network security, as they are frequently exposed to sophisticated social engineering attacks.

The KnowBe4 Security Awareness Training and Simulated Phishing Platform uses a comprehensive new-school approach to help security leaders create and implement a fully mature training program for a more resilient and secure organization. With the platform, KnowBe4 takes a 360-degree approach to security awareness by integrating baseline testing using mock attacks, engaging interactive web-based training, and continuous assessment to keep security top of mind. It helps organizations create a more security-aware culture, by providing a robust and constantly updated training content library, real-world phishing simulations, one-click user reporting with the Phish Alert button, and affordable email threat identification and response using PhishER.

The platform comprises:

- **Baseline testing** to assess the Phish-prone™ percentage of users through a free phishing simulation.
- A comprehensive **library of security awareness training content**, including interactive modules, videos, games, posters, and newsletters, as well as automated training

campaigns with scheduled reminder emails. Three Training Access Levels are available.

- Fully automated **simulated phishing attacks**, including unlimited usage of thousands of templates as well as community phishing templates, available in a variety of formats.
- **Enterprise-wide reporting** with statistics and graphs for both training and phishing, ready for management reporting. Advanced reporting capabilities include 60+ reports providing an overview of an organization's last five campaigns as well as detailed reporting on key organizational awareness training indicators.
- **Risk scoring** via Virtual Risk Officer functionality that shows risk scores by employee, group, and the entire organization over time.
- **PhishER**, an add-on option for the automated identification and prioritization of suspicious emails reported by users.

Customization is key: KnowBe4's platform allows for tailored campaigns and spear phishing scenarios based on employee behavior and user attributes. Organizations can create customized, targeted phishing and spear phishing campaigns, training assignments, remedial learning, and reporting, as well as custom landing pages that allow for point-of-failure education.

*\*Product information provided by KnowBe4*

## Why the KnowBe4 Security Awareness Training and Simulated Phishing Platform is a Cyber Catalyst-Designated Solution

Cyber Catalyst participating insurers rated the KnowBe4 platform highest on the criteria of flexibility, performance, viability, and efficiency.

In their evaluation, the insurers characterized it as:

- “Great product, easy to use, vital for all businesses.”
- “Best in class capability for awareness training – user metrics are readily available. Effective in mitigating risks of social engineering and spear phishing.”
- “Flexible and easy to use interface makes implementation quick.”

## Insurance Policies and Implementation Principle

Organizations that adopt Cyber Catalyst-designated solutions may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers.

Those insurers, when considering potential policy enhancements, will expect organizations to deploy Cyber Catalyst-designated products or services in accordance with certain “implementation principles” that have been developed by the insurers with vendors of Cyber Catalyst-designated solutions.

The implementation principle for the KnowBe4 Security Awareness Training and Simulated Phishing Platform is:

- Training plans are configured to “high awareness”.

## Evaluation Process

Applications for evaluation of cybersecurity solutions were accepted from March 26 through May 5, 2019. More than 150 cybersecurity offerings, spanning a broad range of categories from hardware to messaging security to IoT security, were submitted for evaluation. Cyber Catalyst participating insurers evaluated eligible solutions along six criteria:

1. *Reduction of cyber risk.*
2. *Key performance metrics.*
3. *Viability.*
4. *Efficiency.*
5. *Flexibility.*
6. *Differentiating features.*

Cyber Catalyst designation was awarded to solutions receiving positive votes from at least six of the eight participating insurers, which voted independently. Neither Microsoft — which served as technical advisor — nor Marsh participated in Cyber Catalyst<sup>SM</sup> designation decisions.

The next Cyber Catalyst program is expected to open in 2020.

For more information about Marsh’s cyber risk management solutions, email [cyber.risk@marsh.com](mailto:cyber.risk@marsh.com), visit [marsh.com](http://marsh.com), or contact your Marsh representative.

For more information about the KnowBe4 Security Awareness Training and Simulated Phishing Platform, visit <http://www.knowbe4.com/cyber-catalyst>.

## 2019 CYBER CATALYST DESIGNATED SOLUTIONS

In the inaugural Cyber Catalyst program, 17 cybersecurity products and services have been designated as Cyber Catalyst solutions. More information about all the 2019 Cyber Catalyst-designated cybersecurity solutions is at [www.marsh.com/cybercatalyst](http://www.marsh.com/cybercatalyst).

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the “Marsh Analysis”) are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.