General

CybeReady enables companies to transform their security culture by ensuring continual organizational cyber readiness against phishing threats.

Why CybeReady?

- **CybeReady provides a highly effective, data-driven learning experience.** Your employees learn in real-time through relevant, memorable training episodes that adapt to their weaknesses. Security teams receive ongoing detailed reports that pinpoint vulnerabilities and ultimately, show quantifiable progress.

- **We believe the best phishing training is fully adaptive and culturally-sensitive.** What good is continuous security training if employees can spot it a mile away? We develop contextualized content specific to your industry, language and culture that mimic the efforts of the world's most advanced hackers. Your employees won't see us coming—and you'll be glad they didn't.

- **Our sophisticated solution doesn't require experts to use it**. Our expertise is built into our phishing readiness platform, so there's no need to invest additional time or to seek out external consultants to get the job done. With CybeReady, ease of use and optimal results go hand in hand, freeing up your staff's time to tackle other critical objectives.

- **Our phishing readiness program maximizes your investment while minimizing costs.** We recognize that success is measured in terms of positive outcomes as well as time and money spent; our solution is extremely affordable and (perhaps best of all) is managed by our experts, enabling your security team to focus on other important tasks.

- **Your employees will become enthusiastic partners in cyber security.** Our readiness programs have been proven to transform companies' security cultures, engaging employees across multinational organizations. This is not a solution that merely 'checks the box' of providing training; we pride ourselves on employees' actual growth and engagement.

- **We provide tangible results in minutes**. Time is money, and we're not interested in wasting yours. After a quick deployment, our phishing readiness platform begins making a positive impact on your employees' behavioral responses before you finish writing an email—without any implementation or oversight from your IT team.

We Phish For Fun .We Train For a Living

	Component	Customer Resources using a fully managed CybeReady solution	Customer Resources using a self-managed solution
1.	Implementation of dedicated server to enable solution operation	No Resources Required Pure SaaS, NO implementation/installation/ deployment required from any kind	Server implementation/installation/ deployment and monitoring is required
2.	Server maintenance	No Resources Required	Installing system & Security updates
3.	Planning the first campaign messages	Campaign plan approval and comments	Writing its own mapping plan, including generating and crafting attack messages repository to be presented for management approval
4.	Adjusted educational content development	No Resources Required	Using external consultant to develop and adjust the required educational content
5.	Design educational content & Customized Landing Page	No Resources Required	Using graphic designer to design and adjust the required educational content
6.	Design educational content using videos format	No Resources Required	Using external contractors to develop expensive educational content videos formats
7.	Matching Campaign Messages based on employees' performance	Approving CybeReady based on smart BI analytics	Needs to analyze employees' performances & statistics based on basic internal tools
8.	Matching Campaign Messages to organizational different groups （Users are grouped so a variety of attacks is provided to different groups）	Approving CybeReady based on smart BI analytics	Design and implementation of a diverse campaign according to the purchased or developed product limitation

We Phish For Fun .We Train For a Living

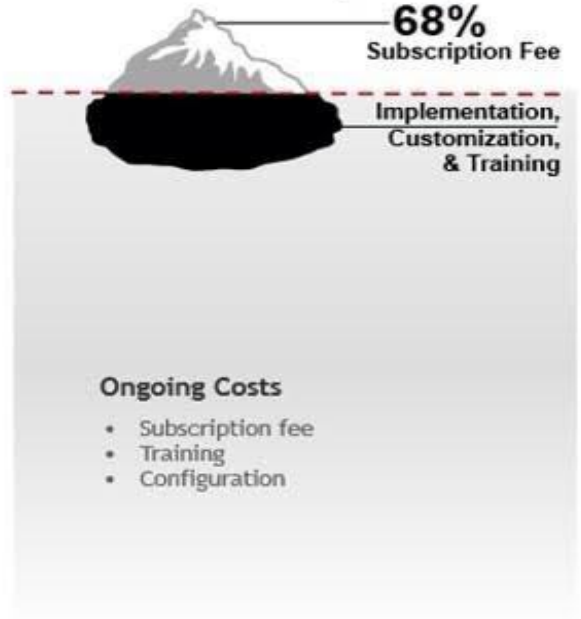| 9.	Implementing attack messages coming from regional organizations and international WW organizations	No Resources Required Customer enjoys CybeReady WW repository of attack messages	Significant Challenge
10.	Implementing attack messages coming from regional organizations and international WW organizations from identical industry segments	No Resources Required Customer enjoys CybeReady WW repository of attack messages	Significant Challenge
11.	Implementing department new creative attack messages ideas	No Resources Required Sending a request to CybeReady	Requires new content development and adjustments
12.	Management BI report	No Resources Required Monthly report, using Tableau Reader. The monthly report reflects: 1.Organization behavior related to phishing attack, 2.Solution's statistics and analysis 3.Users & Organization learning progress and effectiveness	Requires significant resources to centralize, analyse and reflect the statistics in a smart visual report
13.	Data and statistics production and processing of over time	No Resources Required All is conducted by CybeReady	Requires significant resources to centralize, analyse and reflect the statistics in a smart visual report
14.	Users updates	No Resources Required Sending info to CybeReady	Requires the Customer to Sync between new and veteran users
15.	Content adjustment to Internet Browsers ver	No Resources Required	Requires Customer to test compatibility for any new design

Why Cloud Computing for Professional Services Organizations?
Compared to On-Premise, the Cloud Offers Better ROI +
Shifts Fixed CAPEX to Variable OPEX

On-Premises

9%
Software Licenses

Customization &
Implementation

Hardware

IT Personnel

Maintenance

Training

Ongoing Costs

- Apply Fixes, Patches, Upgrade
- Downtime
- Performance tuning
- Rewrite customizations
- Rewrite integrations
- Upgrade dependent applications

- Ongoing burden on IT
- Maintain/upgrade hardware
- Maintain/upgrade network
- Maintain/upgrade security
- Maintain/upgrade database

Cloud Computing

68%
Subscription Fee

Implementation,
Customization,
& Training

Ongoing Costs

- Subscription fee
- Training
- Configuration